CIS 101B Lesson Plan

|  |  |
| --- | --- |
| **Week 4 Class 8** **Tuesday 1-5:00 PM**  **Tuesday 6-10:00 PM** | **Chapter 12 – Security (Chapter 12.13 only)** |

# Hands On

**Turn on BIOS security on the lab computers, add a boot password, research how to clear BIOS password, jumper on motherboard  
LastPass   
Go to grc.com, check out Perfect Password, and Shields Up  
Use @Active Password reset tool, to simply clear a password  
Create users, change user passwords, disable user  
Disable USB storage media with a local policy:  
In the Start -** **Search - GPEDIT.MSC.  
In the left field, open Computer Configuration > Administrator Templates > System > Removable Storage Access.  
Set all these to Enable  
Removable Disk: Deny execute access  
Removable Disk: Deny read access  
Removable Disk: Deny write access  
Run GPUPDATE /FORCE**

12.13 Security Troubleshooting

12.13.2 Network Security Threat Facts

Common network attacks that you should be aware of include the following:

|  |  |
| --- | --- |
| **Attack** | **Description** |
| Man-in-the-middle | A *man-in-the-middle* attack is used to intercept information passing between two communication partners. With a man-in-the-middle attack:   * An attacker inserts himself in the communication flow between the client and server. The client is fooled into authenticating to the attacker. * Both parties at the endpoints believe they are communicating directly with each other, while the attacker intercepts and/or modifies the data in transit. The attacker can then authenticate to the server using the intercepted credentials.   Man-in-the-middle attacks are commonly used to steal credit card numbers, online bank credentials, as well as confidential personal and business information. |
| TCP/IP (session) hijacking | *TCP/IP hijacking* is an extension of a man-in-the-middle attack where the attacker steals an open and active communication session from a legitimate user.   * The attacker takes over the session and cuts off the original source device. * The TCP/IP session state is manipulated so that the attacker is able to insert alternate packets into the communication stream. |
| HTTP (session) hijacking | *HTTP (session) hijacking* is a real-time attack in which the attacker hijacks a legitimate user's cookies and uses the cookies to take over the HTTP session. |
| Replay attack | In a *replay attack*, the attacker uses a protocol analyzer or sniffer to capture authentication information going from the client to the server. The attacker then uses this information to connect at a later time and pretend to be the client. |
| Phishing | A *phishing* scam employs an email pretending to be from a trusted organization, asking to verify personal information or send a credit card number. In a phishing attack:   * A fraudulent message (that appears to be legitimate) is sent to a victim. * The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and websites look almost identical to legitimate websites they are trying to imitate. * The fraudulent website requests that the victim provide sensitive information, such as an account username and password.   Common phishing scams include:   * A Rock Phish kit uses a fake website that imitates a real website (such as banks, PayPal�, eBay�, or Amazon�). Phishing emails direct victims to the fake website where they enter account information. A single server can host multiple fake sites using multiple registered DNS names. These sites can be set up and taken down rapidly to avoid detection. * A *Nigerian scam*, also known as a *419 scam*, involves email which requests a small amount of money to help transfer funds from a foreign country. For their assistance, the victim is promised a reward for a much larger amount of money that will be sent at a later date. * In *spear phishing*, attackers gather information about the victim, such as identifying which online banks they use. They then send phishing emails for the specific bank that the victim uses. * *Whaling* is another form of phishing that is targeted to senior executives and high profile victims. * *Vishing* is similar to phishing but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. The term is a combination of *voice* and *phishing*.   To protect against phishing:   * Check the actual link destination within emails to verify that they go to the correct URL and not a spoofed one. * Do not click on links in emails. Instead, type the real bank URL into the browser. * Verify that HTTPS is used when going to e-commerce sites. HTTPS requires a certificate that matches the server name in the URL that is verified by a trusted CA. You can also look for the lock icon to verify that HTTPS is used. If the website is using an invalid certificate, then an invalid SSL certificate warning appears when you try to access the website. * Implement phishing protections within your browser. |
| Zombie | A *zombie* is a computer that is infected with malware that allows remote software updates and control by a command and control center called a *zombie master*. A zombie:   * Is also known as a *bot* (short for robot) * Is frequently used to aid spammers * Can commit *click fraud*. The Internet uses an advertising model called *pay per click* (PPC). With PPC, ads are embedded on a website by the developer. The advertiser then pays the website owner for each click the ad generates. Zombie computers can imitate a legitimate ad click, generating fraudulent revenue. * Can be used to perform denial of service attacks |
| Botnet | A *botnet* refers to a group of zombie computers that are commanded from a central control infrastructure. A botnet is:   * Under a command and control infrastructure where the zombie master (also known as the *bot herder*) can send remote commands to order all the bots they control to perform actions * Capable of performing distributed denial of service attacks * Detected through the use of firewall logs to determine if a computer is acting as a zombie and participating in external attacks |
| Zero day | A *zero day* attack (also known as a *zero hour* or *day zero* attack) is an attack that exploits computer application vulnerabilities before they are known and patched by the application's developer. |

*Spoofing* is used to hide the true source of packets or to redirect traffic to another location. Spoofing attacks:

* Use modified source and/or destination addresses in packets
* Can include site spoofing that tricks users into revealing information

Network attacks may also falsify source or destination addresses for network communications. This is called *spoofing*. Common methods of spoofing are listed in the table below:

|  |  |
| --- | --- |
| **Attack** | **Description** |
| IP spoofing | IP spoofing changes the IP address information within a packet. It can be used to:   * Hide the origin of the attack by spoofing the source address * Amplify attacks by sending a message to a broadcast address and then redirecting responses to a victim who is overwhelmed with responses |
| MAC spoofing | MAC spoofing occurs when an attacking device spoofs the MAC address of a valid host currently in the MAC address table of the switch. The switch then forwards frames destined for that valid host to the attacking device. This can be used to bypass:   * A wireless AP with MAC filtering on a wireless network * Router ACLs * 802.1x port-based security |
| ARP spoofing | ARP spoofing (also known as ARP *poisoning*) uses spoofed ARP messages to associate a different MAC address with an IP address. ARP spoofing can be used to perform a man-in-the-middle attack as follows:   1. When an ARP request is sent by a client for the MAC address of a device, such as the default gateway router, the attacker's system responds to the ARP request with its own MAC address. 2. The client receives the spoofed ARP response and uses that MAC address when communicating with the destination host. For example, packets sent to the default gateway are sent instead to the attacker. 3. The attacker receives all traffic sent to the destination host. The attacker can then forward these packets on to the correct destination using its own MAC address as the source address.   ARP spoofing can also be used to perform Denial of Service (DoS) attacks by redirecting communications to fake or nonexistent MAC addresses. |

Countermeasures to prevent spoofing use:

* Firewall and router filters to prevent spoofed packets from crossing into or out of your private secured network. Filters will drop any packet suspected of being spoofed.
* Certificates to prove identity
* Reverse DNS lookup to verify the source email address
* Encrypted communication protocols, such as IPsec
* Ingress and egress filters to examine packets and identify spoofed packets. Ingress filters examine packets coming into the network, while egress filters examine packets going out of the network. Any packet suspected of being spoofed on its way into or out of your network will be dropped.

12.13.3 Security Troubleshooting Facts

As a PC technician, there are a variety of security issues that you must deal with each day. Several common workstation security issues and practices are discussed here.

The key to troubleshooting security issues is to do everything you can to prevent them from occurring in the first place. Consider the following preventative measures:

|  |  |
| --- | --- |
| **Preventative Measure** | **Description** |
| Implement malware prevention | Do the following:   * Install antimalware on all systems to search for malware, viruses, worms, trojans, and rootkits. * Enable automatic definition updates on your anti-malware software. * Configure frequent quick malware scans along with less frequent full system scans. * Implement anti-spam measures. This can be done using anti-spam software on each individual workstation. However, it's usually advantageous to implement an anti-spam appliance that filters email messages for your entire organization. |
| Implement browser security | Do the following:   * Disable pop-ups on all web browsers. Pop-ups can covertly install malware or redirect users to malicious websites. Enable pop-ups only for legitimate sites that require them. * Override automatic cookie handling. Configure your browser to prompt you before allowing cookies. * Disable third-party browser extensions. * Disable sounds in web pages. |
| Configure automatic updates | Enable automatic updates for all operating systems. |
| Maintain awareness | Stay current by subscribing to security alerts offered by many security software vendors. |
| Educate end users | Educate users about current security threats and how to respond to them. For example, teach them to:   * Use strong passwords. This includes email account passwords as well as workstation account passwords. * Distrust anything coming from the web: Don't click on anything just because the site says you must do so. * View email with suspicion. A reputable company in the modern world will not send an email asking users to respond with personal information. Any message that does is using phishing to gather personal information. * Recognize social engineering attempts and respond appropriately. |

As a PC technician, there are many key security threats that you need to be aware of:

|  |  |
| --- | --- |
| **Issue** | **Description** |
| Spam | *Spam* may or may not be malicious in nature. However, it wastes time, network bandwidth, and storage space as many organizations are required by law in the United States to retain all email communications for a period of time.  The best way to combat spam is to implement an anti-spam appliance that is placed between your network and the Internet. The appliance scans all emails as they enter the organization and quarantines anything deemed to be spam. |
| Phishing emails | *Phishing* is the process used by attackers to acquire sensitive information such as passwords, credit card numbers, and usernames by masquerading as a trustworthy entity. Phishing e-mails are drafted such that they appear to have come from a legitimate organization, such as banking, social media, or e-commerce websites. They convince the user to click a link that takes them to a malicious website (that looks exactly like the legitimate web site) where they are tricked into revealing sensitive information.  To detect phishing e-mails, train users to recognize their key characteristics:   * The source address of the message may not match the domain of the company it claims to be coming from. * The message tries to create a sense of urgency. For example, it may warn that your bank account will be frozen, that your credit card has been stolen, or that you will be subject to arrest if you don't follow the instructions in the message. * The hyperlinks in the message go to websites that are not associated with the organization the message claims to be coming from. If you hover your mouse over a link (without clicking it) you can see where the link actually leads. If it isn't pointing to the organization's URL, there�s a pretty good chance the message is an exploit. |
| Hijacked email | To hijack an email account, attackers use password hints set up by the user to try to gain access to the user's email account. Users should not use personal information such as their birthplace or mother's maiden name. This information is relatively easy to obtain using social media. Once an account has been hijacked, the attacker can use it to propagate spam or malware to every contact in the user's address book. |
| Pharming | *Pharming* redirects one website's traffic to another, bogus website that is designed to look like the real website. Once there, the attacker tricks the user into supplying personal information, such as bank account and PIN numbers. Pharming works by resolving legitimate URLs to the IP address of malicious websites. This is typically done using one of the following techniques:   * Changing the hosts file on a user's computer * Poisoning a DNS server * Exploiting DHCP servers to deliver the IP address of malicious DNS servers in DHCP leases. |
| Rogue anti-virus | Rogue anti-virus exploits usually employ a pop-up in a browser that tells the user their computer is infected with a virus and that they must click a link to clean it. Sometimes this exploit is used to trick users into paying for worthless software they don't need. However, it also is frequently used to deploy malware on the victim's computer. |
| Cookies | Cookies are data files placed on a client system by a web server for retrieval at a later time. Cookies are primarily used to track the client. By default, cookies can only be retrieved by the server that set them. The cookies themselves are fairly benign; however, cookies can be exploited by an attacker to steal a client's session parameters. This allows the attacker to impersonate the client system and hijack the session, potentially exposing sensitive information. |
| Browser history | The browser history and its cache contain information that an attacker can exploit. If an attacker can gain access to the cash or the browser history, they can learn things about the end user such as:   * The email service they use * The bank where they keep their accounts * Where they shop   An attacker can exploit this information to conduct other attacks, such as stealing cookies or sending phishing emails. |

As a PC technician, you should be familiar with the symptoms of a malware infection. Look for the following:

* Slow computer performance
* Internet connectivity issues
* Operating system lock ups
* Windows update failures
* Renamed system files
* Disappearing files
* Changed file permissions
* Access denied errors

You should frequently check your logs in Event Viewer to identify suspicious behaviors.

If you suspect a system has been infected, you should observe the following best practices to remove the malware:

* Identify the malware symptoms.
* Quarantine the infected system.
* Disable system restore to prevent the malware from being saved in a restore point (and to prevent an uninfected restore point from being potentially deleted to make room for a new restore point).
* Remediate the infected system.
* Update the antimalware definitions.
* Scan for and remove the malware. Some malware can be removed while the system is running normally. However, some malware can only be removed while in Safe Mode or in the Pre-Installation Environment.
* Schedule future scans and updates.
* Re-enable system restore and create a new restore point.
* Educate end user to prevent the infection from happening again.