Attacks and Cyber Security Lesson Plan

Purpose: help students understand how attackers can breach a computer system through vulnerabilities at the physical, human, operating system, and network levels.

****Note: w.x.y.z is used to denote a generalization for an IP address to be inserted according to the respective machine indicated.

Standards

CPP.L3A-09 Explain the principles of security by examining encryption, cryptography, and authentication techniques.

Objectives

Students will be able to explain the principles of security by examining encryption, cryptography, and authentication techniques

Students will be able to discuss the social and economic implications associated with hacking.

Students will be able to describe security and privacy issues that relate to computer networks.

Port Scanning

Reconnaissance, social engineering attacks, gather as much information as one can. Find out what services those systems are running. By knowing what services are available on the target and research vulnerabilities that are available for those services.

The first exploit an attacker will run is called port scanning. This is to see what ports are running services and more importantly what version of the services are running. Typically the older versions will have more vulnerabilities. There are 2^{16} or 65,536 ports.

Using Kali Linux to attack the victim machine using nmap suit of tools to make connections to the victim's machine.

The following can be used to enact the different port scanning techniques:

begin with a ping (ICMP) to the IP address

- ping w.x.y.z

TCP Connect Scan--open scan/three-way system call/easily detected and logged

- -sT w.x.y.z

Syn Scan--half-open scan

- -sS w.x.y.z

stealth scans

Fin Scan--inverse mapping for discovering closed ports

- -sF w.x.y.z

Null Scan--inverse scan--no flag is set

- -sS w.x.y.z

Psh Scan--push flag is sent

- -sP w.x.y.z

Urg Scan--urgent flag is sent

- -sU w.x.y.z

This research is supported by Award #1542465:
RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)

Ack Scan--checks for firewall
- -sA w.x.y.z

Xmas Scan--half-combination of flags set
- -sX w.x.y.z

Snort should be installed to utilize the intrusion detection system (IDS). This will allow packet examination at the application layer and alert the user attempts have been made to connect. IDS can result in false positive, where IDS indicates an attack when none exists; false negative, where IDS fails to acknowledge an attack when one exists, true positive, where IDS identifies a threat/attack when one exists; and true negative, where IDS identifies correctly no threat or attack exists. The approaches include being host-based, meaning at the host/user level activity is being monitored related to applications and the operating system. A second approach is network based, which monitors traffic for a subnet, protects the network, and alerts the server of problems using a statistical analysis of traffic patterns. The components of Snort are packet decoder, preprocessor, detection engine, and logging.

create and edit a file with the IDS rules:
- cd /etc/snort
- vim custom.rules

command to edit file "i" to insert comments in file
- alert tcp any any -> any any (msg: "SSH Brute Force Attempt"; flow: established, to_server; content: "SSH"; nocase; offset: 0; depth:4; detection_filter: track by_src, count 3, seconds 60; sid: 100001; rev: 1;)

To start Snort
- snort -v -I eth0 -l log -c /etc/snort/snort.conf

To write a rule for the Snort IDS, include the action. Possible actions include:
Alert→ if criteria is met, generates alert and log
Log→ just logs
Ignore→ ignores packet(s)
!--> negates

Protocol is used to specify which protocol the IDS should be detecting. Ex: TCP
Source port: any any
Destination port: any any
Rule options: message

Materials
Kali Linux with nmap and Snort
https://sourceforge.net/projects/metasploitable/files/latest/download
https://www.kali.org/downloads/

Metasploit software is for performing an exploit on target machines and finding the vulnerabilities on the target machine.
With these tests the exploits that are available for target's system will be known. These benefits could slow the target, change data on the system, access root account which would allow administrative access. This breaches confidentiality, integrity and availability of the system. Each exploit gives a specific score for accessing the target machine; lowest score provides less power, higher score gives more control.

VICTIM

Using Metaspoitable allows the attacker to penetrate the user's system with built in vulnerabilities. The victim should be configured to the router's gateway

Gateway Commands

- route
- route –n
- route add default gw w.x.y.z eth0 (for attacker and victim)

if default gateway needs to be deleted:
route del default gw w.x.y.z eth0

check IP address

- ifconfig –a

ROUTER

The router is set up with two Ethernet connects to allow forwarding from the attacker to the victim.
To set up forwarding:

- echo 1 > /proc/sys/net/ipv4/ip_forward

To check forwarding:

- cat /proc/sys/net/ipv4/ip_forward

INTRUSION DETECTION SYSTEM

1. check the custom rules and show the attack rule
   - vim custom.rules

2. begin running snort
   - snort -dev -l log -c /etc/snort/snort.conf
   - snort –v –I eth0 –l log –c /etc/snort/snort.conf

Now the IDS snort is running and listening

ATTACKER: Metasploit

1. From the 'root@kali>' prompt, enter **msfconsole**

This will open msf console. The **msfconsole** is probably the most popular interface to the Metasploit Framework (MSF). It provides an "all-in-one" centralized console and allows efficient access to virtually all of the options available in the MSF.

2. From msf>, enter **use exploit/multi/samba/usermap_script**

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Specifically it is attacking the file sharing service called Samba that users could implement to share files.

3. From msf> enter **set RHOST <victims IP address>**

The most important option to set is the **set RHOST <victims IP address>**. This is the ip address of the victim machine that is running with vulnerabilities.

4. At this point, from the msf> prompt you simply enter **run**. Viola! The victims' computer has been exploited
5. Show that the attacker has shell access by
   - ifconfig

This will show the IP address of the victim computer (metasploitable machine)

Use ctrl+c to exit

What can an attacker do after exploitation? This is the fundamental question asked by attackers after they compromise a system. Well, the answer depends on the creativity of the attacker. In the second scenario, we will see how logins and passwords can be retrieved through metasploit.

What can a victim, or in this case, the router do? Once the router has detected an attack is occurring, a rule in the firewall can be created to block the attacker from making a connection to the victim's system.

ROUTER—show intrusion has occurred

1. show alert log and find the alert for the word "detecting" which will give the IP address that is trying to attack the system
   - vim log/alert

   to find press "esc"
   then /detecting

2. write a rule for iptables (Linus firewall) that will drop all connections attempted by the attacker (using his specific IP address)
   - iptables –A INPUT –s w.x.y.z –j DROP

if the attack is able to continue, try
   - iptables –A FORWARD –s w.x.y.z –j DROP

show the iptables
   - iptables –L

to flush (erase) iptables firewall rules
   - iptables -F

ATTACKER try to run the exploit again to show that the firewall is enacted and the attacker will not be successful.

In the msfconsole

   - run

Demo 2

Attacker will penetrated the victim's computer (metasploitable) using a brute force method to obtain the system's password

"A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack may also be referred to as brute force cracking.
For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.

An attack of this nature can be time and resource consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

The following measures can be used to defend against brute force attacks:

- Requiring users to have complex passwords
- Limiting the number of times a user can attempt to log in
- Temporarily locking out users who exceed the specified maximum number of login attempts"

The password needs to be in the dictionary file:

/usr/share/matasploit-framework/data/wordlist/root_userpass.txt

ROUTER

1. change the directory to snort

   - cd /etc/snort

check the custom.config file

- vim custom.rules

  turn off #2, turn on #3

2. start snort

- snort –dev –l log –c snort.conf

ATTACKER Steps to initiate a brute force attack:

1. From the 'root@kali>' prompt, enter msfconsole to return to the msf> prompt

2. From msf>, enter
   - **use auxiliary/scanner/ssh/ssh_login**

SSH, or *Secure Shell*, is a protocol used to securely log onto remote systems. It is the most common way to access remote Linux and Unix-like servers.

3. From auxiliary(ssh login)> **set RHOSTS <victims IP address>**
4. From auxiliary(ssh login)> **set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt**

This allows access to a database, or dictionary, of usernames and passwords.

5. With everything ready to go, we run the module by entering **run**. Failed username and password combinations will scroll on the screen until a successful combination is found.

ROUTER view alert log and write a firewall rule to limit rate for brute force attack

1. show alert log
   - vim log/alert

   to find press "esc"
   then /brute

   note the attacker's IP address and write a rule to limit the number of attempt (this could depend on your connection which values should be used for time and hit count—we're using a switch and will used 100 seconds and 3 for the hit count)

2. iptables rule for limit rate
   - iptables –A INPUT –p tcp --dport 22 –m state --state NEW –m recent --update --seconds 100 --hitcount 3 -j ACCEPT

   iptables rule for dropping all packets after limit rate
   - iptables -A INPUT -j DROP

Alternately, a screenshot could be provided if time does not permit to run the exploit again.