## LESSON: Network Attacks & Mitigations

## Primer For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

* Checking with the students to see if they have any questions or need further clarification from any subject from the last class “Virtual Private Networks (VPN)”.
* Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
* Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
* For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regard to the lesson.
* Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
* At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.
* Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.

### Summary

In this lesson, learners will explore network attacks, their diverse consequences, and classifications. They'll understand the modes of operation, including interception, interruption, modification, and fabrication, as well as the effects, such as disruption, destruction, information disclosure, and access or privilege escalation. Additional aspects include attack sources (internal or external) and targets (host-based, network-based, or application-based). Specific attack methods, such as MAC spoofing, ARP poisoning, and CAM table overflow, will be covered alongside mitigation strategies. Port security on network switches, VLAN hopping, switch spoofing prevention, double tagging prevention, IP spoofing, Smurf attack, routing table poisoning, ping of death, ICMP redirect attack, teardrop attack, OSPF spoofing, TCP reset attack, SYN flood, fraggle attack, land attack, session hijacking, SSL/TLS attacks (BEAST, CRIME, POODLE), DNS spoofing, DHCP attacks, and NTP attacks will be discussed in detail, providing learners with comprehensive knowledge about network attacks and how to defend against them.

### Objectives

* Identify network attacks and their impact.
* Explain where network attacks occur.
* Compare and contrast passive vs active attacks.
* Define classification by mode of operation and effect.
* Explain the attacks: Interception attacks/information disclosure, interruption/disruption, modification/injection, and fabrication/access or privilege escalation.
* Define attack source and attack targets.
* Explain the attacks: MAC spoofing, ARP poisoning, and CAM table overflow.
* Identify port security configuration and setup.
* Explain CDP/LLDP reconnaissance and VLAN hopping
* Illustrate switch spoofing prevention and double tagging prevention.
* Explain IP spoofing, Smurf attack, routing table poisoning, ping of death, ICMP redirect attack, teardrop attack, and OSPF spoofing.
* Explain the TCP reset attack, SYN flood, fraggle attack, and land attack.
* Explain SSL/TLS attacks, DNS spoofing, DHCP attacks, and NTP attacks.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Network Attacks & Mitigations | * Introduce learners to the importance of network attacks and mitigations in cybersecurity. |
| 5 min | **Real World Scenario:**  Network Attacks & Mitigations | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Cyber Uncovered:**  Understanding Network Attacks | * Begin the lesson by explaining the concept of network attacks and their malicious intent. * Emphasize the importance of understanding these attacks in today's digital age. * Discuss the potential consequences of network attacks, including financial loss, data breaches, operational disruption, reputation damage, and legal repercussions. * Explore the different layers of networking where attacks can occur, ranging from the physical layer to the application layer. * Provide examples of common attack points, such as network connections, devices, endpoints, and cloud services. * Introduce the broad categories for classifying network attacks: Passive vs. active attacks. * Discuss passive attacks that involve intercepting data without alteration, including eavesdropping and traffic analysis. * Explain active attacks that introduce or alter data to cause harm, such as denial-of-service (DoS) and man-in-the-middle (MITM) attacks. * Provide more detailed information about denial-of-service attacks, discussing their objectives, classification, and attack flow. * Explore known tools used for DoS attacks and mitigation strategies. * Provide an in-depth understanding of man-in-the-middle attacks, including their objectives and how attackers intercept and alter communication. * Discuss known tools used for MITM attacks and mitigation techniques. * Conclude the lesson by emphasizing the importance of implementing mitigation strategies to protect against network attacks. * Discuss specific strategies mentioned in the content, such as encryption, session timeout policies, and secure protocols. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Cyber Uncovered:**  Active Network Attacks | * Begin the lesson by introducing the classification of network attacks based on their mode of operation. * Explore the four modes of operation, including interception, interruption, modification, and fabrication, and provide real-world examples of each. * Discuss network attack classifications based on their effects and their significance in understanding the impact of attacks. * Present the categories of disruptive, destructive, information disclosure, and access or privilege escalation, and elaborate on their characteristics. * Move on to the connection between interception attacks and information disclosure and explain how some interception attacks can lead to interruption or modification. * Illustrate this with examples like eavesdropping and man-in-the-middle (MITM) attacks. * Shift the focus to interruption attacks and their potential outcomes, from disruption to equipment destruction. * Discuss real-life examples such as ping of death and Smurf attack. * Proceed to explore modification/injection attacks and the potential consequences, highlighting attacks like DNS poisoning and ARP poisoning. * Conclude by discussing fabrication attacks and their role in achieving access or privilege escalation or information disclosure. * Finally, introduce additional aspects to consider in relation to network attacks, such as attack sources (external and internal) and attack targets (host-based, network-based, and application-based). * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20-25 min | **Cyber Uncovered:**  Data Link / OSI Layer 2 Attacks | * Begin the lesson by introducing the concept of MAC spoofing, explaining its objectives, classification, and how attackers alter MAC addresses. * Illustrate the attack flow and use real-world examples to help students understand how MAC spoofing works. * Move on to ARP poisoning, discussing objectives, classification, and how attackers manipulate ARP messages to redirect network traffic. * Provide insights into the attack flow of ARP poisoning and introduce mitigation strategies, such as static ARP tables and ARP inspection. * Transition to CAM table overflow, describing the attack's objectives, classification, and how it disrupts legitimate traffic on a switch. * Explain the attack flow of CAM table overflow and recommend mitigation steps like port security and CAM table monitoring. * Shift the focus to port security, outlining its role in restricting device access based on MAC addresses and its benefits. * Discuss the two ways of configuring port security (Manual and Sticky) and how it reacts to violations. * Conclude this section by presenting port security setup recommendations and violation modes. * Proceed to CDP/LLDP reconnaissance, explaining the objectives, classification, and the use of CDP/LLDP for gathering device information. * Describe the attack flow for CDP/LLDP reconnaissance and introduce mitigation techniques, including disabling CDP/LLDP on unnecessary ports and implementing port security. * Cover VLAN hopping, detailing its objectives and classification, and explain how attackers gain unauthorized access to different VLANs. * Present the attack flow, including methods used by attackers, and mention mitigation strategies, such as disabling auto trunking and implementing VLAN access control lists. * Conclude the lesson with a discussion on switch spoofing prevention and double tagging prevention to safeguard against these attacks. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 25 min | **Lab:**  Data Link / OSI Layer 2 Attacks | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Cyber Uncovered:**  Network / OSI Layer 3 Attacks | * Begin the lesson by explaining the disclaimer to students, highlighting that while some of these attacks are not new and have been mitigated in modern operating systems, they can still serve as critical examples of attack characteristics that persist in modern threats. * Introduce IP spoofing, detailing its objectives, classification, and the concept of falsifying source IP addresses. Explain how this technique can conceal an attacker's identity and its use in other attacks like DoS. * Discuss the attack flow for IP spoofing, where an attacker crafts packets with false source IPs, and how target systems handle these packets. * Present common tools like hping3 and Scapy for IP spoofing and explore mitigation strategies, including ingress and egress filtering on border routers and the use of anomaly-based intrusion detection systems. * Move on to the Smurf attack, explaining its objectives and classification. Describe how the attacker floods a network with ICMP echo request packets, using a spoofed source IP to overwhelm the target with ICMP echo reply packets. * Detail the attack flow for Smurf attacks, where an attacker sends ICMP echo requests to a broadcast address and all devices in the broadcast domain reply, causing the target to become overwhelmed. * Discuss tools like smurf6 and LOIC, which are commonly used for Smurf attacks, and recommend mitigation steps, such as disabling IP directed broadcasts on routers and configuring intrusion detection systems to identify ICMP floods. * Transition to routing table poisoning, outlining its objectives and classification. Explain how attackers introduce false routing information to disrupt network operations. * Present the attack flow for routing table poisoning, where attackers send false routing updates to routers and routers update their tables with incorrect paths. * Discuss tools, like Quagga and BIRD, that attackers use for routing table poisoning and provide mitigation strategies, including the use of routing authentication protocols and route filtering and verification. * Cover the ping of death attack, detailing its objectives and classification, and explain how attackers send oversized and malformed ICMP echo request packets to crash or freeze target systems. * Describe the attack flow for the ping of death, where an attacker sends oversized ICMP packets that older, vulnerable systems fail to handle. * Discuss tools like hping3 and modified ping utilities used for the ping of death and provide mitigation recommendations, such as updating and patching systems and configuring firewalls to block or limit ICMP traffic. * Proceed to the ICMP redirect attack, explaining its objectives and classification. Describe how attackers send fake ICMP redirect packets to alter the target's routing table. * Detail the attack flow for ICMP redirect attacks, where an attacker sends ICMP redirect packets to the target, prompting the target to modify its routing table. * Present tools like hping3 and Scapy that attackers use for ICMP redirect attacks and introduce mitigation techniques, including disabling ICMP redirect acceptance on hosts and monitoring for unusual traffic patterns. * Move on to the teardrop attack, outlining its objectives and classification. Explain how attackers send fragmented IP packets with overlapping, oversized payloads to confuse and crash the target. * Describe the attack flow for the teardrop attack, where an attacker sends overlapping IP fragments to the target, causing the system to struggle with reassembly. * Discuss tools like Scapy with custom scripts used for teardrop attacks and recommend mitigation strategies, such as updating and patching operating systems and deploying IDS/IPS to detect and block malicious fragmented packets. * Conclude the lesson by discussing OSPF spoofing, detailing its objectives and classification. Explain how attackers send forged OSPF packets to manipulate routing tables or disrupt network operations. * Present the attack flow for OSPF spoofing, where attackers craft and send malicious OSPF updates to routers, leading to adjustments in routing tables. * Mention tools like Quagga, which are commonly used for OSPF spoofing, and provide mitigation approaches, including implementing OSPF authentication and using static OSPF neighbors. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 5 min | **Pulse Check** | * After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other. |
| 15-20 min | **Cyber Uncovered:**  Transport / OSI Layer 4 Attacks | * Begin the lesson by introducing the TCP reset attack, explaining its objectives, classification, and the concept of sending forged TCP reset packets to disrupt established connections without consent or knowledge. * Discuss the attack flow for TCP reset attacks, where an attacker monitors or intercepts a TCP session and sends spoofed TCP reset packets to one or both parties, leading to the termination of the connection. * Present common tools like tcpkill and hping3, which are used for TCP reset attacks, and explore mitigation strategies, including the encryption of TCP sessions and the deployment of anomaly-based intrusion detection systems. * Transition to the SYN flood attack, explaining its objectives and classification. Describe how attackers rapidly send a large number of SYN packets, often with spoofed IP addresses, to overwhelm a target system's resources and prevent legitimate users from establishing connections. * Detail the attack flow for SYN flood attacks, where attackers send a barrage of SYN requests and the target allocates resources awaiting handshake completion. With enough SYN requests, server resources become exhausted. * Discuss tools like LOIC and hping3, that attackers use for SYN flood attacks, and provide mitigation recommendations, such as configuring firewalls and routers to limit the rate of SYN packets. * Move on to the fraggle attack, outlining its objectives and classification. Explain how this attack is similar to the Smurf attack but uses UDP echo packets to flood a target network. * Describe the attack flow for fraggle attacks, where attackers send spoofed UDP echo traffic to broadcast addresses, generating a flood of traffic towards the spoofed IP, the victim. * Discuss tools like Scapy, with custom scripts used for fraggle attacks, and recommend mitigation strategies, such as disabling UDP echo and chargen services and filtering broadcast traffic at the router level. * Proceed to the land attack, detailing its objectives and classification. Explain how this attack targets systems with TCP packets that have the same source and destination IP address and port number. * Describe the attack flow for land attacks, where attackers send spoofed TCP SYN packets with matching source and destination IPs and ports, causing vulnerable systems to lock up or crash. * Discuss tools like Visual Packet Builder, that attackers use for land attacks, and provide mitigation approaches, including updating and patching operating systems and using IDS/IPS to detect and block land attack signatures. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Cyber Uncovered:**  Transport to Application / OSI Layers 5-7 Attacks | * Start the lesson with an overview of session hijacking, explaining that it involves the unauthorized takeover of user sessions to gain access to protected resources. * Explain that session hijacking belongs to the classification of interception and outline its objective: Taking control of user sessions. * Explain the attack flow, where an attacker obtains a session token through network sniffing or prediction techniques and then uses it to assume control over the user's session. * Mention known tools like Juggernaut and Hunt, which are used for session hijacking. * Present mitigation strategies, emphasizing the importance of using secure, encrypted protocols (e.g., HTTPS), implementing session timeout policies, and employing random, complex session token generation to prevent session hijacking. * Move on to SSL/TLS attacks, mentioning examples like BEAST, CRIME, and POODLE. Explain that these attacks target SSL and TLS protocols to exploit vulnerabilities and intercept or modify encrypted data. * Classify SSL/TLS attacks as modification/injection/interruption and describe the objectives of exploiting protocol vulnerabilities. * Detail the attack flow, where attackers position themselves between the victim and the server, identify protocol vulnerabilities, and exploit them. * Provide high-level information about custom scripts developed for each SSL/TLS attacks. * Offer mitigation recommendations for specific SSL/TLS attacks: Use TLS 1.2 or newer for BEAST, disable TLS compression for CRIME, and disable SSLv3 support for POODLE. * Proceed to DNS spoofing, explaining that it's an attack involving false DNS responses to redirect traffic to an attacker-controlled IP address. * Describe the objectives, classification as modification/injection, and the attack flow, where the attacker poisons DNS caches and responds with false IP addresses. * Mention tools like Dnsmasq and Ettercap, which are used for DNS spoofing. * Provide mitigation strategies, emphasizing the use of DNSSEC (DNS Security Extensions) and secure DNS resolvers to prevent DNS spoofing. * Transition to DHCP attacks, which involve targeting the Dynamic Host Configuration Protocol to disrupt, intercept, or redirect network traffic. * Discuss the objectives, classification as interruption/fabrication, and the attack flow where the attacker deploys a rogue DHCP server or exhausts IP addresses in the DHCP pool. * Mention tools like Yersinia and DHCPig. * Suggest mitigation methods, such as enabling DHCP snooping on switches and filtering DHCP traffic on untrusted interfaces. * Conclude by introducing NTP attacks, explaining that they exploit the Network Time Protocol for various purposes, including DDoS amplification and manipulating time synchronization. * Describe the objectives and classification of NTP attacks as interruption. * Explain the attack flow for both disruption and reflection attacks, where attackers send malformed or falsified NTP traffic or requests. * Mention known tools like ntpq and Metasploit NTP modules. * Provide mitigation strategies, including configuring NTP servers to ignore requests from outside their designated network and ensuring regular updates and security for NTP software. * Briefly mention NTP authentication and the development of the more secure NTS standard, which uses TLS. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 15 min | **Lesson Closure** | * For this first lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as Understanding Network Attacks, Passive and Active Attacks, and also OSI layer attacks Layer 2-7. * Students should review this information prior to moving to the next module. * Recommend that the students read-ahead and come prepared for the next lesson. * Q&A |

### 