Click Here

Your network is only as good as the cabling. In this video, you'll learn about the characteristics of fiber communication, twisted pair copper cabling, cable categories, cabling in the plenum, and coaxial cables.>Many networking environments use fiber optics for their network communication. This is transmission using light instead of radio frequency. Since there's no radio frequency signal, it becomes very difficult to monitor or tap this information. You'll often see fiber optics used in very highly secure environments.One of the advantages of light, of course, is that it's very slow to degrade. So we can extend it over a very long distance. It's very common to use fiber optic cables to connect sites that are very far apart. And since there's light inside of these cables instead of radio frequencies, it's not subject to interference from things like radio signals or electrical interference.Here's a close-up of a fiber optic connection. The connectors themselves are relatively large. The fiber optic is this smaller strand that's coming out the back of that connector. If we're going over longer distances, we'll even put a coating around that so that there'll be a little bit of a thicker connection so we can go a longer distance without damaging the fiber inside.We often forget how small these fiber optic cables really are. The fiber optics are here in the core of the cable. And then in that smaller strand, you can see that orange cladding that was around the outside. To protect it even further, we'll put that very large coating around the outside as well.These fiber optics are very fragile. And so on the connectors that we use to plug into our components, we usually have this very hard ferrule that's wrapped around the fiber core. It's even difficult to see the fiber core in this picture. I'll get rid of my highlighting so that we can point directly to the center. You can see the little bit of a difference in color there in the very center of that ferrule. And that is the core of the fiber optic.For what we call a short-range communication with fiber optics– this is distances that go up to about two kilometers– we generally use multi-mode fiber. It's called multi-mode because when we put the light into the fiber, it tends to bounce around and hit the sides of the fiber and bounce around to the other side. And it can enter the fiber and bounce around in different modes.You can see three different light sources here. And you can see they're bouncing a little bit differently in those multiple modes within the fiber. We usually have an inexpensive light source, like LEDs. And by using multi-mode fiber, we can keep the cost down instead of using a more expensive fiber type and a more expensive light source.The more expensive fiber types of light sources are going to go longer distances. So we use single-mode fiber for those connections. Single-mode fiber allows us in some cases to go up to 100 kilometers without having to regenerate the signal and send it on its way. This is usually using a laser as the light source. And that's why it's relatively more expensive than a multi-mode fiber connection. This is a single-mode, so when the light goes into the fiber, we have a single light source going all the way through the connection. There won't be multiple light modes coming into the connector on the other side.Instead of using fiber in many of our home offices and larger organizations, we're using a less expensive form of wiring in the form of twisted pair copper cabling. This twisted pair cabling uses a communication method called balanced pair operation. That means that the two wires that we send in a pair are going to send equal and opposite signals through this connection. That means when the signal is received on the other side, if there's any interference in that connection, that common mode signal can be filtered out and you're left with the original signal that came through the wire.That's a big reason why we twist these cables. That means that with the cables constantly twisting, there's one wire that's always going to be farther away from the point of interference. That way, on the other side, it makes it very easy to compare both of those wires, determine what type of interference might be in that signal, and easily remove it.To also help remove that common mode interference, you'll notice that the different pairs of wires within the same cable are twisted at different rates. So it's this combination of a balanced mode operation, the twist within the individual pairs of cables, and the different twists rates that help us remove all of the interference from that cable once the signal is received on the other side.The vast majority of the copper cabling that you'll see used for Ethernet is unshielded twisted pair, or UTP. This unshielded twisted pair doesn't have any additional shielding between those wires in the outside world. So if there is anything creating interference, it isn't stopped by anything inside of that cable itself.For environments that have a lot of electrical interference, you may want to consider using STP, or shielded twisted pair. This is exactly the same type of wiring inside of the cable, but there's additional shielding that's wrapped around those wires to help protect from that interference. It's very common to see STP being used in environments where you're in a factory or environment where there's a lot of radio interference. That way, you can help protect the signal that's inside of that cable. Another feature in an STP cable that is different than the UTP is this ground cable. That way, you're able to keep the same ground across that very long distance on both sides of those connectors.Not all twisted pair cables are created the same. So we've created a set of standards that we call cable categories that help describe how a cable is manufactured. On our list, we have a Category 3 cable. This was one of the earlier types of Ethernet cables that helped support 10BASE-T and allowed us to run that 10BASE-T to 100 meters.Another type of cable that we don't see any longer is the Category 5. This was used for 100BASE-TX and 1000BASE-T. And we generally see that also extending out and allowing us to run 100 meters for those topologies. We no longer see Category 3 or Category 5. Those category types are now deprecated. We tend to see Category 5e and higher these days.Category 5e stands for enhanced. This allows us to run now 100BASE-TX and 1000BASE-T to 100 meters. The Category 5e was created because this 1000BASE-T, this gigabit connection, was extending 100 meters but there were certain situations where the signal was not as strong as we would have liked. So we created the Category 5e as an enhancement to improve this 1000BASE-T distance so that we could really get 100 meters out of it in the largest number of environments.When 10 gigabit Ethernet over copper cabling was introduced, we needed a new category of cabling. So we create Category 6. Category 6 cabling could support 10GBASE-T on distances from 37 to 55 meters maximum. We also created Category 6A. A stands for augmented. This improved on this standard. We could still used this 10GBASE-T connection but we were now able to run it a maximum of 100 meters.Another category of cable that you may see is Category 7. And I put an asterisk next to this so that you can see that it's not a standard from the EIA/TIA. It's just one that we happen to be using because the industry has just chosen the next number in the list. This is a shielded version of Category 6. And it's still allowing 10GBASE-T over 100 meters. But with that shielding, we're able to use it in environments where there's a lot of radio interference.In many commercial buildings, there's actually a space between the ceiling, which is usually a drop ceiling, and the actual ceiling of the building. And inside of that space, you can have a number of different things. There can be pipes, there can be air supplies, and there can be network cabling.If your air system isn't using that section above your ceiling as an air space but instead has its own duct work, then you don't have to worry about having a certain type of cabling up there because there is no plenum where you're pulling air from a shared area above the ceiling. Instead, you have your own ductwork providing air to the floor and your own ductwork that is bringing the air back to the air conditioning system.Some environments may not use duct space for sending or receiving the air to the HVAC. Instead, the air may be provided through ductwork, but the return air may be using the shared area, or the plenum, that's above the drop ceiling. It's the shared plenum where we are more concerned about our network cables that may be in this space. That's because if there's a fire, all of the smoke and chemicals that are on our network cables are going to get into the air space. So we have to think about exactly what type of cables we're going to use in the plenum.Fortunately, there's a type of twisted pair cabling that is designed to be used in the plenum. This uses a flourinated ethylene polymer with a low-smoke PVC, this polyvinyl chloride. This means that we're able to use this cable. And if there is a fire, it's going to have a minimal amount of smoke when you compare it to the other types of twisted pair cabling.This cable, however, may not be as flexible. It's not going to have the same bend radius because it's a different type of jacket on the outside of the cable. But you have to think about this, especially when you're considering the worst-case scenario of a fire and making sure that everyone can get out of the building safely.Another popular copper networking cable is a coaxial cable. Coaxial cable has a single access, or single wire conductor than is shared between two devices. So unlike twisted pair where there are multiple pairs of wires inside of that cable, in the case of coax, there is a single wire conductor.The type of coax cable that we often see– the cable company used into our building– is RG-6. It's used for television and digital cable. And it's commonly used to send that internet connection over that coax, as well. Inside of our buildings, we tend to use RG-59. It's a type of coax cable that's specifically designed for smaller runs of patches inside of our building. We commonly don't see RG-59 being used over longer distances. 75%(4)75% found this document useful (4 votes)2K views57 pagesThis document discusses identity and access management. It covers implementing identity and access management, configuring directory services and access services, and managing accounts. It a…AI-enhanced title and descriptionSaveSave Professor Messer Comptia 220 901 902 a Plus Course... For Later75%75% found this document useful, undefined75%(4)75% found this document useful (4 votes)2K views57 pagesThis document discusses identity and access management. It covers implementing identity and access management, configuring directory services and access services, and managing accounts. It also discusses identity and access management products that are used to identify, authenticate and authorize. It describes several access control models including mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC) and rule-based access control. Physical access control devices like smart cards and biometric devices are also covered. Common directory services, LDAP, and remote access protocols are summarized.75%(4)75% found this document useful (4 votes)2K views57 pagesThis document discusses identity and access management. It covers implementing identity and access management, configuring directory services and access services, and managing accounts. It a…AI-enhanced title and description Ask the publishers to restore access to 500,000+ books. Image not available forColor: To view this video download Flash Player We use many different connectors in our modern networks. In this video, you'll learn about fiber connectors, twisted pair connectors and standards, and common coax network connectors.>-There are three different kinds of fiber connectors that you'll need to know for your A+ certification. The ST, the SC, and the LC.The ST connector is the straight tip connector. It's one that's been around for quite some time. You can see the straight tip on the end of the fiber connectors. And they have this bayonet connection, which means that you push them into the connector, and you twist them to lock them in place. That way, it's very difficult for that fiber connection to fall out, or to be accidentally pulled out of that fiber connection.The SC connector is the subscriber connector. You might also hear it referred to as the standard connector. And some people call it the square connector because the end of it is this square. You also notice there's no bayonet connector on the SCs, but they do lock into place when you push them into the connector. You pull on them slightly, and they unlock, and are then released from the connection.LC stands for the Lucent connector. This might also be called the local connector and most commonly, the little connector because it's much smaller than the ST or the LC connectors. And when you're dealing with large amounts of interfaces on networks switches and other devices, it's good to use the smallest connectors you can, so that you can fit more into that same component.Here is the relative size of all of these connectors. You can see the connectors are here, with dust covers over the fiber connections. You got the ST connector on the right side, the SC connector on the left side, and the LC right in the middle.Let's shift gears to our copper connections. One of the more common copper connections, especially on modem connections is the RJ11 connector. This is a 6 position, 2 conductor connector. That Means there are six positions inside of this, but we're really only using two of those. You can even see the two conductors inside of this RJ11 connector.It's very commonly used for telephone connections. In fact, there's a variant of this that's the RJ14, that still uses the six positions, it fits into exactly the same interface type, but there are four different conductors inside. You'll very often see this used for dual-line configurations, so that you can use two phone line through the same cable.For our ethernet connections, we're using RJ45 connectors. This is an 8 position, 8 conductor cable. And you can see we're using all eight of those copper connections inside of this. If you're running a WAN connection, a T1, or some other type of WAN connectivity, it's using a similar connection, but it's really an RJ48C. It's in 8 position, 4 conductor cable, but they look very similar to each other.Whenever you're installing fiber or copper cable into an environment, you want to be sure it's done exactly the specification. You don't want one end of the wire configured in one way, and the other end configured in another. And very often you want to test these wires prior to going into production. This is one where all the connectors look very similar, you can wire them in similar ways. So it's good to have a mapping device like this that's able to see exactly what the wiring is inside of those cables.You might also consider getting a good cable person. Someone who is accustomed to installing this physical plant. Your network is all going to rely on how well this physical installation is. It's very often a good thing to bring in an expert who's doing this all the time.One set of standards for twisted-pair cabling is the T568A and the T568B standards. These are standards from the Telecommunications Industry Association, and it's really designed so that everybody's using exactly the same wiring type. These pin assignments come from the EIA/TIA-568-B standard. And they're are specific to 8 conductor ethernet cables there are 100 ohms in resistance.You'll find that the A and the B configurations are a bit different. You'll see them listed as the T568A and the T568B. This is really designed for this horizontal cabling that we have between a wiring closet and a computer. But we often see it across all of our ethernet cables.Most organizations are going to use the 568B standard for wiring. But you want to be sure if you're working in a new environment, exactly what type of standard they're following in their organization. You just have to remember that you can't wire one side with the 568A standard and the other side with a 568B standard and expect it to work. Those are two very incompatible types. You want to be sure you're using exactly the same standard on both sides.Here's the color schemes for the standards themselves. The 568A is on the left side and the 568B on the right side. And they're numbered 1 through 8. These are the pins that we use on the end of the RJ45 cable. You can see they're very similar, especially pins 4 and 5, and 7 and 8, or exactly the same between the two standards.Where they differentiate is between pins 1, 2, 3, and 6. You can see that they are white and green and green in the A standard for pins 1 and 2, and orange and white and orange on pins 1 and 2 on the B standard. So those pins 1, 2, 3, and 6 are simply switched with the colors, depending on what standards you're looking at.Another common copper cabling type is the BNC connector. The B stands for the bayonet, which is this twisted connector at the end that you push in and you twist to lock in place. The NC stands for Paul Neill and Carl Concelman, who came up with this standard for the BNC connector.For networking we very commonly see BNC being used for DS3 WAN links, which are brought in on these coax cables. These are often very rigid and bulky cables to work. You're very often are using now smaller, twisted pair cables or even fiber connections, instead. Another very popular connector a networkink– especially on cable modem connections– is the F-connector. We often see this being used with cable television in sending video signals through connection. But because you have so many cable companies now providing internet access, we are sending our internet connections over these RG-6 cables and these threaded F-connectors. Professor Messer's CompTIA 220-901 and220-902 A+ Training CourseThis is the index to my free CompTIA 220-901 and 220-902 A+ training course videos. All of my training videos are completely free; all of the videos online right now!143 Videos – Total Running Time: 17 hours 26 minutesWho is Professor Messer? Are all of these videos really free? Read our frequently asked questions here.Have you downloaded the exam objectives yet? Click here to get them now.CompTIA 220-901 A+ Training VideosSection 0: An Overview of the A+ Certification Section 1: Hardware Section 2: Networking Section 3: Mobile Devices Section 4: Hardware and Network Troubleshooting CompTIA 220-902 A+ Training VideosSection 1: Windows Operating Systems Section 2: Other Operating Systems and Technologies Section 3: Security Section 4: Software Troubleshooting Section 5: Operational Procedures Additional Study: Professor Messer's A+ Study GroupsA+ Study Group Replays This is an overview video for Professor Messer's Free CompTIA A+ Certification Training Course, the industry's first free video-based training for the CompTIA A+ certification. In this introductory module, you'll learn about Professor Messer, the format of the training course, and our goal for building a community of A+ certified professionals. You'll also learn about the history of CompTIA, the advantages of an A+ certification, the exam categories, and best practices to use when taking the CompTIA A+ certification exam at your testing center. 1 2 Professor Messer's CompTIA 220-1102 Core 2 A+ Course Notes James "Professor" Messer 3 Professor Messer's CompTIA 220-1102 Core 2 A+ Course Notes Written by James "Professor" Messer Copyright © 2022 by Messer Studios, LLC All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher. First Edition: March 2022 This is version 1.2 Trademark Acknowledgments All product names and trademarks are the property of their respective owners, and are in no way associated or affiliated with Messer Studios LLC. "Professor Messer" is a registered trademark of Messer Studios LLC. "CompTIA" and "A+" are registered trademarks of CompTIA, Inc. Warning and Disclaimer This book is designed to provide information about the CompTIA 220-1102 A+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book. 4 Contents 1.0 - Operating Systems 1.1 - An Overview of Windows 1.1 - Windows Upgrades 1.2 - Windows Command Line Tools 1.2 - The Windows Network Command Line 1.3 - Task Manager 1.3 - The Microsoft Management Console 1.3 - Additional Windows Tools 1.4 - The Windows Control Panel 1.5 - Windows Settings 1.6 - Windows Network Technologies 1.6 - Configuring Windows Firewall 1.6 - Windows IP Address Configuration 1.6 - Windows Network Connections 1.7 - Installing Applications 1.8 - Operating System Overview 1.9 - Installing Operating Systems 1.9 - Upgrading Windows 1.10 - macOS Overview 1.10 - macos System Preferences 1.10 - macos Features 1.11 - Linux Commands 1.11 - Linux Features 2.0 - Security 2.1 - Physical Security 2.1 - Physical Security for Staff 2.1 - Logical Security 2.1 - Active Directory 2.2 - Wireless Encryption 2.2 - Authentication Methods 2.3 - Malware 2.3 - Anti-Malware Tools 2.4 - Social Engineering 2.4 - Denial of Service 2.4 - Zero-Day Attacks 2.4 - On-Path Attacks 2.4 - Password Attacks 2.4 - Insider Threats 2.4 - SQL Injection 2.4 - Cross-site Scripting 2.4 - Security Vulnerabilities 1 1 2 3 4 5 5 6 7 8 9 9 10 10 10 12 13 14 15 16 16 17 19 19 19 20 21 22 23 24 24 26 26 28 28 28 29 30 30 30 31 5 2.5 - Defender Antivirus 2.5 - Windows Firewall 2.5 - Windows Security Settings 2.6 - Security Best Practices 2.7 - Mobile Device Security 2.8 - Data Destruction 2.9 - Securing a SOHO Network 2.10 - Browser Security 31 32 32 33 34 35 36 37 3.0 - Software Troubleshooting 38 4.0 - Operational Procedures 45 3.1 - Troubleshooting Windows 3.1 - Troubleshooting Solutions 3.2 - Troubleshooting Security Issues 3.3 - Removing Malware 3.4 - Troubleshooting Mobile Devices 3.5 - Troubleshooting Mobile Device Security 4.1 - Ticketing Systems 4.1 - Asset Management 4.1 - Document Types 4.2 - Change Management 4.3 - Managing Backups 4.4 - Managing Electrostatic Discharge 4.4 - Safety Procedures 4.5 - Environmental Impacts 4.6 - Privacy, Licensing, and Policies 4.7 - Communication 4.7 - Professionalism 4.8 - Scripting Languages 4.8 - Scripting Use Cases 4.9 - Remote Access 38 40 41 42 43 44 45 46 46 47 48 50 50 51 51 53 53 54 55 56 6 Introduction The CompTIA A+ certification requires a broad set of knowledge, and it covers more topics than many industry certifications. It's no surprise that the A+ certification has become one of the most sought-after industry certifications by both aspiring technologists and employers. I hope this book helps you with your "last mile" of studies before taking your exam. There's a lot to remember, and perhaps some of the information in this book will help jog your memory while you're sitting in the exam room. Best of luck with your studies! - Professor Messer The CompTIA A+ Certification CompTIA's A+ certification is considered to be the starting point for information technology professionals. Earning the A+ certification requires the completion of two exams and covers a broad range of technology topics. After completing the CompTIA A+ certification, an A+ certified professional will have an understanding of computer hardware, mobile devices, networking, operating systems, security techniques, and much more. The current series of the A+ certification is based on the successful completion of the 220-1101 and the 220-1102 exams. You must pass both exams to earn your CompTIA A+ certification. This book provides a set of notes for the 220-1102 Core 2 exam. The 220-1102 Core 2 exam The 220-1102 exam objectives are focused on operating systems, with over half of the exam detailing operating systems and the troubleshooting of software. Here's the breakdown of the four 220-1102 exam domains: Domain 1.0 - Operating Systems - 31% Domain 2.0 - Security - 25% Domain 3.0 - Software Troubleshooting - 22% Domain 4.0 - Operational Procedures - 22% Study Tips Exam Preparation • Download the exam objectives, and use them as a master checklist: • Use as many training materials as possible. Books, videos, and Q&A guides can all provide a different perspective of the same information. • It's useful to have as much hands-on as possible, especially with network troubleshooting and operating system command prompts. Taking the Exam • Use your time wisely. You've got 90 minutes to get through everything. • Choose your exam location carefully. Some sites are better than others. • Get there early. Don't stress the journey. • Manage your time wisely. You've got 90 minutes to get through everything. • Wrong answers aren't counted against you. Don't leave any blanks! • Mark difficult questions and come back later. You can answer the questions in any order. 7 8 Professor Messer's CompTIA A+ 220-1102 Course Notes 1.1 - An Overview of Windows Windows on the Core 2 exam • 220-1102 exam released in January 2022 – Two Windows versions available – Windows 10 and Windows 11 • CompTIA considers all in-support Windows versions to be in scope for the exam – Mainstream support is 5 years after release • Windows versions are listed in the objectives – Everything else includes both Windows 10 and 11 • Fortunately, these are remarkably similar – Once you know one, you effectively know the other! Windows 10 • Released on July 29, 2015 - We skipped Windows 9 • A single platform – Desktops, laptops, tablets, phones, all-in-one devices • Ongoing updates – More than twelve different released versions – November 2021 (Version 21H2) Windows 10 Home • Home user - Retail sales • Integration with Microsoft account – Microsoft OneDrive backup • Windows Defender – Anti-virus and anti-malware • Cortana - Talk to your operating system Windows 10 Pro • The business version of Windows – Additional management features • Remote Desktop host – Remote control each computer • BitLocker - Full disk encryption (FDE) • Join a Windows domain – Group Policy management 1.1 - Windows Features Windows at work • Large-scale support – Thousands of devices • Security concerns – Mobile devices with important data – Local file shares • Working on a spreadsheet – Watching a movie • Geographical sprawl - Cache data between sites © 2022 Messer Studios, LLC Windows 10 Pro for Workstations • An edition for high-end desktops – Enhanced performance and storage options • More physical CPUs - Up to four • High maximum RAM - Supports up to 6 TB • Support for ReFS - Resilient File System – Same as Windows Server Windows 10 Enterprise • Built for large implementations – Volume licensing • AppLocker - Control what applications can run • BranchCache - Remote site file caching • Granular User Experience (UX) control – Define the user environment – Useful for kiosk and workstation customization Domain Services • Active Directory Domain Services – Large database of your network • Distributed architecture – Many servers - Not suitable for home use • Everything documented in one place – User accounts, servers, volumes, printers • Many different uses – Authentication, centralized management Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 1 9 1.1 - Windows Features (continued) Organizing network devices • Windows Workgroups – Logical groups of network devices – Each device is a standalone system, everyone is a peer • Windows Domain – Business network – Centralized authentication and device access – Supports thousands of devices across many networks Desktop styles • Your computer has many different uses – Those change depending on where you are • Work – Standard desktop – Common user interface – Customization very limited – You can work at any computer • Home – Complete flexibility – Background photos, colors, UI sizing – Centralized authentication and device access – Supports thousands of devices across many networks Availability of RDP • Remote Desktop Protocol – View and control the desktop of a remote device • RDP client – Connects to a Remote Desktop Service – Clients available for almost any operating system • Remote Desktop Service – Provides access for the RDP client – Available in Windows 10 Pro and Enteprise – Not available in Windows 10 Home RAM support limitations • RAM support varies between editions – More advanced editions allow additional RAM BitLocker and EFS • Data confidentiality – Encrypt important information • Encrypting File System – Protect individual files and folders – Built-in to the NTFS file system • BitLocker – Full Disk Encryption (FDE) – Everything on the drive is encrypted – Even the operating system • Home and business use – Especially on mobile devices Group Policy editor • Centrally manage users and systems – Policies can be part of Active Directory or a local system • Local Group Policy – Manages the local device – gpedit.msc • Group Policy Management Console – Integrated with Active Directory – Powerful system management – gpmc.msc 1.1 - Windows Upgrades Why upgrade? • Upgrade vs. Install – Upgrade - Keep files in place – Install - Start over completely fresh • Maintain consistency – Customized configurations – Multiple local user accounts • Upgrades save hours of time – Avoid application reinstall – Keep user data intact – Get up and running quickly Upgrade methods • In-place – Upgrade the existing OS – Keeps all applications, documentations, and settings – Start the setup from inside the existing OS © 2022 Messer Studios, LLC • Clean install – Wipe everything and reload – Backup your files – Start the setup by booting from the installation media Upgrading Windows • Upgrade from the Windows installation media – Downloadable versions are available from Microsoft – Includes a media creation tool • You cannot upgrade x86 to x64 – Or x64 to x86 – Applies to all Windows versions – You'll have to migrate instead Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 2 10 1.1 - Windows Upgrades (continued) Upgrade paths • Many upgrades are between similar editions – Or higher-level Windows editions • In-place upgrade paths to Windows 10 – Windows 7, Windows 8.1 (not Windows 8.0) • In-place upgrade paths to Windows 11 – Windows 10 Post-installation • Does it work? – If it doesn't boot, there are bigger problems • Some testing is useful for unknown hardware configurations – Start > Settings > System > Recovery > Go back • Additional installations – Service packs, security patches, security applications, driver updates, application updates 1.2 - Windows Command Line Tools Privileges • Not all users can run all commands – Some tasks are for the administrator only • Standard privileges – Run applications as normal user – This works fine for many commands • Administrative/elevated privileges – You must be a member of the Administrators group – Right-click Command Prompt, choose Run as Administrator – cmd, Ctrl+Shift+Enter Command line troubleshooting • Use "help" if you're not sure > help dir > help chkdsk • Also use: [command] /? – Close the prompt with exit File management • dir – List files and directories • cd / chdir – Change working directory – Use backslash \ to specify volume or folder name • .. – Two dots/periods – The folder above the current folder • md / mkdir – Make a directory • rd / rmdir – Remove directory Drive letters • Each partitions is assigned a letter – Primary storage drive is usually C • Reference the drive with the letter and a colon – C: • Combine with the folder – Folder names are separated with backslashes – C:\Users\professor © 2022 Messer Studios, LLC hostname • View the name of the device – This is very useful when there are 10 different terminal screen tabs in use • This is the Windows Device name – Name can be changed in the System settings format • Formats a disk for use with Windows • format c: copy (/v, /y) • Copy files from one location to another /v - Verifies that new files are written correctly /y - Suppresses prompting to confirm you want to overwrite an existing destination file xcopy • Copies files and directory trees xcopy /s Documents m:\backups Robust Copy • robocopy – A better Xcopy – Included with Windows 10 and 11 Managing Group Policy • Group Policy – Manage computers in an Active Directory Domain – Group Policy is usually updated at login • gpupdate – Force a Group Policy update – gpupdate /target:{computer|user} / force – gpupdate /target:professor /force • gpresult – Verify policy settings for a computer or user – gpresult /r – gpresult /user sgc/professor /v Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 3 11 1.2 - Windows Command Line Tools (continued) shutdown • Shutdown a computer – And optionally restart • shutdown /s /t nn – Wait nn seconds, then shutdown • shutdown /r /t nn – Shutdown and restart after nn seconds • shutdown /a – Abort the countdown! sfc • System File Checker – Scan integrity of all protected system files • sfc /scannow Check Disk • chkdsk /f – Fixes logical file system errors on the disk • chkdsk /r – Locates bad sectors and recovers readable information – Implies /f • If volume is locked, run during startup DiskPart • Manage disk configurations – diskpart - start the DiskPart command interpreter winver • View the About Windows dialog – A quick check • Useful when troubleshooting – Are you running the latest version? 1.2 - The Windows Network Command Line ipconfig • Most of your troubleshooting starts with your IP address – Ping your local router/gateway • Determine TCP/IP and network adapter information – And some additional IP details • View additional configuration details – DNS servers, DHCP server, etc. ping • Test reachability – Determine round-trip time – Uses Internet Control Message Protocol (ICMP) • One of your primary troubleshooting tools – Can you ping the host? netstat • Network statistics – Many different operating systems • netstat -a – Show all active connections • netstat -b – Show binaries (Windows) • netstat -n – Do not resolve names nslookup • Lookup information from DNS servers – Canonical names, IP addresses, cache timers, etc. • Lookup names and IP addresses – Many different options © 2022 Messer Studios, LLC net • Windows network commands • View network resources – net view \\ – net view /workgroup: • Map a network share to a drive letter – net use h: \\\ • View user account information and reset passwords – net user – net user * /domain tracert • Determine the route a packet takes to a destination – Map the entire path • Takes advantage of ICMP Time to Live Exceeded message – The time in TTL refers to hops, not seconds or minutes – TTL=1 is the first router, TTL=2 is the second router, etc. • Not all devices will reply with ICMP Time Exceeded – Some firewalls filter ICMP – ICMP is low-priority for many devices Flavors of traceroute • Not all traceroutes are the same – Minor differences in the transmitted payload • Windows commonly sends ICMP echo requests – Receives ICMP time exceeded messages – And an ICMP echo reply from the final/destination device – Unfortunately, outgoing ICMP is commonly filtered Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 4 12 1.2 - Windows in the Enterprise (continued) • Some operating systems allow you to specify the protocol Linux, Unix, macOS, etc. • IOS devices send UDP datagrams over port 33434 – The port number can be changed with extended options – The mechanics of traceroute pathping • Combine ping and traceroute – Included with Windows NT and later • First phase runs a traceroute – Build a map • Second phase – Measure round trip time and packet loss at each hop 1.3 - Task Manager Task Manager • Real-time system statistics – CPU, memory, disk access, etc. • Starting the Task Manager – Ctrl-Alt-Del, select Task Manager – Right mouse click the taskbar and select Task Manager – Ctrl-Shift-Esc Processes • View all running processes – Interactive and system tray apps – View processes from other accounts • Manage the view – Move columns, add metrics • Combine all apps, processes, and services into a single tab – Easy to view and sort Performance • What's happening? - CPU, memory, etc. • Statistical views - Historical, real-time • Newer versions include CPU, memory, disk, Bluetooth, and network in the Performance tab Networking • Network performance – Integrated into the Performance tab • View utilization, link speeds, and interface connection state Users • Who is connected? What are they doing? • Other options – Disconnect a user, manage user accounts Services • Non-interactive applications – Hundreds of background processes • Manage from one screen – Start, stop, restart Startup • Manage which programs start with a Windows login – Easily toggle on and off • Multiple reboots – Enable and disable – You'll find it 1.3 - The Microsoft Management Console Task Manager • Build your own console – mmc.exe • A handy starting point – Event Viewer – Local Users and Groups – Disk management – Task Scheduler – And more! Event Viewer • Central event consolidation – What happened? • Application, Security, Setup, System • Information, Warning, Error, Critical, Successful Audit, Failure Audit • eventvwr.msc © 2022 Messer Studios, LLC Disk Management • Manage disk operations – Individual computers and file servers • diskmgmt.msc • WARNING – YOU CAN ERASE DATA – ALWAYS HAVE A BACKUP Task Scheduler • Schedule an application or script – Plan your future • Includes predefined schedules – Click and go • Organize – Manage with folders • taskschd.msc Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 5 13 1.3 - The Microsoft Management Console (continued) Device Manager • The OS doesn't know how to talk directly to most hardware • Device drivers are hardware specific and operating system specific – Older device drivers may not necessarily work in Windows 10 or 11 • devmgmt.msc Certificate Manager • View user and trusted certs – Add and remove • certmgr.msc Local users and groups • Users – Administrator - the Windows super-user – Guest -Limited access – "Regular" Users • Groups – Administrators, Users, Backup Operators, Power Users, etc. • lusrmgr.msc Performance Monitor • Gather long-term statistics – perfmon.msc • OS metrics – Disk, memory, CPU, etc. • Set alerts and automated actions – Monitor and act • Store statistics – Analyze long-term trends • Built-in reports – View the data Group Policy Editor • Centrally manage users and systems – Policies can be part of Active Directory or a local system • Local Group Policy Editor – Manages the local device – gpedit.msc • Group Policy Management Console – Integrated with Active Directory – Powerful system management – gpmc.msc 1.3 - Additional Windows Tools System Information • System overview – msinfo32.exe • Hardware Resources – Memory, DMA, IRQs, conflicts • Components – Multimedia, display, input, network • Software Environment – Drivers, print jobs, running tasks Resource Monitor • Detailed real-time view of performance – Separated by category • Categories – Overview, CPU, Memory, – Disk, and Network • resmon.exe System Configuration • Manage boot processes, startup, services, etc. – One-stop shop • msconfig.exe Disk Cleanup • Find unused or unneeded files – A quick way to free up space • Select the categories – Click the button • cleanmgr.exe © 2022 Messer Studios, LLC defrag • Disk defragmentation – Moves file fragments so they are contiguous – Improves read and write time • Not necessary for solid state drives – Windows won't defrag an SSD • Graphical version in the drive properties • Requires elevated permissions – Command line: – defrag – defrag C: regedit.exe • The Windows Registry Editor – The big huge master database – Hierarchical structure • Used by almost everything – Kernel, Device drivers – Services – Security Account Manager (SAM) – User Interface, Applications • Backup your registry! – Built into regedit Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 6 14 1.4 - The Windows Control Panel Internet Options • General - Basic display • Security - Different access based on site location • Privacy - Cookies, pop-up blocker, InPrivate browsing • Content - Certificates and auto-complete • Connections - VPN and proxy settings • Programs - Default browser, plugins, etc. • Advanced - Detailed configuration options (and reset!) Devices and Printers • Everything on the network – Desktops, laptops, printers, multimedia devices, storage • Quick and easy access – Much less complex than Device Manager – Properties, device configurations Programs and Features • Installed applications - Uninstall, size, version • Windows features - Enable and disable Network and Sharing Center • All network adapters - Wired, wireless, etc. • All network configs – Adapter settings, network addressing System • Computer information - Including version and edition • Performance - Virtual memory • Remote settings • System protection Windows Defender Firewall • Protect from attacks - Scans, malicious software • Integrated into the operating system • Control Panel > Windows Firewall Mail • Icon does not appear unless a mail client, e.g., Outlook, is installed – Otherwise not an option • Access to local mail configuration – Account information, data files Sound • Output options - Multiple sound devices may be available • Set levels for output and input – Speakers and microphone User Accounts • Local user accounts – Domains accounts are stored elsewhere • Account name and type • Change password • Change picture • Certificate information © 2022 Messer Studios, LLC Device Manager • The OS doesn't know how to talk directly to most hardware - You need drivers • Manage devices - Add, remove, disable • First place to go when hardware isn't working – Instant feedback Indexing Options • Speed up the search process – Constantly updates an index • Searches browser history and user folders – Good default options • Add other locations – Modify to include other folders File Explorer Options • Manage Windows Explorer - Many options • General - Windows, expand folders • View - View hidden files, hide extensions • Search – Disable index searches, search non-indexed areas Administrative Tools • Not commonly used utilities – Used for system administration • Useful system tools – Often used options for system administrators and technicians Power Options • Hibernate – Open docs and apps are saved to disk – Common on laptops - Used by Fast Startup • Power plans – Customize power usage • Sleep (standby) – Open apps are stored in memory – Save power, startup quickly – Switches to hibernate if power is low • Choose what closing the lid does – Useful for docking stations • USB selective suspend – Disable individual USB devices – Save power – Fingerprint readers, biometrics • Fast startup – Enable or disable - Useful for troubleshooting Ease of Access Center • Usability enhancements - Useful for everyone • Change display, keyboard, mouse, and other input/output options – Use Windows without a display – Change the mouse pointers Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 7 15 1.5 - Windows Settings Settings • An updated interface – A migration from the Control Panel • One place for most configuration settings – A common UI • Search for "Settings", Or scroll down to "S" Time and Language • Windows can automatically set the time – Active Domain is very sensitive to synchronized clocks – Five minutes of tolerance by default • Windows can speak many different languages – Change or add a language Update and Security • Keep your OS up to date - Security patches, bug fixes • Automatic installation - Updates are always installed • Active hours - You control the update time Personalization • Change the way Windows looks and feels – Colors, wallpaper, lock screen • Extensive customization - Make Windows your own Apps • Manage installed applications – Uninstall or modify an existing app • Add Windows features – Fonts for other languages – OpenSSH Server – SNMP support Privacy • Share app activity - Customized advertising • Share your language - Website content • Speech recognition - Sends audio to an online service © 2022 Messer Studios, LLC System • Change display settings – Night light, scaling, resolution • Audio settings – Input and output • Notifications – Enable/disable – Show on lock screen Devices • Manage devices – Bluetooth, printers, etc. • Mouse settings – Button and wheel options • Typing and writing – Keyboard and pen Network and Internet • Network settings – Internet connectivity • View Internet status – Up or down? • Change IP settings – Modify address information Gaming • Xbox Game Bar - Xbox gaming network • Chat, join games - Look for friends Accounts • Manage login account information – Microsoft account or local account • Email configuration - Specify an email app • Sign-in options - PIN, password, security key, etc. Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 8 16 1.6 - Windows Network Technologies Shared resources • Make a folder or printer available on the network – "Share" with others, view in Windows Explorer • Assign (map) a drive letter to a share – Access a file server – Reconnect automatically • Shares ending with a dollar sign ($) are "hidden" – Not a security feature • Administrative Tools > Computer Management Mapping drives • Access a share – This PC / Map network drive • Local drive letter and share name – May require additional authentication • Or use the command line: net use h: "\\Daedalus\Gate Room" Sharing printers • Similar to sharing a folder – But it's a printer instead • Printer Properties – Access through Windows Explorer, the Settings app, or any other Printer Properties – Share an existing printer Using a shared printer • Similar to sharing a folder – But it's a printer instead • Add a printer – Windows Explorer – Settings app Proxy Settings • Change the traffic flow – An Internet go-between • Settings > Network and Internet – Or use Control Panel > Internet Options > Connections > LAN settings • Define address and exceptions – Proxies don't work for everything Network locations • Private – Share and connect to devices – Home or work network • Public – No sharing or connectivity – Public Wi-Fi • Customize security settings – Profile is determined automatically – Change the settings at any time Network paths • View network paths in File Explorer – Server and share name • Map network drive – Add a drive letter • Disconnect – Toolbar - Right-click the drive Metered connections • Reduce data usage – Slow network links – Limited bandwidth – Usage-based billing • Can modify application communication – Windows Updates – OneDrive sync 1.6 - Configuring Windows Firewall Windows Defender Firewall • Your firewall should always be enabled – Sometimes you need to troubleshoot • Temporarily disable from the main screen – Turn Windows Firewall on or off – Requires elevated permissions • Different settings for each network type – Public / Private Windows Firewall configuration • Block all incoming connections – Ignores your exception list – Useful when you need the most security • Modify notification – App blocking © 2022 Messer Studios, LLC Creating a firewall exception • Allow an app or feature through Windows Firewall – The more secure exception • Port number –

Messer Studios, LLC Prepare the boot drive • Know your drive – Is data on the drive? – Has the drive been formatted? – What partitions are on the drive? • Backup any old data – You may need that data again someday – Save user preferences • Most partitioning and formatting can be completed during the installation – Clear the drive and start fresh Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 14 22 1.9 - Upgrading Windows (continued) Before the installation • Check minimum OS requirements – Memory, disk space, etc. – And the recommended requirements • Run a hardware compatibility check – Runs when you perform an upgrade – Run manually from the Windows setup screen – Windows 10 Upgrade Checker, PC Health Check for Windows 11 • Plan for installation questions – Drive/partition configuration, license keys, etc. • Application and driver compatibility – Check with the app developer and hardware manufacturer Windows product life cycle • Quality updates – Monthly security updates and bug fixes • Feature updates – Annual update with new features – Used to occur every three to five years • Support is provided after the release – 18 to 36 months – Dependent on the Windows version and edition • Also called the Modern Lifecycle Policy – For continuously supported products 1.10 - macOS Overview File types • .dmg – Apple Disk Image – Mountable as a drive in Finder • .pkg – Installer Package – Used to distribute software – Runs through an installer script • .app – Application bundle – Contains the necessary files to use the application – "View Package Contents" from the Finder App store • Centralized updates and patches – For both OS and apps • App Store application – The "Updates" option • Automatic updates – Or manual install • Patch management – Install and view previous updates Uninstallation process – Move the .app file to the Trash – The .app package contains all of the application files – Quick and easy • Some applications include a separate uninstall program – Usually included in the Application folder © 2022 Messer Studios, LLC Apple ID and corporate restrictions • Personal Apple products use a personal Apple ID – Associated with personal data and digital purchases • Companies use Managed Apple IDs using Apple Business Manager – Integrate with Active Directory – Connect with an existing – MDM (Mobile Device Manager) – Assign and move apps and digital content to selected users Backups • Time Machine - Included with macOS • Hourly backups - The past 24 hours • Daily backups - The past month • Weekly backups - All previous months • Starts deleting oldest information when disk is full Anti-virus • macOS does not include anti-virus – Or anti-malware • Many 3rd-party options – From the usual companies • An emerging threat – Still doesn't approach Windows – It's all about the number of desktops • Automate your signature updates – New updates every hour / day Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 15 23 1.10 - macos System Preferences System Preferences • The macOS version of the Windows Control Panel – A close comparison • Access to most customization and personalization options – Includes important configuration utilities • A good place to start – It's probably in here Displays • Configure the location of multiple displays – Side by side, top to bottom • Menu bar can be moved to any display – Doesn't have to be the primary • Modify individual display settings – Resolution, brightness, colors Networks • Configure network interfaces - Wired, wireless • IPv4 and IPv6 - Manual and automatic (DHCP) • Detailed network settings - IP, DNS, 802.1X, etc. Printers & Scanners • Add and remove printers and scanners – Configure individual settings • Share printers and scanners – Configure rights and permissions • View status - Ink and toner levels, scanning status Privacy • Limit application access to private data – Location services, photos, calendars • Control access to cameras and microphones – Enable on a per-app basis • Unauthorized apps can't view your private data – Malware, other apps Accessibility • Allow apps to use system input – Keyboard, mouse, audio, video • Scripting and automation – Requires access for input • Limits third-party applications – Can't take over the keyboard Time Machine • Automated backups – Included with macOS • Hourly backups – The past 24 hours • Daily backups – The past month • Weekly backups – All previous months • Starts deleting oldest information when disk is full 1.10 - macos Features Mission Control and Spaces • Quickly view everything that's running – Spread out the desktop into a viewable area – Swipe upwards with three fingers or – Control-Up arrow • Spaces – Multiple desktops – Add Spaces inside of – Mission Control Keychain • Password management – Passwords, notes, certificates, etc. • Integrated into the OS - Keychain Access • Passwords and Secure Notes are encrypted – Login password is the key Spotlight • Find files, apps, images, etc. – Similar to Windows search • Magnifying glass in upper right • Or press Command-Space • Type anything in - See what you find • Define search categories in System Preferences / Spotlight – Enable/disable categories © 2022 Messer Studios, LLC iCloud • Integrates Apple technologies – macOS, iOS • Share across systems – Calendars, photos, documents, contacts, etc. • Backup iOS devices – Never lose data again • Store files in an iCloud drive – Similar to Google Drive, Dropbox – Integrated into the operating systems Gestures • You can do more than just point and click – Extend the capabilities of your trackpad • Use one, two, three fingers – Swipe, pinch, click • Customization – Enable/disable – System Preferences / Trackpad Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 16 24 1.10 - macos Features (continued) Finder • The central OS file manager – Compare with Windows Explorer • File management – Launch, delete, rename, etc. • Integrated access to other devices – File servers – Remote storage – Screen sharing Remote Disc • Use an optical drive from another computer – Has become more important over time – Designed for copying files – Will not work with audio CDs or video DVDs • Set up sharing in System Preferences – Sharing options – Appears in the Finder Dock • Fast access to apps – Quickly launch programs • View running applications – Dot underneath the icon • Keep folders in the dock – Easy access to files • Move to different sides of the screen – Auto-hide or always display 1.11 - Linux Commands Linux commands • The command line - Terminal, XTerm, or similar • Commands are similar in both Linux and macOS – Mac OS derived from BSD (Berkeley Software Distribution) Unix – This section is specific to Linux • Download a Live CD or install a virtual machine – Many pre-made Linux distributions are available – I'm using Ubuntu in a virtual machine • Use the man command for help – An online manual > man grep ls • List directory contents – Similar to the dir command in Windows • Lists files, directories – May support color coding; – Blue is a directory, red is an archive file, etc. • For long output, pipe through more: > ls -l | more (use q or Ctrl-c to exit) © 2022 Messer Studios, LLC Disk Utility • Manage disks and images - Resolve issues • File system utilities - Verify and repair file systems – Modify partition details – Erase disks • Create, convert, and restore images - Manage disk images FileVault • Full Disk Encryption (FDE) for macOS – Decryption uses a local key or iCloud authentication • Proper authentication is required before macOS can start – Data is unavailable to others • Available in System Preferences – Security & Privacy > FileVault Terminal • Command line access to the operating system – Manage the OS without a graphical interface • OS access – Run scripts, manage files – Configure OS and application settings Force Quit • Stop an application from executing – Some applications are badly written • Command-Option-Escape - List application to quit • Hold the option key when right-clicking the app icon in the dock – Choose Force Quit pwd • Print Working Directory – Displays the current working directory path – Useful when changing directories often mv • Move a file – Rename a file • mv SOURCE DEST > mv first.txt second.txt cp • Copy a file – Duplicate files or directories • cp SOURCE DEST > cp first.txt second.txt rm • Remove files or directories – Deletes the files • Does not remove directories by default – Directories must be empty to be removed or must be removed with -r Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 17 25 1.11 - Linux Commands (continued) chmod • Change mode of a file system object – r=read, w=write, x=execute – Can also use octal notation – Set for the file owner (u), the group(g), others(o), or all(a) • chmod mode FILE > chmod 744 script.sh • chmod 744 first.txt – User; read, write execute – Group; read only – Other; read only • chmod a-w first.txt – All users, no writing to first.txt • chmod u+x script.sh – The owner of script.sh can execute the file chown • Change file owner and group – Modify file settings • sudo chown [OWNER:GROUP] file > sudo chown professor script.sh su / sudo • Some command require elevated rights – There are some things normal users can't do • su – Become super user or change to a different user – You continue to be that user until you exit • sudo – Execute a command as the super user or user ID – Only that command executes as the super user apt-get • Advanced Packaging Tool – Handles the management of application packages – Applications and utilities • Install, update, remove > sudo apt-get install wireshark © 2022 Messer Studios, LLC yum • Yellowdog Updater, Modified (yum) - Install, delete, update • Manages RPM packages – Red Hat Package Manager - RPM Package Manager – A Linux distribution will commonly use either yum or apt-get ip • Manage the network interfaces – Enable, disable, configure addresses, manage routes, ARP cache, etc. • ip address – View interface addresses • ip route – View the IP routing table • sudo ip address add 192.168.121.241/24 dev eth0 – Configure the IP address of an interface df • Disk Free - View file systems and free space • df – View number of blocks • df -h – View human-readable sizes grep • Find text in a file - Search through many files at a time grep PATTERN [FILE] > grep failed auth.log find • Find a file by name or extension - Search through any or all directories • Find files with a specific extension > find . -name "*.txt" dig • Lookup information from DNS servers – Canonical names, IP addresses, cache timers, etc. • dig (Domain Information Groper) – Detailed domain information – Add dig to Windows: - cat • Concatenate - Link together in a series • Copy a file/files to the screen cat file1.txt file2.txt • Copy a file/files to another file cat file1.txt file2.txt > both.txt nano • Full-screen text editor - Easy to edit • Included with many Linux distributions - Easy to install • Select, mark, copy/cut, and paste text – Similar features to graphical-based editors Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 18 26 1.11 - Linux Features Backups • Many options – Command line and graphical – May be included with the distribution • tar – Tape Archive – Easy to script into – a backup schedule • rsync – Sync files between storage devices – Instant synchronization or scheduled • Command line tools apt-get, yum • Graphical update managers – Software updater • Patch management – Updates can be scheduled • Software center – The Linux "App Store" Anti-Virus / Anti-malware • Relatively few viruses and malware for Linux – Still important to keep updated • Clam Antivirus – Open source antivirus engine • Same best practice as any other OS – Always update signature database – Always use real-time scanning Shell/Terminal • Command line access to the operating system – Common to manage in Linux • OS maintenance – Run scripts, manage files – Configure OS and application settings Samba • Add SMB (Server Message Block) to Linux – File and print sharing – Active Directory integration • Integrate Linux into a Windows environment – Linux becomes a Windows file server 2.1 - Physical Security Access control vestibule • All doors normally unlocked – Opening one door causes others to lock • All doors normally locked – Unlocking one door prevents others from being unlocked • One door open / other locked – When one is open, the other cannot be unlocked • One at a time, controlled groups – Managed control through an area Badge reader • Magnetic swipe, RFID, or NFC – Many different identification methods • Different applications – Time clocks – Security guard patrols – Door access Video surveillance • CCTV (Closed circuit television) – Can replace physical guards • Camera features are important – Object detection can identify a license plate or person's face • Often many different cameras – Networked together and recorded over time • Motion detection – Radio reflection or passive infrared – Useful in areas not often in use © 2022 Messer Studios, LLC Alarm systems • Circuit-based – Circuit is opened or closed – Door, window, fence – Useful on the perimeter • Motion detection – Identify motion without a camera • Duress – Triggered by a person – The big red button Door locks • Conventional - Lock and key • Deadbolt - Physical bolt • Electronic - Keyless, PIN • Token-based - RFID badge, magnetic swipe card, or key fob • Biometric - Hand, fingers or retina • Multi-factor - Smart card and PIN Equipment locks • Data center hardware is usually managed by different groups – Responsibility lies with the owner • Racks can be installed together – Side-to-side • Enclosed cabinets with locks – Ventilation on front, back, top, and bottom Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 19 27 2.1 - Physical Security (continued) Guards and access lists • Security guard – Physical protection at the reception area of a facility – Validates identification of existing employees – Provides guest access • ID badge – Picture, name, other details – Must be worn at all times • Access list – Physical list of names – Enforced by security guard • Maintains a visitor log Barricades / bollards • Prevent access – There are limits to the prevention • Channel people through a specific access point – And keep out other things – Allow people, prevent cars and trucks • Identify safety concerns – And prevent injuries • Can be used to an extreme – Concrete barriers / bollards – Moats Fences • Build a perimeter – Usually very obvious – May not be what you're looking for • Transparent or opaque – See through the fence (or not) • Robust – Difficult to cut the fence • Prevent climbing – Razor wire – Build it high 2.1 - Physical Security for Staff Key fobs • Small RFID key – Add to physical keychain • Replaces a physical key – Commonly used for door locks – Proximity operation and contactless Smart cards • Certificate-based authentication – Something you have – Usually requires additional factors • Integrated card reader – Built into the laptop • External reader – USB connected Keys • Some doors may not have an electronic lock – Rarely used – Standalone locks – Safe, storage bin, cabinet • Use a key cabinet – Formal check in/check out – Well-defined storage location – Allows for auditing and timestamps © 2022 Messer Studios, LLC Biometrics • Biometric authentication – Usually stores a mathematical representation of your biometric – Your actual fingerprint isn't usually saved • Difficult to change – You can change your password – You can't change your fingerprint • Used in very specific situations – Not foolproof Biometric factors • Retina scanner – Unique capillary structure in the back of the eye • Fingerprint scanner - Phones, laptops, door access • Palmprint scanner - Shape of the hand and fingers Lighting • More light means more security – Attackers avoid the light – Easier to see when lit – Non IR cameras can see better • Specialized design – Consider overall light levels – Lighting angles may be important – Facial recognition – Avoid shadows and glare Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 20 28 2.1 - Physical Security for Staff (continued) Magnetometers • Passive scanning - Detect metal objects • Not useful for non-metal objectives – Won't identify ceramic or plastic Mobile Device Management (MDM) • Manage company-owned and user-owned mobile devices – BYOD - Bring Your Own Device • Centralized management of the mobile devices – Specialized functionality • Set policies on apps, data, camera, etc. – Control the remote device – The entire device or a "partition" • Manage access control – Force screen locks and PINs on these single user devices 2.1 - Logical Security Least privilege • Rights and permissions should be set to the bare minimum – You only get exactly what's needed to complete your objective • All user accounts must be limited – Applications should run with minimal privileges • Don't allow users to run with administrative privileges – Limits the scope of malicious behavior Access Control Lists (ACLs) • Used to allow or deny traffic – Also used for NAT, QoS, etc. – Commonly used on the ingress or egress of a router interface • ACLs evaluate on certain criteria – Source IP, Destination IP, – TCP port numbers, UDP port numbers, ICMP • Deny or permit – What happens when an ACL matches the traffic? • Also used in operating systems – Allow or deny access to the filesystem Multi-factor authentication • More than one factor – Something you are, something you have, something you know, somewhere you are, something you do • Can be expensive – Separate hardware tokens Software tokens • Authenticator application – Pseudo-random number generator – Can't guess it – Changes constantly © 2022 Messer Studios, LLC • Saves money – Free smartphone applications – No separate device to lose Short message service (SMS) • Text messaging – Includes more than text these days • Login factor can be sent via SMS to a predefined phone number – Provide username and password – Phone receives an SMS – Input the SMS code into the login form • Security issues exist – Phone number can be reassigned to a different phone – SMS messages can be intercepted – SMS spoofing Voice call • A phone call provides the token – The computer is talking to you – "Your code is 1-6-2-5-1-7." • Similar disadvantages to SMS – Phone call can be intercepted or forwarded – Phone number can be added to another phone Email filtering • Unsolicited email – Stop it at the gateway before it reaches the user – On-site or cloud-based • Scan and block malicious software – Executables, known vulnerabilities – Phishing attempts – Other unwanted content Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 21 29 2.1 - Active Directory Active Directory Home folder • A database of everything on the network • Assign a user Home folder to a network folder – Computers, user accounts, file shares, – Manage and backup files from the network printers, groups, and more – Avoid storing files on the local computer • Manage authentication • When added to the user profile, the directories – Users login using their AD credentials are automatically created – And proper permissions are assigned • Centralized access control – Determine which users can access resources • Requires some training – Encourage users to store files on the • Commonly used by the help desk network Home folder – Reset passwords – Add and remove accounts Folder redirection • Some users and applications use the Domain Windows Library folders • The name associated with this related – Desktop, Downloads, group of users, computers, and resources – Music, Documents, etc. – Each domain has a name • Redirect the folders to a network share • Domain controllers store this central domain database – Group Policy > User Configuration > – Active Directory is the service that – Windows settings > Folder Redirection manages this directory • This is often paired with the Offline Files feature • Often referenced when troubleshooting – You're not always connected – Is this computer on the domain? – Can you reset the domain password? Security groups • Create a group Organizational units (OU) – Assign permissions to the group • Keep the (very large) database organized – Users, Computers • Set the rights and permissions to the group – Add users to the group • Create your own hierarchy – Countries, states, buildings, departments, etc. • Some built-in groups – Users, guests • Apply policies to an OU – Remote management users – Can be very large: – Event Log Readers – Domain Users – Can be for a specific group: • Save time – Marketing, North America, – Avoid confusion and mistakes – Pegasus galaxy Login script • Automate a series of tasks during login – Assign a script to a specific user, group, or OU Group Policy and login scripts • Associate the script with a Group Policy – User Configuration > Policies > – Windows Settings > Scripts • Create different login scripts for different OUs – Customize based on your needs Group Policy/updates • Manage the computers or users with Group Policies – Local and Domain policies – Group Policy Management Editor • A central console – Login scripts – Network configurations (QoS) – Security parameters Update a client with the gpupdate utility: > gpupdate /force © 2022 Messer Studios, LLC Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 22 30 2.2 - Wireless Encryption Securing a wireless network • An organization's wireless network can contain confidential information – Not everyone is allowed access • Authenticate the users before granting access – Who gets access to the wireless network? – Username, password, multi-factor authentication • Ensure that all communication is confidential – Encrypt the wireless data • Verify the integrity of all communication – The received data should be identical to the original sent data – A message integrity check (MIC) WPA (Wi-Fi Protected Access) • 2002: WPA was the replacement for serious cryptographic weaknesses in WEP (Wired Equivalent Privacy) – Don't use WEP • Needed a short-term bridge between WEP and whatever would be the successor – Run on existing hardware • WPA: RC4 with TKIP (Temporal Key Integrity Protocol) – Initialization Vector (IV) is larger and an encrypted hash – Every packet gets a unique 128-bit encryption key Wireless encryption • All wireless computers are radio transmitters and receivers – Anyone can listen in • Solution: Encrypt the data – Everyone has an encryption key • Only people with the right key can transmit and listen – WPA2 and WPA3 WPA2 and CCMP • Wi-Fi Protected Access II (WPA2) – WPA2 certification began in 2004 • CCMP block cipher mode – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, or Counter/CBC-MAC Protocol • CCMP security services – Data confidentiality with AES encryption – Message Integrity Check (MIC) with CBC-MAC © 2022 Messer Studios, LLC WPA3 and GCMP • Wi-Fi Protected Access 3 (WPA3) – Introduced in 2018 • GCMP block cipher mode – Galois/Counter Mode Protocol – A stronger encryption than WPA2 • GCMP security services – Data confidentiality with AES – Message Integrity Check (MIC) with – Galois Message Authentication Code (GMAC) The WPA2 PSK problem • WPA2 has a PSK brute-force problem – Listen to the four-way handshake – Some methods can derive the PSK hash without the handshake – Capture the hash • With the hash, attackers can brute force the pre-shared key (PSK) • This has become easier as technology improves – A weak PSK is easier to brute force – GPU processing speeds – Cloud-based password cracking • Once you have the PSK, you have everyone's wireless key – There's no forward secrecy SAE • WPA3 changes the PSK authentication process – Includes mutual authentication – Creates a shared session key without sending that key across the network – No more four-way handshakes, no hashes, no brute force attacks – Adds perfect forward secrecy • Simultaneous Authentication of Equals (SAE) – A Diffie-Hellman derived key exchange with an authentication component – Everyone uses a different session key, even with the same PSK – An IEEE standard - the dragonfly handshake Wireless security modes • Configure the authentication on your wireless access point / wireless router • Open System – No authentication password is required • WPA/2/3-Personal / WPA/2/3-PSK – WPA2 or WPA3 with a pre-shared key – Everyone uses the same 256-bit key • WPA/2/3-Enterprise / WPA/2/3-802.1X – Authenticates users individually with an authentication server (i.e., RADIUS) Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 23 31 2.2 - Authentication Methods RADIUS (Remote Authentication Dial-in User Service) • One of the more common AAA protocols – Supported on a wide variety of platforms and devices – Not just for dial-in • Centralize authentication for users – Routers, switches, firewalls – Server authentication – Remote VPN access – 802.1X network access • RADIUS services available on almost any server operating system TACACS • Terminal Access Controller – Access-Control System – Remote authentication protocol – Created to control access to dial-up lines to ARPANET • TACACS+ – The latest version of TACACS – More authentication requests and response codes – Released as an open standard in 1993 Kerberos • Network authentication protocol – Authenticate once, trusted by the system – No need to re-authenticate to everything – Mutual authentication - the client and the server – Protect against on-path or replay attacks • Standard since the 1980s – Developed by the Massachusetts Institute of Technology (MIT) • Microsoft starting using Kerberos in Windows 2000 – Based on Kerberos 5.0 open standard – Compatible with other operating systems and devices SSO with Kerberos • Authenticate one time – Lots of backend ticketing – Cryptographic tickets • No constant username and password input! – Save time • Only works with Kerberos – Not everything is Kerberos-friendly • There are many other SSO methods – Smart-cards, SAML, etc. Which method to use? • Many different ways to communicate to an authentication server – More than a simple login process • Often determined by what is at hand – VPN concentrator can talk to a RADIUS server – We have a RADIUS server • TACACS+ – Probably a Cisco device • Kerberos - Probably a Microsoft network Multi-factor authentication • More than one factor – Something you are – Something you have – Something you know – Somewhere you are – Something you do • Can be expensive – Separate hardware tokens – Specialized scanning equipment • Can be inexpensive - Free smartphone applications 2.3 - Malware Malware • Malicious software - These can be very bad • Gather information - Keystrokes • Participate in a group - Controlled over the 'net • Show you advertising - Big money • Viruses and worms – Encrypt your data and ruin your day Malware types and methods • Trojan Horse • Rootkit • Viruses • Spyware • Ransomware • Keylogger • Boot sector virus • Cryptominers © 2022 Messer Studios, LLC How you get malware • These all work together – Malicious software takes advantage of a vulnerability – Installs malware that includes a remote access backdoor – Bot may be installed later • Your computer must run a program – Email link - Don't click links – Web page pop-up – Drive-by download – Worm • Your computer is vulnerable – Operating system - Keep your OS updated! – Applications - Check with the publisher Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 24 32 2.3 - Malware (continued) Trojan horse • Used by the Greeks to capture Troy from the Trojans – A digital wooden horse • Software that pretends to be something else – So it can conquer your computer – Doesn't really care much about replicating • Circumvents your existing security – Anti-virus may catch it when it runs – The better Trojans are built to avoid and disable AV • Once it's inside it has free reign – And it may open the gates for other programs Rootkits • Originally a Unix technique – The "root" in rootkit • Modifies core system files – Part of the kernel • Can be invisible to the operating system – Won't see it in Task Manager • Also invisible to traditional anti-virus utilities – If you can't see it, you can't stop it – Finding and removing rootkits • Look for the unusual – Anti-malware scans • Use a remover specific to the rootkit – Usually built after the rootkit is discovered • Secure boot with UEFI – Security in the BIOS Virus • Malware that can reproduce itself – It needs you to execute a program • Reproduces through file systems or the network – Just running a program can spread a virus • May or may not cause problems – Some viruses are invisible, some are annoying • Anti-virus is very common – Thousands of new viruses every week – Is your signature file updated? – Boot sector virus • Most viruses run after the OS is loaded – Like most applications • Some boot loaders can be modified to run malware – Runs every time you start your computer • Modern UEFI BIOS includes Secure Boot – Prevent unsigned software from running during the boot process © 2022 Messer Studios, LLC Spyware • Malware that spies on you – Advertising, identity theft, affiliate fraud • Can trick you into installing – Peer to peer, fake security software • Browser monitoring - Capture surfing habits • Keyloggers – Capture every keystroke – Send it back to the mother ship Ransomware • A particularly nasty malware – Your data is unavailable until you provide cash • Malware encrypts your data files – Pictures, documents, music, movies, etc. – Your OS remains available – They want you running, but not working • You must pay the bad guys to obtain the decryption key – Untraceable payment system – An unfortunate use of public-key cryptography Keyloggers • Your keystrokes contain valuable information – Web site login URLs, passwords, email messages • Save all of your input – Send it to the bad guys • Circumvents encryption protections – Your keystrokes are in the clear • Other data logging – Clipboard logging, screen logging, instant messaging, search engine queries Cryptominers • Some cryptocurrency mining requires "proof of work" – Usually consists of a difficult math problem – Answer the problem and earn some currency • This requires extensive CPU processing – One CPU isn't enough – Attackers want to use your CPU • May appear in different ways – Visit a website and CPU utilization spikes – Malware is installed and mining is always occurring Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 25 33 2.3 - Anti-Malware Tools Windows Recovery Environment • Very powerful • Very dangerous – Last resort • Complete control – Fix your problems before the system starts – Remove malicious software • Requires additional information – Use, copy, rename, or replace operating system files and folders – Enable or disable service or device startup – Repair the file system boot sector or the master boot record (MBR) Starting the console • All Windows versions – Hold Shift key while clicking Restart – Or boot from installation media • Windows 10 – Settings > Update and Security > Recovery > Advanced startup • Windows 11 – System > Recovery > Advanced startup > Restart now • After rebooting – Troubleshoot > Advanced Options > Command Prompt Anti-virus and anti-malware • You need both – Often included together • Real-time options – Not just an on-demand scan • Modern anti-malware recognizes malicious activity – Doesn't require a specific set of signatures Software firewalls • Monitor the local computer – Alert on unknown or unauthorized network communication • Prevent malware communication – Downloads after infection – Botnet communication • Use Windows Firewall - At a minimum • Runs by default – Constantly monitoring – Any network connection Anti-phishing training • No single technology can stop social engineering – Don't give away private information – The user is the best anti-phishing • Extensive training - Avoid becoming a victim • Test the users – Send a phishing email – Find out who clicks and gives up information • Train again End user education • One on one - Personal training • Posters and signs - High visibility • Message board posting - The real kind • Login message - These become invisible • Intranet page - Always available OS reinstallation • Only one way to guarantee malware removal – Delete everything – Install from scratch • Restore from backup (fast) – As long as the backup is not also infected • Manual installation (slowest) – Backup data files – Install Windows from installation media • Image the system (fastest) – User's data files are on a network share – Recover from a prebuilt image 2.4 - Social Engineering Effective social engineering • Constantly changing - You never know what they'll use next • May involve multiple people – And multiple organizations – There are ties connecting many organizations • May be in person or electronic – Phone calls from aggressive "customers" – Emailed funeral notifications of a friend or associate © 2022 Messer Studios, LLC Phishing • Social engineering with a touch of spoofing – Often delivered by email, text, etc. • Don't be fooled - Check the URL • Usually there's something not quite right – Spelling, fonts, graphics • Vishing (Voice phishing) is done over the phone or voicemail – Caller ID spoofing is common – Fake security checks or bank updates Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 26 34 2.4 - Social Engineering (continued) Shoulder surfing • You have access to important information – Many people want to see – Curiosity, industrial espionage, competitive advantage • This is surprisingly easy – Airports / Flights, hallway-facing monitors, or coffee shops • Surf from afar – Binoculars / Telescopes (easy in the big city) – Webcam monitoring Preventing shoulder surfing • Control your input – Be aware of your surroundings • Use privacy filters – It's amazing how well they work • Keep your monitor out of sight – Away from windows and hallways • Don't sit in front of me on your flight – I can't help myself Spear phishing • Targeted phishing with inside information – Makes the attack more believable • Spear phishing the CEO is "whaling" – Targeted phishing with the possibility of a large catch – The CFO (Chief Financial Officer) is commonly speared • These executives have direct access to the corporate bank account – The attackers would love to have those credentials Tailgating and piggybacking • Tailgating uses an authorized person to gain unauthorized access to a building – The attacker does not have consent – Sneaks through when nobody is looking • Piggybacking follows the same process, but the authorized person is giving consent – Hold the door, my hands are full of donut boxes – Sometimes you shouldn't be polite • Once inside, there's little to stop you – Most security stops at the border © 2022 Messer Studios, LLC Watching for tailgating • Policy for visitors - You should be able to identify anyone • One scan, one person – A matter of policy or mechanically required • Access Control Vestibule / Airlock – You don't have a choice • Don't be afraid to ask – Who are you and why are you here? Impersonation • Pretend to be someone you aren't – Halloween for the fraudsters • Use some of those details you got from the dumpster – You can trust me, I'm with your help desk • Attack the victim as someone higher in rank – Office of the Vice President for Scamming • Throw tons of technical details around – Catastrophic feedback due to the depolarization of the differential magnetometer • Be a buddy – How about those Cubs? Dumpster diving • Mobile garbage bin – United States brand name "Dumpster" – Similar to a rubbish skip • Important information thrown out with the trash – Thanks for bagging your garbage for me! • Gather details that can be used for a different attack – Impersonate names, use phone numbers • Timing is important – Just after end of month, end of quarter – Based on pickup schedule Wireless evil twins • Looks legitimate, but actually malicious – The wireless version of phishing • Configure an access point to look like an existing network – Same (or similar) SSID and security settings/captive portal • Overpower the existing access points – May not require the same physical location • WiFi hotspots (and users) are easy to fool – And they're wide open • You encrypt your communication, right? – Use HTTPS and a VPN Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 27 35 2.4 - Denial of Service Denial of service • Force a service to fail – Overload the service • Take advantage of a design failure or vulnerability – Keep your systems patched! • Cause a system to be unavailable – Competitive advantage • Create a smokescreen for some other exploit – Precursor to a DNS spoofing attack • Doesn't have to be complicated – Turn off the power A "friendly" DoS • Unintentional DoSing – It's not always a ne'er-do-well • Network DoS – Layer 2 loop without STP • Bandwidth DoS – Downloading multi-gigabyte Linux distributions over a DSL line • The water line breaks – Get a good shop vacuum Distributed Denial of Service (DDoS) • Launch an army of computers to bring down a service – Use all the bandwidth or resources - traffic spike • This is why the bad guys have botnets – Thousands or millions of computers at your command – At its peak, Zeus botnet infected over 3.6 million PCs – Coordinated attack • The attackers are zombies – Many people have no idea they are participating in a botnet Mitigating DDoS attacks • May be able to filter out traffic patterns – Stop the traffic at your firewall • Internet service provider may have anti-DDoS systems – These can help "turn down" the DDoS volume • Third-party technologies – CloudFlare, etc. 2.4 - Zero-Day Attacks Zero-day attacks • Many applications have vulnerabilities – We've just not found them yet • Someone is working hard to find the next big vulnerability – The good guys share these with developers • Attackers keep these yet-to-be-discovered holes to themselves – They want to use these vulnerabilities for personal gain • Zero-day – The vulnerability has not been detected or published – Zero-day exploits are increasingly common • Common Vulnerabilities and Exposures (CVE) – Zero-day vulnerabilities • December 9, 2021 - Log4j remote code execution – Java-based logging utility provided as an Apache service – Installed on millions of servers – Vulnerability introduced on September 14th, 2013 • December 14th - Fix is released – Extensive patching • December 17th – Two new issues fixed – Everyone is looking for bugs 2.4 - On-Path Attacks On-path network attack • How can an attacker watch without you knowing? – Formerly known as man-in-the-middle • Redirects your traffic – Then passes it on to the destination – You never know your traffic was redirected • ARP poisoning – On-path attack on the local IP subnet – ARP has no security – ARP poisoning (spoofing) © 2022 Messer Studios, LLC On-path browser attack • What if the middleman was on the same computer as the victim? – Malware/Trojan does all of the proxy work – Formerly known as man-in-the-browser • Huge advantages for the attackers – Relatively easy to proxy encrypted traffic – Everything looks normal to the victim • The malware in your browser waits for you to login to your bank – And cleans you out Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 28 36 2.4 - On-Path Attacks (continued) ARP poisoning (spoofing) 1 2 ARP Response: I am 192.168.1.1 A legitimate response to an ARP request is received from the default gateway. The ARP response is cached on the local device. An attacker sends an ARP response that spoofs the IP address of the router and includes the attacker's MAC address. The malicious ARP information replaces the cached record, completing the ARP poisoning. My MAC address is 11:22:33:44:55:66 192.168.1.9 c8:bc:c8:a7:38:d5 192.168.1.1 11:22:33:44:55:66 ARP Cache 192.168.1.1 = 11:22:33:44:55:66 ARP 192.168.1.9 c8:bc:c8:a7:38:d5 My M Resp o nse: AC ad d I am 192 ress i s .168 aa:b .1.1 b:cc: ARP Cache 192.168.1.1 = 11:22:33:44:55:66 192.168.1.1 = aa:bb:cc:dd:ee:ff 192.168.1.1 11:22:33:44:55:66 dd:e e:ff 192.168.1.4 aa:bb:cc:dd:ee:ff 2.4 - Password Attacks Plaintext / unencrypted passwords • Some applications store passwords "in the clear" – No encryption. You can read the stored password. – This is rare, thankfully • Do not store passwords as plaintext – Anyone with access to the password file or database has every credential • What to do if your application saves passwords as plaintext: – Get a better application Hashing a password • Hashes represent data as a fixed-length string of text – A message digest, or "fingerprint" • Will not have a collision (hopefully) – Different inputs will not have the same hash • One-way trip – Impossible to recover the original message from the digest – A common way to store passwords The password file • Different across operating systems and applications – Different hash algorithms © 2022 Messer Studios, LLC Brute force • Try every possible password combination until the hash is matched • This might take some time – A strong hashing algorithm slows things down • Brute force attacks - Online – Keep trying the login process – Very slow – Most accounts will lockout after a number of failed attempts • Brute force the hash - Offline – Obtain the list of users and hashes – Calculate a password hash, compare it to a stored hash – Large computational resource requirement Dictionary attacks • Use a dictionary to find common words – Passwords are created by humans • Many common wordlists available on the 'net – Some are customized by language or line of work • The password crackers can substitute letters – p&ssw0rd • This takes time – Distributed cracking and GPU cracking is common • Discover passwords for common words – This won't discover random character passwords Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 29 37 2.4 - Insider Threats Insider threats • More than just passwords on sticky notes – Some insiders are out for no good • Sophistication may not be advanced, but the insider has institutional knowledge – Attacks can be directed at vulnerable systems – The insider knows what to hit • Extensive resources – Eating away from the inside Recruiting insiders • We're getting better with protecting the network perimeter – It's an ongoing race • Ransomware actors are targeting insiders – Offering Bitcoin in exchange for access – One ransomware infection can earn millions for an attacker • Keep aware – Maintain good security fundamentals – Always have backups 2.4 - SQL Injection Code injection • Code injection – Adding your own information into a data stream • Enabled because of bad programming – The application should properly handle input and output • So many different data types – HTML, SQL, XML, LDAP, etc. SQL injection • SQL - Structured Query Language – The most common relational database management system language • SQL Injection – Modify SQL requests (Your application shouldn't allow this) • If you can manipulate the database, then you control the application – A significant vulnerability 2.4 - Cross-site Scripting Cross-site scripting • XSS – Cascading Style Sheets (CSS) are something else entirely • Originally called cross-site because of browser security flaws – Information from one site could be shared with another • One of the most common web application development errors – Takes advantage of the trust a user has for a site – Complex and varied • Malware that uses JavaScript – Do you allow scripts? Me too. Non-persistent (reflected) XSS attack • Web site allows scripts to run in user input – Search box is a common source • Attacker emails a link that takes advantage of this vulnerability – Runs a script that sends credentials / session IDs / cookies to the attacker • Script embedded in URL executes in the victim's browser – As if it came from the server • Attacker uses credentials/session IDs/ cookies to steal victim's information without their knowledge – Very sneaky © 2022 Messer Studios, LLC Persistent (stored) XSS attack • Attacker posts a message to a social network – Includes the malicious payload • It's now "persistent"- Everyone gets the payload • No specific target - All viewers to the page • For social networking, this can spread quickly – Everyone who views the message can have it posted to their page – Where someone else can view it and propagate it further... Hacking a Subaru • June 2017, Aaron Guzman - Security researcher • When authenticating with Subaru, users get a token – This token never expires (bad!) • A valid token allowed any service request – Even adding your email address to someone else's account – Now you have full access to someone else's car • Web front-end included an XSS vulnerability – A user clicks a malicious link, and you have their token Protecting against XSS • Be careful when clicking untrusted links – Never blindly click in your email inbox. Never. • Consider disabling JavaScript – Or control with an extension – This offers limited protection • Keep your browser and applications updated – Avoid the nasty browser vulnerabilities • Validate input – Don't allow users to add their own scripts to an input field Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 30 38 2.4 - Security Vulnerabilities Non-compliant systems • A constant challenge – There are always changes and updates • Standard operating environments (SOE) – A set of tested and approved hardware/software systems – Often a standard operating system image • Operating system and application updates – Must have patches to be in compliance – OS updates, anti-virus signatures – Can be checked and verified before access is given Protecting against non-compliant systems • Operating system control – Apply policies that will prevent non-compliant software • Monitor the network for application traffic – Next-generation firewalls with application visibility • Perform periodic scans – Login systems can scan for non-compliance – Require correction before the system is given access Unpatched systems • Microsoft Patch Tuesday – Second Tuesday of each month (10:00 AM PST) • Suddenly, systems are vulnerable to security flaws – Patch the operating system and applications • An organization might have thousands of systems – Some of those are major services • One forgotten system may be the weakest link – This happens quite a bit • Patch management is a critical practice – Test, prioritize, and deploy Unprotected systems • Security issues are often roadblocks – Applications may not work properly without additional configurations • Some troubleshooting tasks can be insecure – Disable antivirus and try again – Disable the firewall and try again • Permanently disabling security isn't the answer – You don't fix a bad door lock by removing the door – Become an expert in application troubleshooting Product support lifetime • End of life (EOL) operating systems – Manufacturer stops selling an OS – May continue supporting the OS – Important for security patches and updates • End of service life (EOSL) – Manufacturer stops selling an OS – Support is no longer available – No ongoing security patches or updates – May have a premium-cost support option • Technology EOSL is a significant concern – Security patches are part of normal operation BYOD • Bring Your Own Device / Bring Your Own Technology • Employee owns the device – Need to meet the company's requirements • Difficult to secure – It's both a home device and a work device – How is data protected? – What happens to the data when a device is sold or traded in? – An infected device could disclose proprietary company information 2.5 - Defender Antivirus Microsoft Defender Antivirus • Built-in antivirus for Windows 10 and 11 – No additional third-party products required • Included in the Windows Security app – Virus & threat protection • May not specifically display "Defender Antivirus" – The name has changed over time – Windows Defender – Microsoft Defender Antivirus Activate or deactivate • Don't disable your security protection – This is for temporary troubleshooting – This will increase risk – Make sure you know what you're doing © 2022 Messer Studios, LLC • Defender Antivirus operates in real-time – Enable or disable this feature • Windows Security app – Virus & threat protection settings > – Manage settings > Real-time protection Updated definitions • Antivirus is only as good as the latest signatures – It's important to stay up to date • Virus & threat protection updates – Check for updates • Click the "Check for updates" button – Automatic updates are normally configured Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 31 39 2.5 - Windows Firewall Enabling and disabling Windows Firewall • Your firewall should always be enabled – Sometimes you need to troubleshoot • Temporarily disable from the Control Panel or from Windows Security – Turn Windows Firewall on or off – Requires elevated permissions • Different settings for each network type - Public / Private Windows Firewall configuration • Block all incoming connections – Ignores your exception list – Useful when you need security • Modify notification - App blocking Creating a firewall exception • Allow an app or feature through Windows Firewall – The more secure exception • Port number – Block or allow • Predefined exceptions – List of common exceptions – Custom rule – Every firewall option 2.5 - Windows Security Settings Windows authentication • Login to the Windows desktop – And access network resources • Local accounts – Only associated with a specific Windows device • Microsoft accounts – Sync settings between devices, integrate applications (Skype, Office) with OneDrive, and more • Windows Domain accounts – Centrally managed from Active Directory Users and groups • Users – Administrator – The Windows super-user – Guest (Limited access) – Standard Users • Groups – Power Users – Not much more control than a regular user – Permissions removed in Windows Vista and later Login options • Username / password – Common authentication credentials • Personal Identification Number (PIN) – A local access code • Biometrics – Fingerprint, facial recognition • Single sign-on (SSO) – Windows Domain credentials – Sign in one time © 2022 Messer Studios, LLC NTFS vs. Share permissions • NTFS permissions apply from local and network connections • Share permissions only apply to connections over the network – A "network share" • The most restrictive setting wins – Deny beats allow • NTFS permissions are inherited from the parent object – Unless you move to a different folder on the same volume Explicit and inherited permissions • Explicit permissions – Set default permissions for a share • Inherited permissions – Propagated from the parent object to the child object – Set a permission once, it applies to everything underneath • Explicit permissions take precedence over inherited permissions – Even inherited deny permissions Run as administrator • Administrators have special rights and permissions – Editing system files, installing services • Use rights and permissions of the administrator – You don't get these by default, even if you're in the Administrators group • Right-click the application – Run as administrator – Or search and click "Run as administrator" Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 32 40 2.5 - Windows Security Settings (continued) UAC (User Account Control) • Limit software access - Protect your computer • Standard users – Use the network or change your password • Administrators – Install applications or configure Remote Desktop • Secure Desktop - Limits automated access BitLocker • Encrypt an entire volume – Protects all of your data, including the OS – Support for all Windows editions except Home • Lose your laptop? - Doesn't matter without the password • Data is always protected – Even if the physical drive is moved to another computer • BitLocker To Go - Encrypt removable USB flash drives EFS • Encrypting File System – Encrypt at the file system level – Requires the NTFS file system • OS support – Support for all Windows editions except Home • Uses password and username to encrypt the key – Administrative resets will cause EFS files to be inaccessible 2.6 - Security Best Practices Data encryption • Full-disk encryption – Encrypt data-at-rest • File system encryption – Individual files and folders • Removable media – Protect those USB flash drives • Key backups are critical – You always need to have a copy – This may be integrated into Active Directory – You'll want to keep the key handy Password complexity and length • Make your password strong – Resist guessing or brute-force attack • Increase password entropy – No single words, no obvious passwords – Mix upper and lower case and use special characters • Stronger passwords are at least 8 characters – Consider a phrase or set of words Password expiration and recovery • All passwords should expire – Change every 30 days, 60 days, 90 days – System remembers password history, requires unique passwords • Critical systems might change more frequently – Every 15 days or every week • The recovery process should not be trivial! – Some organizations have a very formal process Password best practices • Changing default usernames/passwords – All devices have defaults – There are many web sites that document these © 2022 Messer Studios, LLC • BIOS/UEFI passwords – Supervisor/Administrator password: Prevent BIOS changes – User password: Prevent booting • Requiring passwords – Always require passwords – No blank passwords – No automated logins End-user best practices • Require a screensaver password – Integrate with login credentials – Can be administratively enforced • Does not require user intervention – Automatically locks after non-use or timeout • Secure critical hardware – Laptops can easily walk away – Lock them down Securing PII and passwords • Personally identifiable information – Name, address, social security number, etc. • Control your input – Be aware of your surroundings • Use privacy filters – It's amazing how well they work • Keep your monitor out of sight – Away from windows and hallways • Don't sit in front of me on your flight – I can't help myself Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 33 41 2.6 - Security Best Practices (continued) Account management • User permissions – Everyone isn't an Administrator – Assign proper rights and permissions – This may be an involved audit • Assign rights based on groups – More difficult to manage per-user rights – Becomes more useful as you grow • Login time restrictions – Only login during working hours – Restrict after-hours activities Disabling unnecessary accounts • All operating systems include other accounts – Guest, root, mail, etc. • Not all accounts are necessary – Disable/remove the unnecessary – Disable the guest account • Disable interactive logins – Not all accounts need to login • Change the default usernames – User:admin Password:admin – Helps with brute-force attacks Locking the desktop • Failed password attempts – Should lock the account and/or reboot after a certain threshold – Prevents online brute force attacks • Automatically lock the system – After a certain amount of inactivity – Or when you walk away AutoRun and AutoPlay • Disable AutoRun on older OSes – autorun.inf in Vista – No Autorun in Windows 7, 8/8.1, 10, or 11 – Disabled through the registry • Disable AutoPlay – Configure in Settings > Bluetooth & devices > AutoPlay • Get the latest security patches – Updates to autorun.inf and AutoPlay 2.7 - Mobile Device Security Screen locks • Restrict access to the device – You're going to leave it somewhere • Facial recognition - Unlock with your face • PIN – Choose a personal identification number • Fingerprint – Built-in fingerprint reader • Swipe – Choose a pattern • Failed attempts – iOS: Erase everything after 10 failed attempts – Android: Lock the device and require a Google login or wipe the device Locator applications and remote wipe • Built-in GPS – And location "helpers" • Find your phone – On a map. • Control from afar – Make a sound – Display a message • Wipe everything – At least your data is safe © 2022 Messer Studios, LLC Patching/OS updates • All devices need updates - Even mobile devices • Device patches - Security updates • Operating system updates – New features, bug fixes • Don't get behind! – Avoid security problems Full device encryption • Encrypt all device data – Phone keeps the key • iOS 8 and later – Personal data is encrypted with your passcode • Android – Version 5.0 and later is probably already encrypted Remote backup • Difficult to backup something that's always moving – Backup to the cloud • Constant backup – No manual process • Backup without wires – Use the existing network • Restore with one click – Restores everything – Authenticate and wait Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 34 42 2.7 - Mobile Device Security (continued) Anti-virus and anti-malware • Apple iOS – Closed environment, tightly regulated – Malware has to find a vulnerability • Android – More open, apps can be installed from anywhere – Easier for malware to find its way in • Apps run in a "sandbox" – You control what data an app can view • Third-party virus and malware protection – Available from the usual providers Firewalls • Mobile phones don't include a firewall – Most activity initiates outbound, not inbound • Some mobile firewall apps are available – Most for Android – None seem to be widely used • Enterprise environments can control mobile apps – Firewalls can allow or disallow access Policies and procedures • Manage company-owned and user-owned mobile devices – BYOD - Bring Your Own Device • Centralized management of the mobile devices – Specialized functionality / Mobile Device Manager (MDM) • Set policies on apps, data, camera, etc. – Control the remote device – The entire device or a "partition" • Manage access control – Force screen locks and PINs on these single user devices IoT (Internet of Things) • Sensors - Heating and cooling, lighting • Smart devices - Home automation, video doorbells • Wearable technology - Watches, health monitors • Facility automation - Temperature, air quality, lighting • Weak defaults – IoT manufacturers are not security professionals – Consider isolating IoT devices on their own network 2.8 - Data Destruction Physical destruction • Shredder – Heavy machinery - complete destruction • Drill / Hammer – Quick and easy - Platters, all the way through • Electromagnetic (degaussing) – Remove the magnetic field – Destroys the drive data and the electronics • Incineration - Fire hot. Certificate of destruction • Destruction is often done by a 3rd party – How many drills and degaussers do you have? • Need confirmation that your data is destroyed – Service should include a certificate • A paper trail of broken data – You know exactly what happened Disk formatting • Low-level formatting – Provided at the factory – Not recommended for the user • Standard formatting / Quick format – Sets up the file system, installs a boot sector – Clears the master file table but not the data – Can be recovered with the right software • Standard formatting / Regular format – Overwrites every sector with zeros – Default for Windows Vista and later – Can't recover the data © 2022 Messer Studios, LLC Erasing data • File level overwriting – Sdelete – Windows Sysinternals – Remaining files are still available • Whole drive wipe secure data removal – DBAN - Darik's Boot and Nuke – Removes all data on the drive – Use the drive again • Physical drive destruction – One-off or industrial removal and destroy – Drive is no longer usable Hard drive security • 2019 study from Blancco and Ontrack – 159 storage drives from eBay – 42% of the used drives contain sensitive data • Different data types – 66 drives had data, 25 drives with PII • Varied data sources – Travel company email archive – Freight company shipping details – University student papers – Audio, video, and other personal files Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 35 43 2.9 - Securing a SOHO Network Change default passwords • All access points have default usernames and passwords – Change yours! • The right credentials provide full control – Administrator access • Very easy to find the defaults for your access point or router – Firmware updates • Small office / home office appliances – Appliance are usually a closed architecture – Updates are provided by the manufacturer • Updates may address different requirements – Bug fixes – New features – Security patches • Install the latest software – Update and upgrade the firmware – Firewalls, routers, switches, etc. IP address filtering • Content filtering, IP address ranges – Or a combination • Allow list – Nothing pass through the firewall unless it's approved – Very restrictive • Deny list – Nothing on the "bad list" is allowed – Specific URLs – Domains – IP addresses Content filtering • Control traffic based on data within the content – URL filtering, website category filtering • Corporate control of outbound and inbound data – Sensitive materials • Control of inappropriate content – Not safe for work – Parental controls • Protection against evil – Anti-virus, anti-malware Physical placement • Often a single device – Router, switch, access point, firewall, etc. • Location may be restricted to a secure room – Prevent access to servers and network devices – For wireless, location becomes more important – Above ceiling tiles or another high point – This may cause problems for power cycling • Plan before the installation – May require additional setup time © 2022 Messer Studios, LLC IP addressing • DHCP (automatic) IP addressing vs. manual IP addressing • IP addresses are easy to see in an unencrypted network • If the encryption is broken, the IP addresses will be obvious • Configuring a static IP address is not a security technique – Security through obscurity DHCP reservations • Address reservation – Administratively configured • Table of MAC addresses – Each MAC address has a matching IP address • Other names – Static DHCP Assignment – Static DHCP – Static Assignment – IP Reservation Static WAN IP • Wide area network / Internet link – External IP address • Many ISPs dynamically allocate WAN addresses – The default for most ISPs • It's easier to manage if the IP address is static – The IT team always knows the IP address – A SOHO might provide a service • This may be an additional cost – Contact the ISP for options UPnP (Universal Plug and Play) • Allows network devices to automatically configure and find other network devices – Zero-configuration • Applications on the internal network can open inbound ports using UPnP – No approval needed – Used for many peer-to-peer (P2P) applications • Best practice would be to disable UPnP – Only enable if the application requires it – And maybe not even then Screened subnet • Previously known as the demilitarized zone (DMZ) – An additional layer of security between the Internet and you – Public access to public resources Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 36 44 2.9 - Securing a SOHO Network (continued) SSID management • Service Set Identifier – Name of the wireless network – LINKSYS, DEFAULT, NETGEAR • Change the SSID to something not-so obvious • Disable SSID broadcasting? – SSID is easily determined through wireless network analysis – Security through obscurity Wireless channels and encryption • Open System – No authentication password is required • WPA/2/3-Personal / WPA/2/3-PSK – WPA2 or WPA3 with a pre-shared key – Everyone uses the same 256-bit key • WPA/2/3-Enterprise / WPA/2/3-802.1X – Authenticates users individually with an authentication server (i.e., RADIUS, LDAP, etc.) • Use an open frequency – Some access points will automatically find good frequencies Disable guest networks • Limit access to outsiders – Guest networks are often enabled by default • Some guest networks can be used for other connections – Internet of Things – Lab networks • Don't enable without security – WPA2 or WPA3 2.10 - Browser Security Disabling ports • Enabled physical ports – Conference rooms – Break rooms • Administratively disable unused ports – More to maintain, but more secure • Network Access Control (NAC) – 802.1X controls – You can't communicate unless you are authenticated Port forwarding • 24x7 access to a service hosted internally – Web server, gaming server, security system, etc. • External IP/port number maps to an internal IP/port – Does not have to be the same port number • Also called Destination NAT or Static NAT – Destination address is translated from a public IP to a private IP – Does not expire or timeout Screened Subnet Screened Subnet Switch Internal Network Internet Browser download and installation • Always use trusted sources – Attackers want you to install the malware for them – No fancy exploit required • Avoid untrusted third-party sites – Don't click links in emails – Don't follow links from other websites – Always visit a browser site directly • Use hashes to verify the download – Confirm the downloaded file matches the version on the server Hash verification • Install a hash checking application – Available for command line and GUI – Options available in the Microsoft Store • Hash values may be available on the download site – Usually includes a digital signature for verification • Verify the downloaded file – Compare the downloaded file hash with the posted hash value © 2022 Messer Studios, LLC Firewall Internal Network Switch Extensions and plug-ins • Trusted sources – Official browser extension library – Chrome Web Store – Microsoft Store – Known-good websites • Untrusted sources – Random or unfamiliar websites – Installed by malware • This is a significant attack vector – Almost everything we do is in our browser Malicious browser extensions • March 2021 – More than 24 malicious – Google Chrome extensions identified – Includes 40 malicious domains – Not identified by security technologies Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 37 45 2.10 - Browser Security (continued) • Malicious activity identified – Credential theft – Screenshots and keylogging – Data exfiltration • Don't trust any software - Always have backups Password managers • Password vaults – All passwords in one location – A database of credentials • Secure storage – All credentials are encrypted – Cloud-based synchronization options • Create unique passwords – Passwords are not the same across sites • Personal and enterprise options – Corporate access Secure connections • Security alerts and invalid certificates – Something isn't quite right – Should raise your interest • Look at the certificate details – May be expired or the wrong domain name – The certificate may not be properly signed (untrusted certificate authority) – Correct time and date is important Enable pop-up blockers • Pop-up blocker – Prevent unwanted notification windows • Enable or disable – Should usually be enabled – Disable temporarily when troubleshooting • Block and allow – Control pop-up blocking on certain websites Clearing private data • Clear browsing data – History – Saved passwords – List of downloaded files • Clear cache – Parts of a website are stored locally – Remove all local data Private browsing mode • Don't store information from a browsing session – Good for privacy – Useful when testing or troubleshooting • Removes the information when the browser is closed – No history tracking – No download file list – Cached information is deleted Browser data synchronization • Share browsing data across multiple systems – Sign in to the browser • Use with other computers, tablets, and mobile devices – Browsing history – Favorites – Installed extensions – Other settings Ad blockers • Some browsers can block advertising – This isn't always an option • Many sites will track visits – And recognize a return visit • Difficult to always recognize an advertisement – You can control the security level 3.1 - Troubleshooting Windows Bluescreens and frequent shutdowns • Startup and shutdown BSOD – Bad hardware, bad drivers, bad application • Use Last Known Good, System Restore, or Rollback Driver – Try Safe mode • Reseat or remove the hardware – If possible • Run hardware diagnostics – Provided by the manufacturer – BIOS may have hardware diagnostics Sluggish performance • Task Manager – Check for high CPU utilization and I/O • Windows Update - Latest patches and drivers © 2022 Messer Studios, LLC • Disk space - Check for available space and defrag • Laptops may be using power-saving mode – Throttles the CPU • Anti-virus and anti-malware - Scan for attackers Boot errors • Can't find operating system – "Operating system not found", "Missing operating system" • Boot loader replaced or changed – Multiple operating systems installed • Check boot drives - Remove any media • Startup Repair • Modify the Windows Boot Configuration Database (BCD) – Formerly boot.ini – Recovery Console: bootrec /rebuildbcd Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 38 46 3.1 - Troubleshooting Windows (continued) Startup Repair • Missing NTLDR – The main Windows boot loader is missing – Run Startup Repair or replace manually and reboot – Disconnect removable media • Missing operating system – Boot Configuration Data may be incorrect – Run Startup Repair or manually configure BCD store • Boots to Safe Mode – Windows is not starting normally – Run Startup Repair Starting the system • Device not starting – Check Device Manager and Event Viewer – Often a bad driver – Remove or replace driver • "One or more services failed to start" – Bad/incorrect driver, bad hardware – Try starting manually – Check account permissions – Confirm service dependencies – Windows service; check system files – Application service; reinstall application Applications crashing • Application stops working – May provide an error message – May just disappear • Check the Event Log – Often includes useful reconnaissance • Check the Reliability Monitor – A history of application problems – Checks for resolutions • Reinstall the application – Contact application support Low memory warnings • Your computer is low on memory – Applications need RAM to run – More applications need more RAM • Close large-memory processes – Check Task Manager • Increase virtual memory – More room for swapping applications – System > About > Advanced system settings > Performance > Settings > Virtual memory © 2022 Messer Studios, LLC USB controller resource warnings • USB devices contain buffers called "endpoints" – Different USB controllers support a different number of endpoints – (96 endpoints, 254 endpoints, etc.) • Different devices require a different number of endpoints – Exceed the number of endpoints and you run out of resources – It's difficult to determine the number of endpoints used by a device • The controller does not have enough resources for this device. – The endpoints are these resources • Move the device to a different USB interface – USB 2.0 interfaces might support a larger number of endpoints • Match the USB interface to the device capabilities – USB 2.X devices or USB 3.X devices – More endpoints for all devices System instability • General system failures – Software errors, system hangs, application failures • Time for a full diagnostic - This could be anything • Hardware diagnostic – Most systems include manufacturer diagnostics – Also run storage and memory checks • Check the operating system – Run SFC (System File Checker) – Perform an anti-malware scan Slow profile load • Roaming user profile – Your desktop follows you to any computer – Changes are synchronized • Network latency to the domain controller – Slows login script transfers – Slow to apply computer and user policies – May require many hundreds (or thousands) of LDAP queries • Client workstation picks a remote domain controller instead of local DC – Problems with local infrastructure Time drift • A computer's internal clock will drift over time – Computers aren't great timekeepers • The solution is to fix the symptom – Fixing the problem would require changing the design of every computer • Enable automatic time setting – Settings > Time & language > Date & time – Time zone may need to be configured manually if privacy settings are enabled Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 39 47 3.1 - Troubleshooting Solutions Reboot • Have you tried turning it off and on again? – There's a reason it works • Bug in your router software - Reboot the router • Application is using too many resources – Stops the app • Memory leak slowly consumes all available RAM – Clears the RAM and starts again Restart services • Services – Applications that run in the background – No user interaction • Similar issues as a normal process – Resource utilization – Memory leaks – Crashes • View status in Task Manager – Services tab – Right-click to start, stop, or restart Uninstall/reinstall/update applications • Application issues – Problems with the application files or configurations • Settings > Apps > Apps & features – Repair, reset, or uninstall • Some options in the Control Panel – Programs and Features • Run the application setup again – Other options may be available from the setup program • Repair – Install missing files – Replace corrupted files – Fix application shortcuts – Repair registry entries – Update or reconfigure drivers • Reset – Remove all application data – A factory reset / original install • Uninstall - Remove the application Verify requirements • Every operating system and application publishes a set of

requirements – These are commonly the bare minimums • Check with the manufacturer – Get the official requirements • Hardware and software resources – CPU speed, total RAM, video options, device drivers, runtime libraries • Use System Information – View the current configuration © 2022 Messer Studios, LLC Add resources • Check resource utilization – Task Manager • Consider a long-term analysis – Performance Monitor • Compare existing resources with manufacturer requirements – Add or replace hardware (CPU, SSD, RAM) • Free drive space – Disk Cleanup System file checker • Verify the integrity of the operating system – Check every important system file with sfc Startup Repair • Start from Settings – Settings > System > Recovery • Also available from the – Advanced Boot Options – Repair Windows Windows Restore • Start the System Restore application – System > About > System Protection – This assumes you've not disabled restore points • Pick a restore point and let the system reboot – The operating system configuration will revert to the previous date and time – User data will not be modified Reimage or reload OS • Windows is big – And complex • Spend time trying to find the needle – Or simply build a new haystack • Many organizations have prebuilt images – Don't waste time researching issues • Windows includes a reset option – Windows 10: Settings > Update & Security > Recovery – Windows 11: Settings > System > Recovery Update and patch • Windows Update – Centralized OS and driver updates • Lots of flexibility – Change active hours – Manage metered connections • Applications must be patched – Security issues don't stop at the OS – Download from the publisher Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 40 48 3.1 - Troubleshooting Solutions (continued) Roll back updates • Updates are installed automatically by default – Important security patches • View the history – Windows 10: – Settings > Update & Security > – Windows Update – Windows 11: – Settings > Windows Update Rebuild Windows profiles • Profiles can become corrupted – The User Profile Service failed the logon. – User Profile cannot be loaded. – User documents may be "missing" • If a profile doesn't exist, it's recreated – We're going to delete the profile and force the rebuilding process Deleting Windows profiles • Login to the computer with Domain Administrator rights • Rename the \Usersame folder - This will save important files • Backup the user's registry – HKLM\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ProfileList – Right-click / Export • Delete the registry entry – You have a backup - Restart the computer Reconstructing Windows profiles • Login to the computer with the user account – The profile will be rebuilt – This will recreate the \Usersame folder • Login as Domain Administrator – Copy over any important files from the old profile • Do not copy the entire profile – Corrupted files might exist in the old profile • Logout as Domain Administrator, login with the user account 3.2 - Troubleshooting Security Issues Unable to access the network • Slow performance, lock-up – Malware isn't the best written code • Internet connectivity issues – Malware likes to control everything – You go where it wants you to go – You can't protect yourself if you can't download • OS updates failures – Malware keeps you vulnerable – Some malware uses multiple communication paths • Reload or clean – Malware cleaner or recover from known good backup Desktop alerts • Browser push notification messages – Pretends to be a malware infection – Actual notifications come from your antivirus utility • Disable browser notifications – Create an allow list of legit sites • Scan for malware – Consider a cleaning – Rebuild from scratch or known good backup to guarantee removal False antivirus alerts • False antivirus message • May include recognizable logos and language – May require money to "unlock" your PC – Or to "subscribe" to their service • Often requires a specific anti-malware removal utility or technique – The attackers are very, very good © 2022 Messer Studios, LLC Altered system or personal files • Renamed system files - Won't need that anymore • Files disappearing - Or encrypted • File permission changes - Protections are modified • Access denied – Malware locks itself away – It doesn't leave easily • Use a malware cleaner or restore from known good backup – Some malware is exceptionally difficult to remove Browser security alerts • Security alerts and invalid certificates – Something isn't quite right – Should raise your interest • Look at the certificate details – Click the lock icon – May be expired or the wrong domain name – The certificate may not be properly signed (untrusted certificate authority) – Correct time and date is important Browser redirection • Instead of your Google result, your browser goes somewhere else – This shouldn't ever happen • Malware is the most common cause – Makes money for the bad guys • Use an anti-malware/anti-virus cleaner – This is not the best option • Restore from a good known backup – The only way to guarantee removal Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 41 49 3.3 - Removing Malware Malware removal • This is almost never the best practice – It's impossible to know if all of the malware has been removed • Ideally, you should delete everything and start over – Restore from a known-good backup – Install from the original media • There are reasons to remediate – Important user documents may need to be recovered – Get the system running well enough to backup certain files 1. Verify malware symptoms • Odd error messages – Application failures, security alerts • System performance issues – Slow boot, slow applications • Research the malware – Know what you're dealing with 2. Quarantine infected systems • Disconnect from the network – Keep it contained • Isolate all removable media – Everything should be contained • Prevent the spread – Don't transfer files, don't try to backup – That ship sailed 3. Disable System Restore • Restore points make it easy to rewind – Malware infects restore points • Disable System Protection – No reason to save an infected config • Delete all restore points – Remove all infection locations 4a. Remediate: Update anti-virus • Signature and engine updates – The active anti-virus engine – Signature updates – A very, very tiny shelf life • Automatic vs. manual – Manual updates are almost pointless • Your malware may prevent the update process – Copy from another computer 4b. Remediate: Scan and remove • Microsoft and others - The big anti-virus apps • Malware-specific – Scan and remove difficult malware • Stand-alone removal apps – Check with your anti-virus company • There's really no way to know if it's really gone – Delete and rebuild © 2022 Messer Studios, LLC 4b. Remediate: Scan and remove • Safe mode – Load the bare minimum operating system – Just enough to get the OS running – Can also prevent the bad stuff from running • Pre-installation environment (WinPE) – Recovery Console, bootable CD/DVDs/USBs – Build your own from the Windows – Assessment and Deployment Kit (ADK) • May require the repair of boot records and sectors 5. Schedule scans and run updates • Built into the antivirus software – Automated signature updates and scans • Task scheduler – Run any task • Operating system updates – Make sure its enabled and working 6. Enable System Protection • Now you're clean – Put things as they were • Create a restore point – Start populating again 7. Educate the end user • One on one – Personal training • Posters and signs – High visibility • Message board posting – The real kind • Login message – These become invisible • Intranet page – Always available Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 42 50 3.4 - Troubleshooting Mobile Devices App issues • Problematic apps – Apps not loading – Slow app performance • Restart the phone – Hold power button, power off • Stop the app and restart – iPhone: Double-tap home|slide up, slide app up – Android: Settings/Apps, select app, Force stop • Update the app - Get the latest version App fails to close or crashes • App hangs – But other apps are still working • App crashes – May provide an error message, or just disappear • Restart the device – Clear the slate, try the app again • Update the app – A bug fix might resolve the issue • Delete and reinstall the app – Be careful not to remove important app data App fails to update • App does not update to a new version – But other apps are still working • Check the Store to manually upgrade – Force the upgrade process – Some stores require a valid method of payment on file • Restart the device – Try the update process again OS fails to update • Device operating system will not update – New features, bug fixes, security updates • Check available storage – Remove unused documents and apps • Check download bandwidth – Connect to Wi-Fi • Try a different network connection – Update server may not be accessible • Reboot - Always a good idea Battery life issues • Bad reception – Always searching for signal – Airplane mode on the ground • Aging battery – There's only so many recharges • Disable unnecessary features – 802.11 wireless, Bluetooth, GPS • Check application battery usage – iOS: Settings/Battery – Android: Settings/Battery © 2022 Messer Studios, LLC Random reboots • A device reboots during normal operation – May occur randomly • Check the OS and app versions – Keep everything up to date • Perform a hardware check – Check the battery health – Not many diagnostics options • Contact Tech Support for options – Crash logs should be on the device Connectivity issues • Intermittent connectivity – Move closer to access point – Try a different access point • No WiFi connectivity – Check/Enable WiFi – Check security key configuration – Hard reset can restart wireless subsystem • No Bluetooth connectivity – Check/Enable Bluetooth – Check/Pair Bluetooth component – Hard reset to restart Bluetooth subsystem • NFC not working – Limited troubleshooting options – Device may allow disable/enable of NFC – Reset the device – If payment related, remove and add the card again • AirDrop not working – Distance between devices < 30 feet – Turn on Wi-Fi and Bluetooth – Check AirDrop discovery options – "Allow me to be discovered by" Screen does not autorotate • Turning the device doesn't rotate the view – It should know which way is up • Disable rotation lock – Prevents autorotation when enabled • Restart the app – The device might be working properly • Restart the device – Perhaps the device isn't working properly • Contact device support – If nothing rotates, you could have a sensor issue Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 43 51 3.5 - Troubleshooting Mobile Device Security Android package source • Once malware is on a phone, it has a huge amount of access – Don't install APK files from an untrusted source • iOS – All apps are curated by Apple • Android – Apps can be downloaded from Google Play or sideloaded – This is where problems can occur Developer mode • Enables developer-specific settings – USB debugging – Memory statistics – Demo mode settings • iOS and iPadOS – Enable using Xcode – Must use macOS • Android – Enabled from Settings > About Phone – Tap the build number seven times Root access/jailbreaking • Mobile devices are purpose-built systems – You don't need direct access to the operating system • Gaining access – Android - Rooting – Apple iOS - Jailbreaking • Install custom firmware – Replaces the existing operating system • Uncontrolled access – Circumvent security features, sideload apps without using an app store – The MDM becomes relatively useless Application spoofing • Install what appears to be a legitimate app – Actually a bootleg or malicious application • Google removed 150 apps from the store in 2021 – Photo editing, camera filters, games, QR code scanners – UltimaSMS app tried to subscribe users to $40/month SMS service • Infect the application used to build the apps – A malicious version of Xcode: XcodeGhost malware • Always check the source of a download – And the legitimacy of the app – You are giving this app permissions and control High network traffic • Higher than normal network use – May indicate installed malware – Command & control – Proxy network use • Check built-in data use reports – Some of these are quite detailed © 2022 Messer Studios, LLC • Use a third-party reporting app – Use a trusted source • Run a malware scan – Always a good precaution Data-usage limit notification • Built-in Android feature – Not native in iOS • Set a warning and limit – Get notification when traffic is excessive • Can indicate a malware infection – Drill-down on individual app usage • Run a malware scan – Find the problem app Sluggish response time • Running slowly – Screen lags, poor input response time • Restart – Clear the slate • Check for OS and app updates – Fix the buggy code • Close apps that are not in use – Less resources to manage • Factory reset – A last chance to resolve the problem Limited or no Internet connectivity • Malware doesn't want to be removed – It will prevent access to network resources • Disable and enable Wi-Fi – Or enable/disable airplane mode • Restart the device – Clear memory and reload drivers • Perform a malware scan – Find and remove High number of ads • Malware wants to show you advertising – Revenue for each view and click • May be difficult to find – 2019: Ads Blocker for Android promised to remove ads – Actually did the opposite – Once installed, wasn't listed in available apps – FakeAdsBlock malware strain • Run anti-malware utility – Remove the adware Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 44 52 3.5 - Troubleshooting Mobile Device Security (continued) Fake security warnings • The easiest way to get on a phone – Have the user install their own malware • The warnings seem legitimate – They are not actual security issues – Do not install any software • Malware can directly access user data – Steals credit card details, stored passwords, browsing history, text messages • Don't click - If you click, run a malware removal tool Unexpected application behavior • Apps unexpectedly close - Or have excessive delays • App doesn't seem to have all of the normal features – Or included features are not working • High battery utilization – Only when this application is running • Update the app - Get the latest version Leaked personal files • Unauthorized account access – Unauthorized root access – Leaked personal files and data • Determine cause of data breach – Perform an app scan, run anti-malware scan • Factory reset and clean install – This is obviously a huge issue • Check online data sources – Apple iCloud/Apple Configurator, Google Workspace, Microsoft OneDrive – Change passwords 4.1 - Ticketing Systems Ticketing systems • The best way to manage support requests – Document, assign, resolve, report • Usually a responsibility of the help desk – Take the calls and triage • Determine the best next step – Assign the ticket and monitor • There are many different ticketing systems – They're all very similar in function Managing a support ticket • Information gathering – User and device information – Problem description • Applying context – Categorization of the problem – Assign severity – Determine if escalation is required • Clear and concise communication – Problem description, progress notes, resolution details User information • You can't address a person's problem unless you know who has the issue – Add the name of the person reporting the problem • Usually integrated into a name service – Active Directory or similar • May be added automatically – Many issues arrive from a portal or email gateway • Always confirm the contact information – The database may not be up to date © 2022 Messer Studios, LLC Device and description • Device information – Laptop, printer, conference room projector, etc. • Description – One of the most important fields in the ticket – Make the description clear and concise • The description determines the next step – Call back for more information – Associate with another event – Assign to another person Categorization and escalation • Categories – Broad description – Change request, hardware request, problem investigation, hardware failure, onboarding/offboarding, etc. • Severity – Often an established set of standards – Low, medium, high, critical • Escalation levels – Difficult problems can be handled by a specialist – Escalate to a new tier or to a specific group Resolving the issue • Progress notes – Many people may read and/or work on a single ticket – Keep the progress information concise – Document any changes or additional information • Problem resolution – Document the solution – May be referenced later by others with the same problem – A "live" knowledgebase of issues and resolutions Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 45 53 4.1 - Asset Management Asset management • A record of every asset – Laptops, desktops, servers, routers, switches, cables, fiber modules, tablets, etc. • Associate a support ticket with a device make and model – Can be more detailed than a user's description • Financial records, audits, depreciation – Make/model, configuration, purchase date, location, etc. • Add an asset tag – Barcode, RFID, visible tracking number, organization name Asset database • A central asset tracking system – Used by different parts of the organization • Assigned users – Associate a person with an asset – Useful for tracking a system • Warranty – A different process if out of warranty • Licensing – Software costs – Ongoing renewal deadlines Procurement life cycle • The purchasing process – Multi-step process for requesting and obtaining goods and services • Start with a request from the user – Usually includes budgeting information and formal approvals • Negotiate with suppliers – Terms and conditions – Purchase, invoice, and payment – The money part 4.1 - Document Types Acceptable use policies (AUP) • What is acceptable use of company assets? – Detailed documentation – May be documented in the Rules of Behavior • Covers many topics – Internet use, telephones, computers, mobile devices, etc. • Used by an organization to limit legal liability – If someone is dismissed, these are the well-documented reasons why Network topology diagram • Describes the network layout – May be a logical diagram – Can include physical rack locations Compliance • Compliance – Meeting the standards of laws, policies, and regulations • A healthy catalog of rules – Across many aspects of business and life – Many are industry-specific or situational • Penalties - Fines, loss of employment, incarceration • Scope - Domestic and international requirements Splash screens • A message, logo, or graphic shown during startup or login – Can be used for branding or to require compliance • Can be informational – Maintenance notifications or system changes • May be required for legal or administrative purposes – Warnings about system misuse – Information about relying on application data © 2022 Messer Studios, LLC Incident reports • Security policy – An ongoing challenge – Documentation must be available – No questions • Incidents are ongoing – Organizations have formal incident plans • Reports and documentation – Details of any security incident – Create a reference for future incidents Standard operating procedures • Organizations have different business objectives – Processes and procedures • Operational procedures – Downtime notifications, facilities issues • Software installation and upgrades – Custom installation of a software package – Testing, change control • Documentation is the key – Everyone can review and understand the policies On-boarding • Bring a new person into the organization – New user setup checklist • IT agreements need to be signed – May be part of the employee handbook or a separate AUP • Create accounts – Associate the user with groups and departments • Provide required IT hardware – Laptops, tablets, etc. – Preconfigured and ready to go Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 46 54 4.1 - Document Types (continued) Off-boarding • All good things… – End-user termination checklist • This process should be predefined – You don't want to decide how to do things at this point • What happens to the hardware? • What happens to the data? • Account information is usually deactivated – But not always deleted Knowledge base and articles • External sources – Manufacturer knowledge base – Internet communities • Internal documentation – Institutional knowledge – Usually part of help desk software • Find the solution quickly – Searchable archive – Automatic searches with helpdesk ticket keywords 4.2 - Change Management Change management • How to make a change – Upgrade software, patch an application, change firewall configuration, modify switch ports • One of the most common risks in the enterprise – Occurs very frequently • Often overlooked or ignored – Did you feel that bite? • Have clear policies – Frequency, duration, installation process, rollback procedures • Sometimes extremely difficult to implement – It's hard to change corporate culture Rollback plan • The change will work perfectly and nothing will ever go bad – Of course it will • You should always have a way to revert your changes – Prepare for the worst, hope for the best • This isn't as easy as it sounds – Some changes are difficult to revert • Always have backups Sandbox testing • Isolated testing environment – No connection to the real world or production system – A technological safe space • Use before making a change to production – Try the upgrade, apply the patch – Test and confirm before deployment • Confirm the rollback plan – Move everything back to the original – A sandbox can't consider every possibility Responsible staff members • A team effort - Many different parts of the organization • IT team - Implements the change • Business customer - The user of the technology or software • Organization sponsor – Someone's budget is responsible for the process – Or responsible for the profit © 2022 Messer Studios, LLC Change management process • A formal process for managing change – Avoid downtime, confusion, and mistakes • Nothing changes without the process – Complete the request forms – Determine the purpose of the change – Identify the scope of the change – Schedule a date and time of the change – Determine affected systems and the impact – Analyze the risk associated with the change – Get approval from the change control board – Get end-user acceptance after the change is complete Change request forms • A formal process always seems to include a bit of paperwork – This is usually an online system • Nothing gets missed – Easy to manage – Create detailed reports and statistics • Usually a transparent process – Many different groups and people are usually involved Purpose of the change • Why are we doing this? – There needs to be a compelling reason • Application upgrades – New features – Bug fixes – Performance enhancements • Security fixes – Monthly patches and vulnerability fixes • There needs to be a good reason – Changes are costly Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 47 55 4.2 - Change Management (continued) Scope of the change • Determine the effect of the change – May be limited to a single server – Or an entire site • A single change can be far reaching – Multiple applications, Internet connectivity, remote site access, external customer access • How long will this take? – Specific date and time for the change – May have no impact, could have hours of downtime Risk analysis • Determine a risk value - i.e., high, medium, low • The risks can be minor or far-reaching – The "fix" doesn't actually fix anything – The fix breaks something else – Operating system failures – Data corruption • What's the risk with NOT making the change? – Security or application vulnerability – Unexpected downtime to other services Change board and approvals • Go or no go – Lots of discussion • All important parts of the organization are represented – Potential changes can affect the entire company • Some changes have priority – The change board makes the schedule – Some changes happen quickly, some take time • This is the last step – The actual work comes next End-user acceptance • Nothing happens without a sign-off – The end users of the application / network • One of your jobs is to make them successful – They ultimately decide if a change is worth it to them • Ideally, this is a formality – Of course, they have been involved throughout this entire process – There's constant communication before and after 4.3 - Managing Backups Backups • Incredibly important – Recover important and valuable data – Plan for disaster Full Backup • Backup everything – All operating system and user files • This is usually the longest backup process – It's everything in one backup • Might be impractical every day – Long backup times – Lots of storage space Incremental Backup • A full backup is taken first • Subsequent backups contain data changed since the last full backup and last incremental backup – These are usually smaller than the full backup • A restoration requires the full backup and all of the incremental backups • Many different implementations – Total amount of data – Type of backup – Backup media – Storage location – Backup and recovery software – Day of the week Full Backup Full Backup Full Backup Full Backup Full Backup Monday Tuesday Wednesday Thursday Recovery Incremental Incremental Incremental Full Backup Monday © 2022 Messer Studios, LLC Incremental Incremental Incremental Full Backup Tuesday Wednesday Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 48 Thursday Recovery 56 4.3 - Managing Backups (continued) Differential backup • A full backup is taken first – Subsequent backups contain data changed since the last full backup – These usually grow larger as data is changed • A restoration requires the full backup and the last differential backup Synthetic backup • Create a full backup – Without actually performing a full backup • Synthetic backup – The first full backup copies every file – Subsequent full backups are created from previous backups • Can be faster and less bandwidth intensive – The advantage of a full backup – The efficiency of an incremental backup Backup testing • It's not enough to perform the backup – You have to be able to restore • Disaster recovery testing – Simulate a disaster situation – Restore from backup • Confirm the restoration – Test the restored application and data • Perform periodic audits – Always have a good backup – Weekly, monthly, quarterly checks On site vs. off site backups • On site backups – No Internet link required – Data is immediately available – Generally less expensive than off site • Off site backups – Transfer data over Internet or WAN link – Data is available after a disaster – Restoration can be performed from anywhere • Organizations often use both – More copies of the data – More options when restoring © 2022 Messer Studios, LLC Grandfather-father-son (GFS) • Three separate backup rotations – Monthly, weekly, daily • Twelve monthly full backups (grandfather) – A good choice for offsite storage • Four (or five) weekly full backups (father) – Depends on which day of the month is selected • Thirty-one daily incremental or differential backups (son) – Backup any daily changes GFS backup schedule • Choose a rotation – Every organization is different • Grandfather – Last day of every month • Father – Every Monday • Son – Monday through Friday 3-2-1 backup rule • A popular and effective backup strategy – For business or home use • 3 copies of data should always be available – One primary copy and two backups • 2 different types of media should be used – Local drive, tape backup, NAS • 1 copy of the backup should be offsite – Offsite storage, cloud backup Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 49 57 4.4 - Managing Electrostatic Discharge What is electrostatic discharge? • Static electricity – Electricity that doesn't move • Static electricity isn't harmful to computers – It's the discharge that gets them • ESD can be very damaging to computer components – Silicon is very sensitive to high voltages • Feel static discharge: ~3,500 volts – Damage an electronic component: 100 volts or less Controlling ESD • Humidity over 60% helps control ESD – Won't prevent all possible ESD – Keeping an air conditioned room at 60% humidity isn't very practical • Use your hand to "self-ground" – Touch the exposed metal chassis before touching a component – You'll want to unplug the power connection – Always. Really. • Do not connect yourself to the ground of an electrical system! Preventing static discharge • Anti-static strap – Connect your wrist to a metal part of the computer • Anti-static pad – A workspace for the computer • Anti-static mat – A mat for standing or sitting • Anti-static bag – Safely move or ship components Component handling and storage • Try not to touch components directly – Card edges only • Store in an HVAC regulated environment – Between 50 and 80 degrees Fahrenheit or 10 to 27 degrees Celsius • Avoid high humidity – Silica gel packets can help control humidity • Store in the original padded box – Bubble wrap can be a good alternative 4.4 - Safety Procedures WARNING • Power is dangerous • Remove all power sources before working • Don't touch ANYTHING if you aren't sure • Replace entire power supply units – Don't repair internal components • High voltage – Power supplies, displays, laser printers Equipment grounding • Most computer products connect to ground – Divert any electrical faults away from people • Also applies to equipment racks – Large ground wire • Don't remove the ground connection – It's there to protect you • Never connect yourself to the ground of an electrical system – This is not a way to prevent ESD © 2022 Messer Studios, LLC Personal safety • Lifting technique – Lift with your legs, keep your back straight – Don't carry overweight items – You can get equipment to lift • Electrical fire safety – Don't use water or foam – Use carbon dioxide, FM-200, or other dry chemicals – Remove the power source • Safety goggles – Useful when working with chemicals – Printer repair, toner, batteries • Air filter mask – Dusty computers – Printer toner Local government regulations • Health and safety laws – Vary widely depending on your location – Keep the workplace hazard-free • Building codes – Fire prevention, electrical codes • Environmental regulation – High-tech waste disposal Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 50 58 4.5 - Environmental Impacts Disposal procedures • Read your Material Safety Data Sheets (MSDS) – United States Department of Labor, – Occupational Safety and Health Administration (OSHA) – , Index page • Provides information for all hazardous chemicals – Batteries, display devices / CRTs, chemical solvents and cans, toner and ink cartridges • Sometimes abbreviated as Safety Data Sheet (SDS) – Different names in each country MSDS info • Product and company information • Composition / ingredients • Hazard information • First aid measures • Fire-fighting measures • Accidental release / leaking • Handling and Storage • Much more Handling toxic waste • Batteries – Uninterruptible Power Supplies – Dispose at your local hazardous waste facility • Toner – Recycle and reuse – Many printer manufacturers provide a return box – Some office supply companies will provide a discount for each cartridge • Other devices and assets – Refer to the MSDS – Don't throw out without clear directions Room control • Temperature – Devices need constant cooling – So do humans • Humidity level – High humidity promotes condensation – Low humidity promotes static discharges – 50% is a good number • Proper ventilation – Computers generate heat – Don't put everything in a closet Battery backup • Uninterruptible Power Supply – Backup power – Power failures, under-voltage events, surges • UPS types – Standby UPS – Line-interactive UPS – On-line UPS • Features – Auto shutdown, battery capacity, outlets, phone line suppression Surge suppressor • Not all power is "clean" – Self-inflicted power spikes and noise – Storms, power grid changes • Spikes are diverted to ground • Noise filters remove line noise – Decibel (Db) levels at a specified frequency – Higher Db is better Surge suppressor specs • Joule ratings – Surge absorption – 200=good, 400=better – Look for over 600 joules of protection • Surge amp ratings – Higher is better • UL 1449 voltage let-through ratings – Ratings at 500, 400, and 330 volts – Lower is better 4.6 - Privacy, Licensing, and Policies Incident response: Chain of custody • Control evidence - Maintain integrity • Everyone who contacts the evidence – Avoid tampering, use hashes • Label and catalog everything – Seal, store, and protect - Use digital signatures Incident response: First response • Identify the issue - Logs, in person, monitoring data • Report to proper channels – Don't delay – May include internal management and law enforcement • Collect and protect information relating to an event – Many different data sources and protection mechanisms © 2022 Messer Studios, LLC Incident response: Copy of drive • Copy the contents of a disk – Bit-for-bit, byte-for-byte • Remove the physical drive – Use a hardware write-blocker – Preserve the data • Software imaging tools – Use a bootable device • Use hashes for data integrity – Drive image is hashed to ensure that data has not been modified Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 51 59 4.6 - Privacy, Licensing, and Policies (continued) Incident response: Documentation • Document the findings – For Internal use, legal proceedings, etc. • Summary information – Overview of the security event • Detailed explanation of data acquisition – Step-by-step method of the process • The findings - An analysis of the data • Conclusion - Professional results, given the analysis Software licenses • Most software includes a license – Terms and conditions – Overall use, number of copies, and backup options • Valid licenses – Per-seat or concurrent • Non-expired licenses – Ongoing Subscriptions – Annual, three-year, etc. – Use the software until the expiration date Licenses • Personal license – Designed for the home user – Usually associated with a single device – Or small group of devices owned by the same person – Perpetual (one time) purchase • Corporate use license – Per-seat purchase / Site license – The software may be installed everywhere – Annual renewals Open source license • Free and Open Source (FOSS) – Source code is freely available – End user can compile their own executable • Closed source / Commercial – Source code is private – End user gets compiled executable • End User Licensing Agreement (EULA) – Determines how the software can be used Regulating credit card data • Payment Card Industry – Data Security Standard (PCI DSS) – A standard for protecting credit cards • Six control objectives – Build and Maintain a Secure Network and Systems – Protect Cardholder Data – Maintain a Vulnerability Management Program – Implement Strong Access Control Measures – Regularly Monitor and Test Networks – Maintain an Information Security Policy © 2022 Messer Studios, LLC Personal government-issued information • Used for government services and documentation – Social security number, driver license • There may be restrictions on collecting or storing government information - Check your local regulations • U.S. Office of Personnel Management (OPM) – Compromised personal identifiable information – Personnel file information; name, SSN, date of birth, job assignments, etc. – July 2015 - Affected ~21.5 million people PII - Personally identifiable information • Any data that can identify an individual – Part of your privacy policy - How will you handle PII? • Not everyone realizes the importance of this data – It becomes a "normal" part of the day – It can be easy to forget its importance • Attackers use PII to gain access or impersonate – Bank account information – Answer badly-written password-reset questions GDPR - General Data Protection Regulation • European Union regulation – Data protection and privacy for individuals in the EU – Name, address, photo, email address, bank details, posts on social networking websites, medical information, a computer's IP address, etc. • Controls export of personal data – Users can decide where their data goes • Gives individuals control of their personal data – A right to be forgotten, right of erasure • Site privacy policy – Details all of the privacy rights for a user PHI - Protected Health Information • Health information associated with an individual – Health status, health care records, payments for health care, and much more • Data between providers – Must maintain similar security requirements • HIPAA regulations – Health Insurance Portability and Accountability Act of 1996 Data retention requirements • Keep files that change frequently for version control – Files change often - Keep at least a week, perhaps more • Recover from virus infection – Infection may not be identified immediately – May need to retain 30 days of backups • Often legal requirements for data retention – Email storage may be required over years – Some industries must legally store certain data types – Different data types have different storage requirements – Corporate tax information, customer PII, tape backups, etc. Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 52 60 4.7 - Communication Communication skills • One of the most useful skills for the troubleshooter • One of the most difficult skills to master • A skilled communicator is incredibly marketable Avoid jargon • Abbreviations and TLAs – Three Letter Acronyms • Avoid acronyms and slang – Be the translator • Communicate in terms that everyone can understand – Normal conversation puts everyone at ease – Decisions are based on what you say • These are the easiest problems to avoid Maintain a positive attitude • Positive tone of voice – Partner with your customer – Project confidence • Problems can't always be fixed – Do your best – Provide helpful options • Your attitude has a direct impact on the overall customer experience Avoid interrupting • But I know the answer! • Why do we interrupt? – We want to solve problems quickly – We want to show how smart we are • Actively listen, take notes – Build a relationship with the customer – They'll need help again someday – Don't miss a key piece of information – Especially useful on the phone • This skill takes time to perfect – The better you are, the more time you'll save later Clarify customer statements • Ask pertinent questions – Drill-down into the details – Avoid an argument – Avoid being judgmental • Repeat your understanding of the problem back to the customer – Did I understand you correctly? • Keep an open mind – Ask clarifying questions, even if the issue seems obvious – Never make assumptions Setting expectations • Offer different options – Repair or replace • Document everything – No room for questions • Keep everyone informed – Even if the status is unchanged • Follow up afterwards – Verify satisfaction 4.7 - Professionalism Professional appearance • Match the attire of the current environment – Everyone should feel comfortable about their dress • Formal – Some organizations have specific requirements • Business casual – A more relaxed style • Find the right balance – Follow the organization's lead Avoid being judgmental • Cultural sensitivity – Use appropriate professional titles • You're the teacher – Not the warden – Leave insults on the playground • Make people smarter – They'll be better technologists • You're going to make some BIG mistakes – Remember them. © 2022 Messer Studios, LLC Be on time and avoid distractions • Don't allow interruptions – No personal calls, no texting, no Twitter – Don't talk to co-workers • Apologize for delays and unintended distractions – Create an environment for conversation – In person • Open and inviting – Candy bowl can be magical – On the phone – Quiet background, clear audio – Stay off the speakerphone Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 53 61 4.7 - Professionalism (continued) Difficult situations • Technical problems can be stressful • Don't argue or be defensive – Don't dismiss – Don't contradict • Diffuse a difficult situation with listening and questions – Relationship-building • Communicate – Even if there's no update • Never take the situation to social media Maintain confidentiality • Privacy concerns – Sensitive information – Both professional and private – On the computer, desktop, or printer • Professional responsibilities – IT professionals have access to a lot of corporate data • Personal respect – Treat people as you would want to be treated 4.8 - Scripting Languages Scripting languages • Automate with the right tools – The script should match the requirement • May be specific to a task or operating system – Your choices may already be limited • You will probably learn more than one of these – An important skill for any technician Batch files • .bat file extension – Scripting for Windows at the command line – Legacy goes back to DOS and OS/2 Windows PowerShell • Command line for system administrators – .ps1 file extension – Included with Windows 8/8.1 and 10 • Extend command-line functions – Uses cmdlets (command-lets) – PowerShell scripts and functions – Standalone executables • Automate and integrate – System administration – Active Domain administration Microsoft Visual Basic Scripting Edition • VBScript – .vbs file extension • General purpose scripting in Windows – Back-end web server scripting – Scripting on the Windows desktop – Scripting inside of Microsoft Office applications © 2022 Messer Studios, LLC Shell script • Scripting the Unix/Linux shell – Automate and extend the command line • Starts with a shebang or hash-bang #! – Often has a .sh file extension JavaScript • Scripting inside of your browser – .js file extension • Adds interactivity to HTML and CSS – Used on almost every web site • JavaScript is not Java – Different developers and origins – Very different use and implementation Python • General-purpose scripting language – .py file extension • Popular in many technologies – Broad appeal and support #!/bin/sh // Add the first input string INPUT_STRING=hello // Keep looping if the string isn't equal to bye while ["$INPUT_STRING" != "bye"] do echo "Please type something in (bye to quit)" read INPUT_STRING echo "You typed: $INPUT_STRING" done Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 54 62 4.8 - Scripting Use Cases Basic automation • Automate tasks – You don't have to be there – Solve problems in your sleep – Monitor and resolve problems before they happen • The need for speed – The script is as fast as the computer – No typing or delays – No human error • Automate mundane tasks – You can do something more creative Restarting machines • Turning it off and back on again – An important task • Application updates – Some apps require a system restart • Security patches – Deploy overnight and reboot the system • Troubleshooting – The once-a-day restart – You may not have physical access Remapping network drives • Shared network drives – The link between the user and their data • A common task during startup – Login scripts provide the connection • Automate software changes – Map a drive to the repository • Add or move user data – Automate the process Application installations • Install applications automatically – Don't walk a flash drive to every computer – Many applications have an automated installation process – Scripting can turn this into a hands-off process • On-demand or automatic installation scripts – Map the application installation drive – Install the application without user prompts – Disconnect the drive – Restart the system Automated backups • Usually performed at night or during off-hours – Get a copy of all important data • Time consuming – File systems, network connections • Script an automated backup process – Works while you sleep – Don't have to think about it © 2022 Messer Studios, LLC Information gathering • Get specific information from a remote device – Monitoring and reporting • Performance monitoring – Confirm proper operation of a device • Inventory management – Check the hardware or software configuration • Security and vulnerability checks – Check for certain application or library versions – Plan for the latest patches Initiating updates • Nothing ever stays the same – Constant changes and updates • Operating systems – New features – Security patches • Device drivers – Bug fixes – New hardware or OS support • Applications – New version rollouts Other scripting considerations • Unintentionally introducing malware – Make sure you know what you're installing • Inadvertently changing system settings – Test all updates – Track the file and registry changes • Browser or system crashes – Mishandling of resources – A single character in a script can have unintended consequences – Always have a backup – Always test before deployment Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 55 63 4.9 - Remote Access Remote desktop connections • Share a desktop from a remote location – It's like you're right there • RDP (Microsoft Remote Desktop Protocol) – Clients for Mac OS, Linux, and others as well • VNC (Virtual Network Computing) – Remote Frame Buffer (RFB) protocol – Clients for many operating systems – Many are open source • Commonly used for technical support – And for scammers Remote desktop security • Microsoft Remote Desktop – An open port of tcp/3389 is a big tell – Brute force attack is common • Third-party remote desktops – Often secured with just a username and password – There's a LOT of username/password re-use • Once you're in, you're in – The desktop is all yours – Easy to jump to other systems – Obtain personal information, bank details – Make purchases from the user's browser VPNs • Virtual Private Networks – Encrypted (private) data traversing a public network • Concentrator – Encryption/decryption access device – Often integrated into a firewall • Many deployment options – Specialized cryptographic hardware – Software-based options available • Used with client software – Sometimes built into the OS VPN security • VPN data on the network is very secure – The best encryption technologies • Authentication is critical – An attacker with the right credentials can gain access • Almost always includes multi-factor authentication (MFA) – Require more than just a username and password SSH (Secure Shell) • Encrypted console communication - tcp/22 • Looks and acts the same as Telnet - tcp/23 SSH security • The network traffic is encrypted – Nothing to see in the packets • Authentication is a concern – SSH supports public/private key pair authentication • Certain accounts should be disabled in SSH – For example, root – Consider removing all password-based authentication • Limit access to SSH by IP address – Configure a local firewall or network filter RMM • Managed Service Providers (MSP) – Many customers and systems to monitor – Many different service levels • Remote Monitoring and Management (RMM) – Manage a system from a remote location • Many features – Patch operating systems – Remote login – Anomaly monitoring – Hardware/software inventory Client-to-site VPN • On-demand access from a remote device – Software connects to a VPN concentrator • Some software can be configured as always-on Corporate Network © 2022 Messer Studios, LLC Internet VPN Concentrator Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 56 Remote User 64 4.9 - Remote Access (continued) RMM security • A popular attack point • The RMM has a great deal of information and control • Access should be limited – Don't allow everyone to connect to the RMM service • Auditing is important – Know who's connecting to which devices and what they're doing Microsoft Remote Assistance (MSRA) • Get access to a remote user's desktop – No firewall configurations or port forwarding required • User makes a request – Sends an invitation with the details • Technician connects – Uses the password in the request • Replaced by Quick Assist in Windows 10 – The latest version of MSRA © 2022 Messer Studios, LLC MSRA/Quick Assist security • No ongoing Remote Desktop service required – Avoids unintended access – No port forwarding • Email with invitation details is always a concern – Consider using voice communication • Perhaps a bit too easy to use – Social engineering can be an issue Third-party tools • Screen-sharing – See and control a remote device – GoToMyPC, TeamViewer • Video-conferencing – Multi-user meetings with video and audio – Zoom, WebEx • File transfer – Store and share documents in the cloud – Dropbox, Box.com, Google Drive • Desktop management – Manage end-user devices and operating systems – Citrix Endpoint Management, ManageEngine Desktop Central Professor Messer's CompTIA 220-1102 A+ Course Notes - Page 57 65 66 Continue your journey on ProfessorMesser.com: Professor