1. CCNA Security

Lab - Researching Network Attacks and Security Audit Tools/Attack Tools

1. Objectives

Part 1: Researching Network Attacks

* Research network attacks that have occurred.
* Select a network attack and develop a report for presentation to the class.

Part 2: Researching Network Security Audit Tools and Attack Tools

* Research network security audit tools.
* Select a tool and develop a report for presentation to the class.

1. Background / Scenario

Attackers have developed many tools over the years to attack and compromise networks. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users access to resources. When network resources are inaccessible, worker productivity can suffer, and business income may be lost.

To understand how to defend a network against attacks, an administrator must identify network vulnerabilities. Specialized security audit software, developed by equipment and software manufacturers, can be used to help identify potential weaknesses. These same tools used by individuals to attack networks can also be used by network professionals to test the ability of a network to mitigate an attack. After the vulnerabilities are discovered, steps can be taken to help protect the network.

This lab provides a structured research project that is divided into two parts: Researching Network Attacks and Researching Security Audit Tools. Inform your instructor about which network attack(s) and network security audit tool(s) you have chosen to research. This will ensure that a variety of network attacks and vulnerability tools are reported on by the members of the class.

In Part 1, research network attacks that have occurred. Select one of these attacks and describe how the attack was perpetrated and the extent of the network outage or damage. Next, investigate how the attack could have been mitigated, or what mitigation techniques might have been implemented to prevent future attacks. Finally, prepare a report based on the form included in this lab.

In Part 2, research network security audit tools and attack tools. Investigate one that can be used to identify host or network device vulnerabilities. Create a one-page summary of the tool based on the form included within this lab. Prepare a short (5–10 minute) presentation to give to the class.

You may work in teams of two, with one person reporting on the network attack and the other reporting on the tools. All team members deliver a short overview of their findings. You can use live demonstrations or PowerPoint, to summarize your findings.

1. Required Resources

* Computer with Internet access for research
* Presentation computer with PowerPoint or other presentation software installed
* Video projector and screen for demonstrations and presentations

1. Researching Network Attacks

In Part 1 of this lab, you will research real network attacks and select one on which to report. Fill in the form below based on your findings.

* + 1. Research various network attacks.

List some of the attacks you identified in your search.

* Distributed Denial of service
* Man, in the middle
* Code/SQL injection
  + 1. Fill in the following form for the network attack selected.

|  |  |
| --- | --- |
| Name of attack: | The 2016 Dyn attack |
| Type of attack: | DoS |
| Dates of attacks: | October 21, 2016 |
| Computers / Organizations affected: | Dyn (DNS Provider) also affected AirBnB, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub |
| How it works and what it did: | |
| This was done using a [malware](https://www.cloudflare.com/learning/ddos/glossary/malware/) called [Mirai](https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/). Mirai creates a botnet out of compromised [Internet of Things (IoT)](https://www.cloudflare.com/learning/ddos/glossary/internet-of-things-iot) devices such as cameras, smart TVs, radios, printers, and even baby monitors. To create the attack traffic, these compromised devices are all programmed to send requests to a single victim. | |
| Mitigation options: | |
| There are 4 stages of mitigating a DDoS attack using a cloud-based provider:  **Detection** - to stop a distributed attack, a website needs to be able to distinguish an attack from a high volume of normal traffic. If a product release or other announcement has a website swamped with legitimate new visitors, the last thing the site wants to do is throttle them or otherwise stop them from viewing the content of the website. IP reputation, common attack patterns, and previous data assist in proper detection.  **Response** - in this step, the DDoS protection network responds to an incoming identified threat by intelligently dropping malicious bot traffic and absorbing the rest of the traffic. Using [WAF](https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/) page rules for [application layer (L7)](https://www.cloudflare.com/learning/ddos/what-is-layer-7/) attacks, or another filtration process to handle lower level (L3/L4) attacks such as [memcached](https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/) or [NTP amplification](https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/), a network is able to mitigate the attempt at disruption.  **Routing** - By intelligently routing traffic, an effective DDoS mitigation solution will break the remaining traffic into manageable chunks preventing [denial-of-service](https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/).  **Adaptation** - A good network analyzes traffic for patterns such as repeating offending IP blocks, attacks coming from certain countries, or particular protocols being used improperly. By adapting to attack patterns, a protection service can harden itself against future attacks. | |
| References and info links: | |
| <https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/#:~:text=The%20biggest%20DDoS%20attack%20to,of%20126.9%20million%20per%20second.>  <https://www.cloudflare.com/learning/ddos/ddos-mitigation/#:~:text=DDoS%20mitigation%20refers%20to%20the,to%20mitigate%20the%20incoming%20threat.> | |
| Presentation support graphics (include PowerPoint filename or web links): | |
|  | |

1. Researching Network Security Audit Tools and Attack Tools

In Part 2 of this lab, research network security audit tools and attack tools. Investigate one that can be used to identify host or network device vulnerabilities. Fill in the report below based on your findings.

* + 1. Research various network security audit tools and attack tools.

List some of the tools that you identified in your search.

* [**SolarWinds Network Configuration Manager**](https://www.comparitech.com/go/solarwinds-network-configuration-manager-more-information/l/list_dd_d__post__276195/d/276195/d/276195/)
* **Netwrix Auditor**
* **Nmap**
* **OpenVAS**
* **Acunetix**
* **Kaseya VSA**
* **Spiceworks Inventory**
* **Network Inventory Advisor**
* **ManageEngine AdAudit Plus**
* **Metasploit**
  + 1. Fill in the following form for the network security audit tool/attack tool selected.

|  |  |
| --- | --- |
| Name of tool: | **Metasploit** |
| Developer: | [Rapid7 LLC](https://www.google.com/search?rlz=1C1CHBF_en-GBAU894AU894&q=Rapid7+LLC&stick=H4sIAAAAAAAAAONgVuLWT9c3NDKqKjQpN1zEyhWUWJCZYq7g4-MMAKSMTKYcAAAA&sa=X&ved=2ahUKEwjJoujEuYPrAhW0oekKHcRTAoUQmxMoATAnegQICxAD) |
| Type of tool (character-based or GUI): | character-based and GUI |
| Used on (network device or computer host): | Computer Host |
| Cost: | Metasploit is free but the pro version is 15,000 per named user per year |
| Description of key features and capabilities of product or tool: | |
| * Command shell payloads that enable users to run scripts or random commands against a host * Dynamic payloads that allow testers to generate unique payloads to evade antivirus software * Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files * Static payloads that enable port forwarding and communications between networks | |
| References and info links: | |
| <https://www.varonis.com/blog/what-is-metasploit/>  <https://www.comparitech.com/net-admin/network-security-auditing-tools/> | |

1. Reflection
   1. What is the impact of network attacks on the operation of an organization? What are some key steps organizations can take to help protect their networks and resources?

Impacts incude reputaional damage i.e. loss of customers loss of sales reduction in profits etc. and financial loss  
  
business can protect themselves by

Put in And Monitor Firewall Performance

Update Passwords At Least Every Quarter

Maintain Your Anti-Virus Software

Create A Virtual Private Network (VPN)

Training Your Employees

* 1. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact on the organization and what did it do about it?

Epic DoS themselves with the free release of GTA V on their store, “We are aware that users may be encountering slow loading times, 500 errors, or launcher crashing at this time and we are actively working to scale. We'll provide an update as soon as we can.” Epic Games on twitter

* 1. What steps can you take to protect your own PC or laptop computer?
* **use strong passwords and change them periodically**
* **Install anti-virus software**
* **Install anti-spyware and anti-malware software**
* **Perform daily full system scans**
* **Create a periodic system backup schedule**:
* **Regularly update your computer system**
* **Use your firewall**