Nem Negash

09/11/2021

CMSC 426

Lab 2

**Exercise 1 – Scanning with Nmap**

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

**Exercise 2 – Reverse Shell with Metasploit**

**Step 1: Generate the executable payload:**

Graphical user interface, text

Description automatically generated

**Step 6: Obtain Administrator access on box B (the victim’s box):**

Graphical user interface, text

Description automatically generated

**Exercise 3 – Let’s Play with Armitage!!**

Graphical user interface, website

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

**Conclusion and Lab Report:**

1. Which of the tools/techniques used in this lab would you personally find most useful as a penetration tester?
   1. Nmap seems like an incredible tool that can be used for penetration testing. Using the information found using OSINT foot printing it can find vulnerabilities of a system. Using the IP address of a servers it can allow you to find the vulnerabilities and essentially give you full control of the server. Nmap is used for penetration testing by many security teams in the industry. It is a tool widely used and often updated with new features.
   2. Armitage is also another great tool for beginner hacker with the way it gives a graphic tool compared to just having to know terminal commands. This tool is not used as much as Nmap in the industry, but it is a great way to start learning about penetration testing. It is also a little out of date and has not been updated in over 6 years.
2. Did these exercises make you think of other capabilities that you would find helpful for gaining user credentials on targeted systems?
   1. While these tools are great for getting access it is hard to use them without making any noise or in cyber terms without being detected. Another way to get access is by compromising a certified user by getting their credentials to the network. This is because it is proven that users are the weakest link to the security of a network. Hacker can get the credentials of a user by sending emails to the user with a link that looks like the network login and get the credentials when the user tries to login. Another way is by having the user download a malicious file onto their computer. From there the hacker can create backdoors to get further access to the network without the knowledge of the user.
3. What are some well-known exploits that have utilized a reverse shell to gain access?
   1. PowerShell Nishang script is one of the most common ways to create a reverse shell access to the windows machine. An attacker can download the Invoke-PowerShellTcp.ps1 script and modify it with the target IP and port. From there the attacker can host the script on a webserver and Use RCE or webshell to run powershell command to download and execute Invoke-PowerShellTcp.ps1.
   2. Shellgen is also another tool to launch reverse shells to a Linux target. An attacker would simply have to just edit the script manually or use the interface to enter the target IP address and port. Shellgen also give you the option to generate a command in you desired scripting language. The attacker can then copy and paste the script to their desired RCE vector.