## "SmartDefend: Intelligent Attack Detection and Protection"

**Technology :-** Kali linux,Debian,Snort,Iptables,Metasploit,Nmap

**Description:-**This project focused on enhancing security through the strategic utilization of Snort and iptables. By leveraging Snort's real-time traffic analysis and packet logging capabilities, we successfully detected and monitored various cyber attacks.

This project also encompassed the implementation of iptables for IP packet management, allowing us to inspect, modify, and redirect traffic effectively. To bolster our defense mechanisms, I integrated fail2ban and Xtables into the architecture, fortifying our resilience against denial-of-service (DoS) and distributed DoS (DDoS) attacks.

This initiative resulted in a robust and adaptive security framework that significantly elevated the network's protection against a wide range of threats.

## IPTABLES RULES :-

## (Sequence in iptables rules matter a lot )

```
# Clear existing rules and set default policies
iptables -F
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Allow loopback traffic
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Allow established and related connections
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT

# Allow incoming SSH from the specified IP address
iptables -A INPUT -p tcp --dport 22 -s 192.168.80.1 -j ACCEPT

# Drop incoming SSH from all other sources
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# syn flood prevent
iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j DROP

#os fingerprint attempt
iptables -A INPUT -p tcp --dport 1:65535 -m string --string "Nmap" --algo bm --to 65535 -j DROP
```

```
# Create a new chain for detecting and handling port scans
iptables -N PORTSCAN

# Add rules to the PORTSCAN chain
iptables -A PORTSCAN -m recent --name portscan --set -j DROP
iptables -A PORTSCAN -j RETURN

# Add rules to the INPUT chain to redirect suspicious traffic to PORTSCAN chain
iptables -A INPUT -p tcp --tcp-flags ALL SYN -m recent --name portscan --rcheck --seconds 60 --hitcount 10 -j PORTSCAN

# Allow HTTP and HTTPS traffic
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# Allow DNS
iptables -A INPUT -p udp --dport 53 -j ACCEPT

# Allow NTP
iptables -A INPUT -p udp --dport 123 -j ACCEPT

# Allow ICMP (Ping)
iptables -A INPUT -p icmp -j ACCEPT

#smurf attack protect
iptables -A INPUT -p icmp --icmp-type echo-request -d 192.168.80.255 -j DROP
```

```
#block outside country
#china #pak

#iptables -A INPUT -m geoip --src-cc CN -j DROP
#iptables -A INPUT -m geoip --src-cc PK -j DROP

iptables -A INPUT -m geoip --src-cc CN -j LOG --log-level debug --log-prefix "friend from china"
iptables -A INPUT -m geoip --src-cc PK -j LOG --log-level debug --log-prefix "friend from pakistan"

#iptables -A INPUT -j DROP
#iptables -L -v
iptables -L
```

# Snort Rules :-

```
alert ip any any -> any any (msg:"ping" ; sid:10000001;)
#ssh attempt
#alert tcp  $EXTERNAL_NET  any -> $HOME_NET 22 (msg:"SSH Login Attempt"; sid:100004;)


#syn flood
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (flags: S; threshold: type both, track by_dst, count 100, seconds 5; msg: "Possible SYN Flood Detected"; sid:100005;)


#buffer overflow
#alert tcp any any -> any any (msg:"Possible Buffer Overflow Attempt"; content:"|90 90 90 90|"; depth:4; sid:1000007;)


#Rule to Detect Port Scans:
#alert tcp any any -> $HOME_NET any (msg:"Port Scan Detected"; flags: FPU, S; threshold: type threshold, track by_src, count 5, seconds 10; sid:100008;)


#ftp attempt
#alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"FTP Login Attempt"; content:"USER "; nocase; threshold: type limit, track by_src, count 1, seconds 60; sid:100009; rev:1;)


#mac flood detect
#alert udp any 68 -> any 67 (msg:"Potential MAC Flooding Attack"; threshold: type both, track by_src, count 100, seconds 60; sid:1000010;)


#smurf attack
```

```
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Possible Smurf
Attack Detected"; dsize:0; itype:8; icode:0; threshold: type threshold, track
by_src, count 1, seconds 1; sid:1000012;)
```

## Snort configuration :-

```
sudo apt-get install snort
which snort
sudo snort –version
sudo nano /etc/snort/snort.conf
```

(add my.rules in site specific rules)

```
sudo nano /etc/snort/rules/my.rules
```

(write rule in this file eg:- alert ip  any any -> any any (msg:”up” ; sid:1000001;)

```
sudo snort -c /etc/snort/snort.conf -T :- test
sudo snort -c /etc/snort/snort.conf -A console – run
sudo snort -i ens33 -u snort -g snort -c /etc/snort/snort.conf -A console :- run  on
ens33
```

**Iptables configuration :-**

```
sudo apt-get install iptables
sudo nano ip.sh
sudo chmod 777 ip.sh
sudo ./ip.sh
sudo nano /etc/snort/rules/my.rules
sudo apt-get install iptables-persistent
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
sudo sh -c "iptables-restore < /etc/iptables/rules.v4"
```

Xtables-addons:-

```
Sudo apt-get update
Sudo apt-get dist-upgrade
Sudo apt-get install automake ca-certificates gcc iptables-dev libc6-dev
libnet-cidr-lite-perl libtext-csv-xs-perl linux-headers-$(uname -r) make
pkg-config unzip wget xz-utils -y
cd /tmp/
tmp$ wget (path to download xtables-addons-3.23.tar.xz)
tar -xf xtables-addons-3.23.tar.xz
ls -l
cd xtables-addons-3.23
sudo ./configure
sudo make
sudo make install
ls -l /usr/local/libexec/xtables-addons/
```

```
cd :- home dir
mkdir xtables
cd xtables
sudo /usr/local/libexec/xtables-addons/xt_geoip_build -D /usr/share/xt_geoip/ *.csv
ls -l /usr/share/xt_geoip/
cd
sudo depmod -a :-  refresh the module dependency information for all kernel modules
sudo iptables -m geoip -h
```

then  add geoip rules :-

```
#block outside country
#china #pak
#drop
#iptables -A INPUT -m geoip --src-cc CN -j DROP
#iptables -A INPUT -m geoip --src-cc PK -j DROP
#allow
iptables -A INPUT -m geoip --src-cc CN -j LOG --log-level debug --log-prefix "friend from china"
iptables -A INPUT -m geoip --src-cc PK -j LOG --log-level debug --log-prefix "friend from pakistan"
```

after ping see log file in

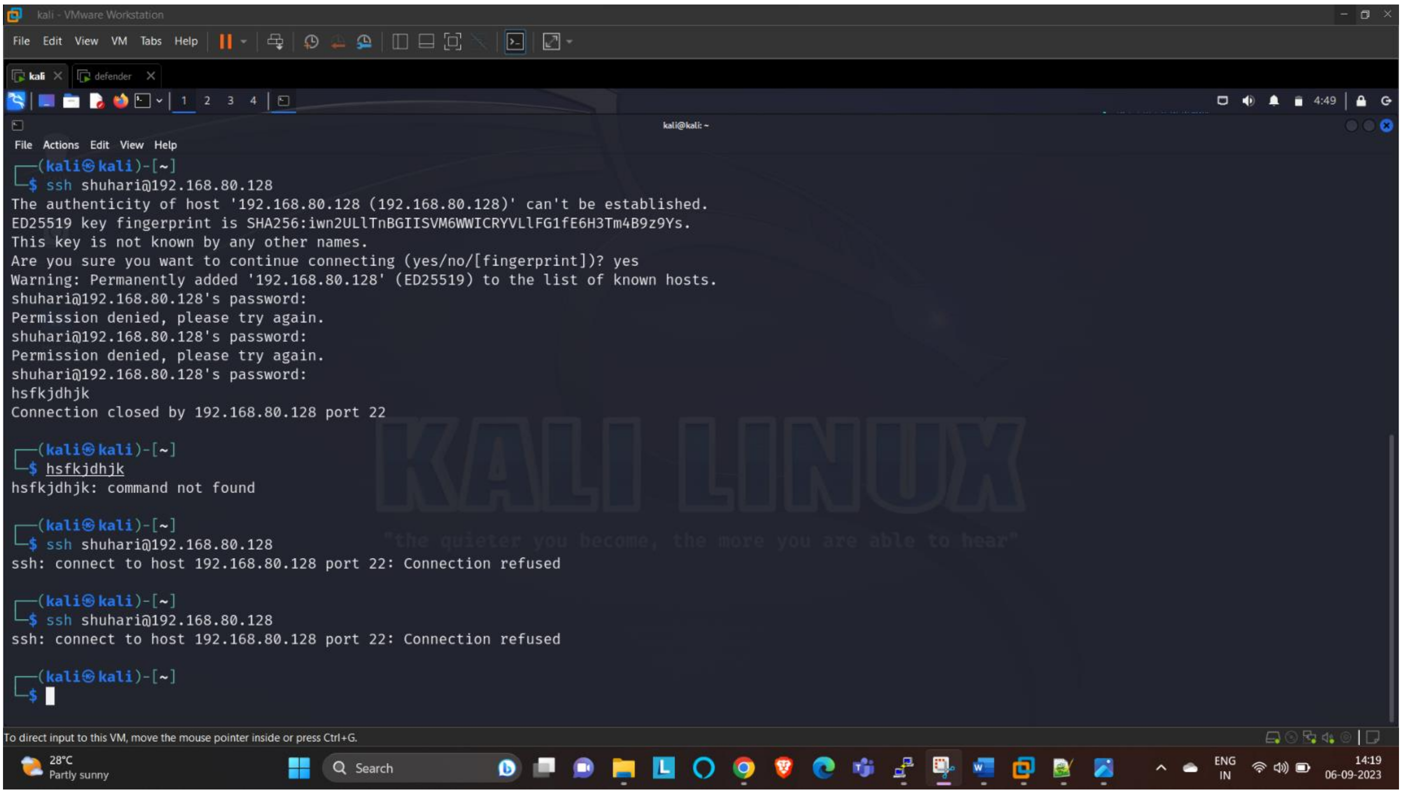
```
sudo tail -f /var/log/syslog
```

## Configure fail2ban

```
Sudo apt-get install  fail2ban
Sudo fail2ban-client status
Sudo fail2ban-client status
Sudo watch fail2ban-client status sshd :- any wrong attempt it will add to jail
```

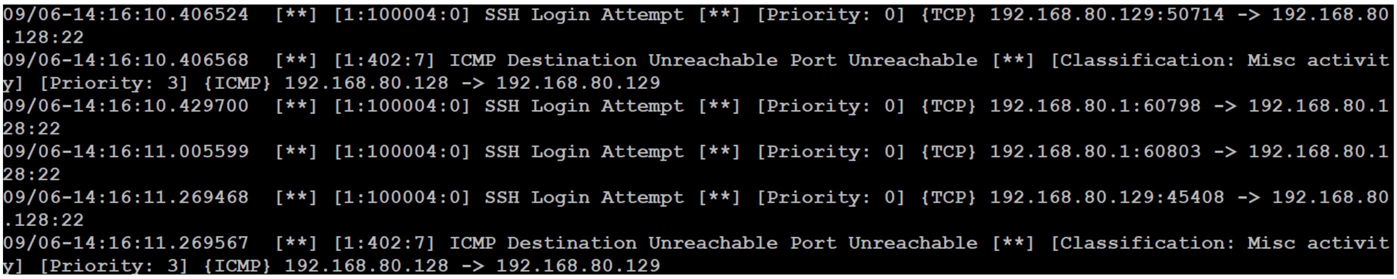
# Attacks :-

Ssh attempt :- ssh username@(ip)


kali - VMware Workstation
File Edit View VM Tabs Help
kali
defender
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
28°C
Partly sunny
Search
ENG
IN
14:19
06-09-2023

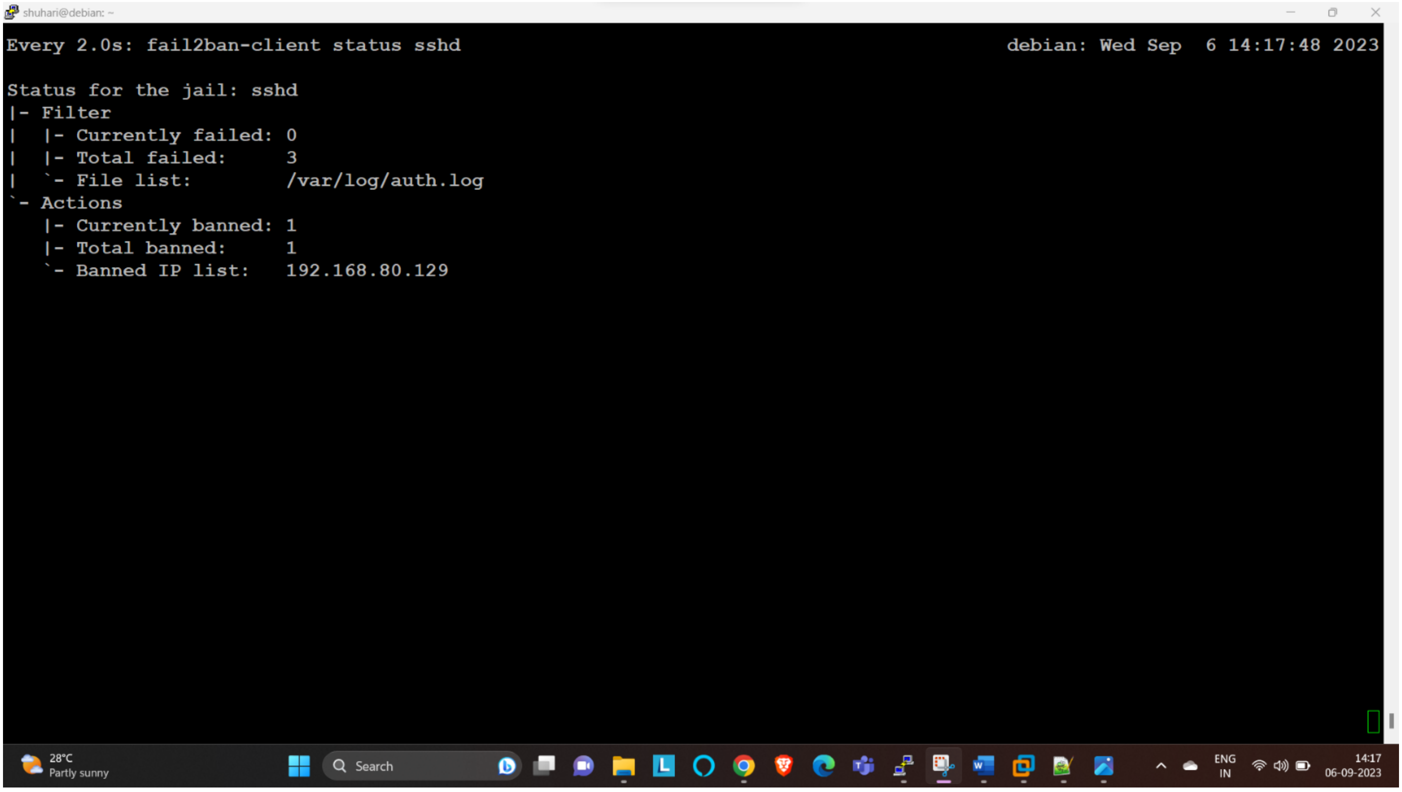
```
┌──(kali㉿kali)-[~]
└─$ ssh shuhari@192.168.80.128
The authenticity of host '192.168.80.128 (192.168.80.128)' can't be established.
ED25519 key fingerprint is SHA256:iwn2ULlTnBGIISVM6WWICRYVLlFG1fE6H3Tm4B9z9Ys.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.80.128' (ED25519) to the list of known hosts.
shuhari@192.168.80.128's password:
Permission denied, please try again.
shuhari@192.168.80.128's password:
Permission denied, please try again.
shuhari@192.168.80.128's password:
hsfkjdhjk
Connection closed by 192.168.80.128 port 22

┌──(kali㉿kali)-[~]
└─$ hsfkjdhjk
hsfkjdhjk: command not found

┌──(kali㉿kali)-[~]
└─$ ssh shuhari@192.168.80.128
ssh: connect to host 192.168.80.128 port 22: Connection refused

┌──(kali㉿kali)-[~]
└─$ ssh shuhari@192.168.80.128
ssh: connect to host 192.168.80.128 port 22: Connection refused

┌──(kali㉿kali)-[~]
└─$ ▌
```

Snort detect ssh



```
09/06-14:16:10.406524  [**] [1:100004:0] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.80.129:50714 -> 192.168.80
.128:22
09/06-14:16:10.406568  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activit
y] [Priority: 3] {ICMP} 192.168.80.128 -> 192.168.80.129
09/06-14:16:10.429700  [**] [1:100004:0] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.80.1:60798 -> 192.168.80.1
28:22
09/06-14:16:11.005599  [**] [1:100004:0] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.80.1:60803 -> 192.168.80.1
28:22
09/06-14:16:11.269468  [**] [1:100004:0] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.80.129:45408 -> 192.168.80
.128:22
09/06-14:16:11.269567  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activit
y] [Priority: 3] {ICMP} 192.168.80.128 -> 192.168.80.129
```

Fail2ban block ip



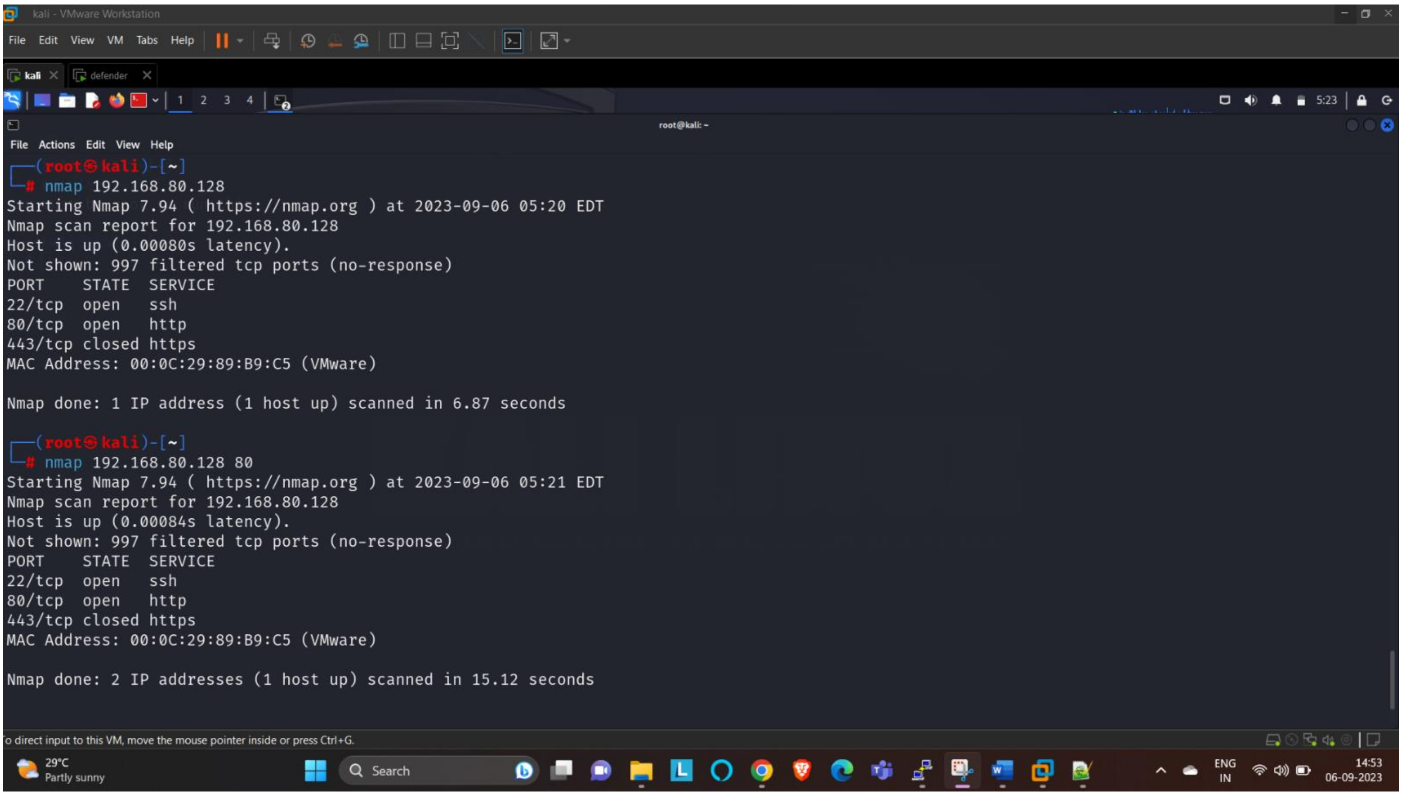
```
Every 2.0s: fail2ban-client status sshd                     debian: Wed Sep  6 14:17:48 2023

Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.80.129
```

Nmap :-

Sudo apt-get install nmap

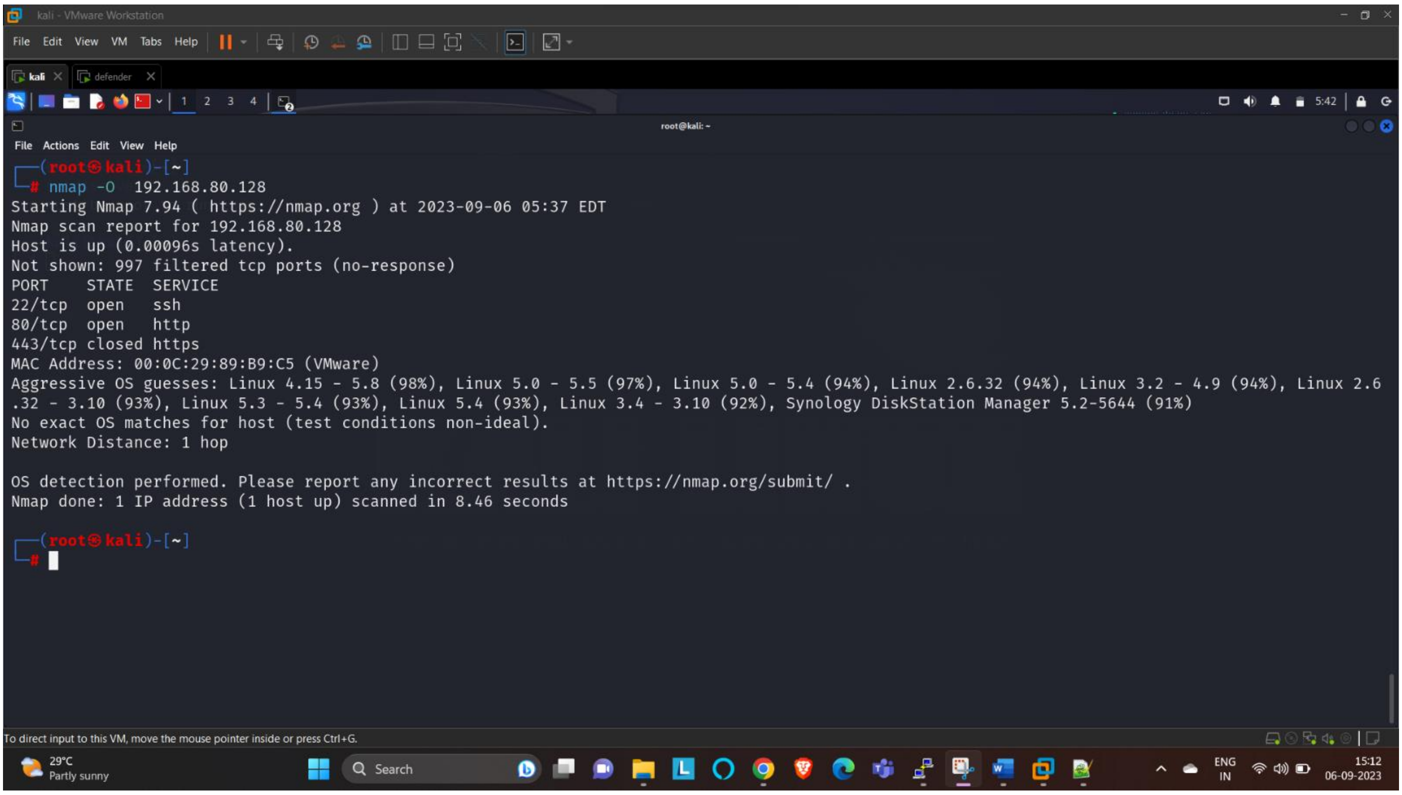
Nmap (ip)

Nmap(ip)(port)


kali - VMware Workstation
File Edit View VM Tabs Help
kali
defender
root@kali: ~
File Actions Edit View Help
5:23
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Partly sunny
Search
ENG
IN
14:53
06-09-2023

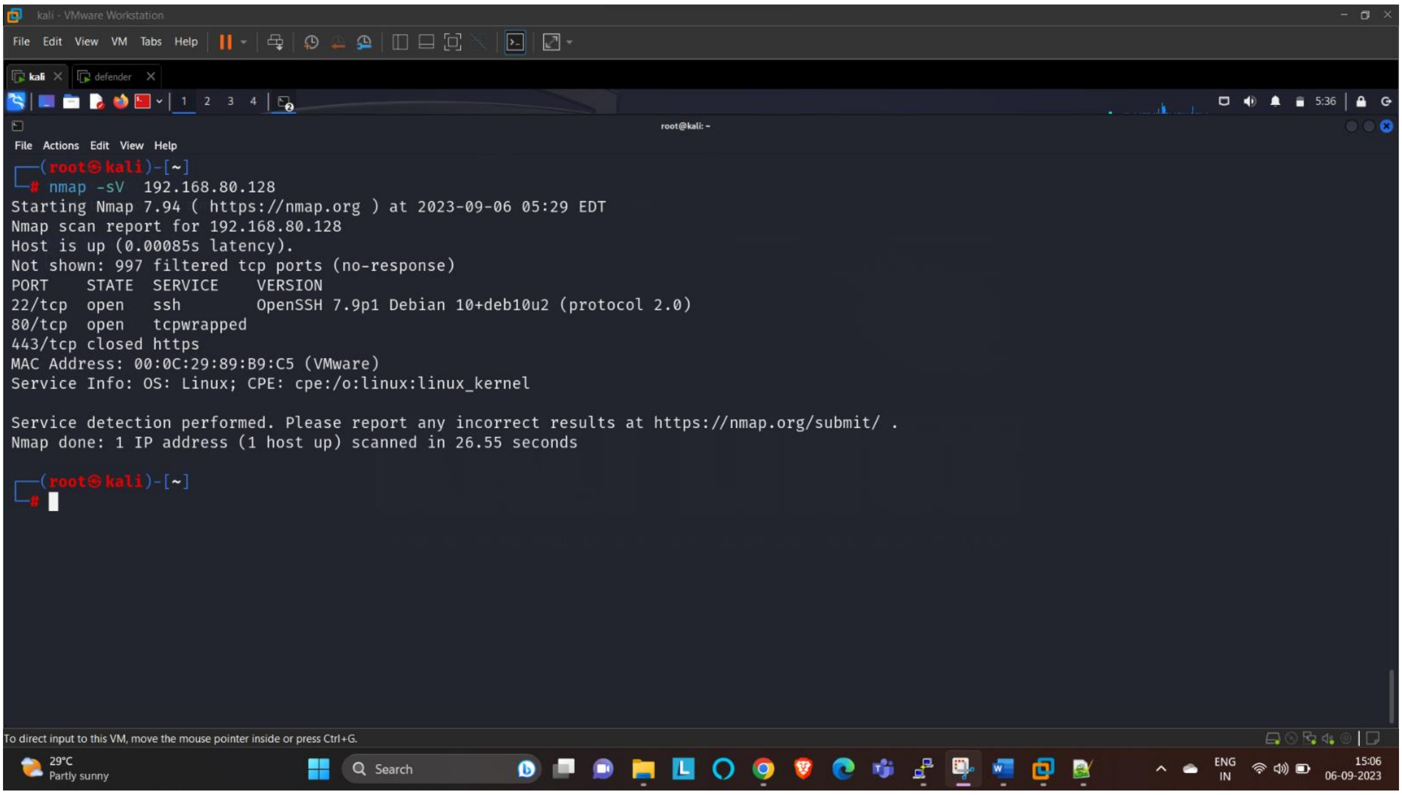
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.80.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 05:20 EDT
Nmap scan report for 192.168.80.128
Host is up (0.00080s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp closed https
MAC Address: 00:0C:29:89:B9:C5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.87 seconds

┌──(root㉿kali)-[~]
└─# nmap 192.168.80.128 80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 05:21 EDT
Nmap scan report for 192.168.80.128
Host is up (0.00084s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp closed https
MAC Address: 00:0C:29:89:B9:C5 (VMware)

Nmap done: 2 IP addresses (1 host up) scanned in 15.12 seconds
```

Os detection


kali - VMware Workstation
File Edit View VM Tabs Help
kali
defender
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the pointer inside or press Ctrl+G.
29°C
Partly sunny
Search
ENG
IN
15:12
06-09-2023

```
┌──(root㉿kali)-[~]
└─# nmap -O  192.168.80.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 05:37 EDT
Nmap scan report for 192.168.80.128
Host is up (0.00096s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:89:B9:C5 (VMware)
Aggressive OS guesses: Linux 4.15 - 5.8 (98%), Linux 5.0 - 5.5 (97%), Linux 5.0 - 5.4 (94%), Linux 2.6.32 (94%), Linux 3.2 - 4.9 (94%), Linux 2.6
.32 - 3.10 (93%), Linux 5.3 - 5.4 (93%), Linux 5.4 (93%), Linux 3.4 - 3.10 (92%), Synology DiskStation Manager 5.2-5644 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.46 seconds

┌──(root㉿kali)-[~]
└─# 
```

# Service version detection


kali - VMware Workstation
File Edit View VM Tabs Help
kali
defender
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the pointer inside or press Ctrl+G.
29°C
Partly sunny
Search
ENG
IN
15:06
06-09-2023

```
┌──(root㉿kali)-[~]
└─# nmap -sV  192.168.80.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 05:29 EDT
Nmap scan report for 192.168.80.128
Host is up (0.00085s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE    VERSION
22/tcp  open   ssh        OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp  open   tcpwrapped
443/tcp closed https
MAC Address: 00:0C:29:89:B9:C5 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.55 seconds

┌──(root㉿kali)-[~]
└─# 
```

## All other nmap commands :-

Basic Scan Commands:

Scan a single target:

```
nmap target_ip
```

Scan multiple targets:

```
nmap target1_ip target2_ip
```

Scan Types:

TCP SYN scan (default):

```
nmap -sS target_ip
```

TCP Connect scan:

```
nmap -sT target_ip
```

UDP scan:

```
nmap -sU target_ip
```

Scan Techniques:

Stealthy scan (SYN scan with no ping):

```
nmap -sS -Pn target_ip
```

Scan all 65,535 ports (not recommended for large networks):

```
nmap -p- target_ip
```

### Service Version Detection:

Detect service versions:

```
nmap -sV target_ip
```

### Operating System Detection:

Detect the operating system of the target:

```
nmap -O target_ip
```

### Output Options:

Save scan results to a file:

```
nmap -oN output.txt target_ip
```

Save scan results in XML format:

```
nmap -oX output.xml target_ip
```

### Script Scanning:

Run Nmap scripts against a target:

```
nmap --script script_name target_ip
```

### Timing and Performance:

Adjust scan timing (e.g., aggressive scan):

```
nmap -T4 target_ip
```

Increase verbosity for more details:

```
nmap -v target_ip
```

Firewall Evasion:

Use decoy IPs to hide the source:

```
nmap -D RND:10 target_ip
```

Other Options:

Scan a range of IPs using CIDR notation:

```
nmap 192.168.1.0/24
```

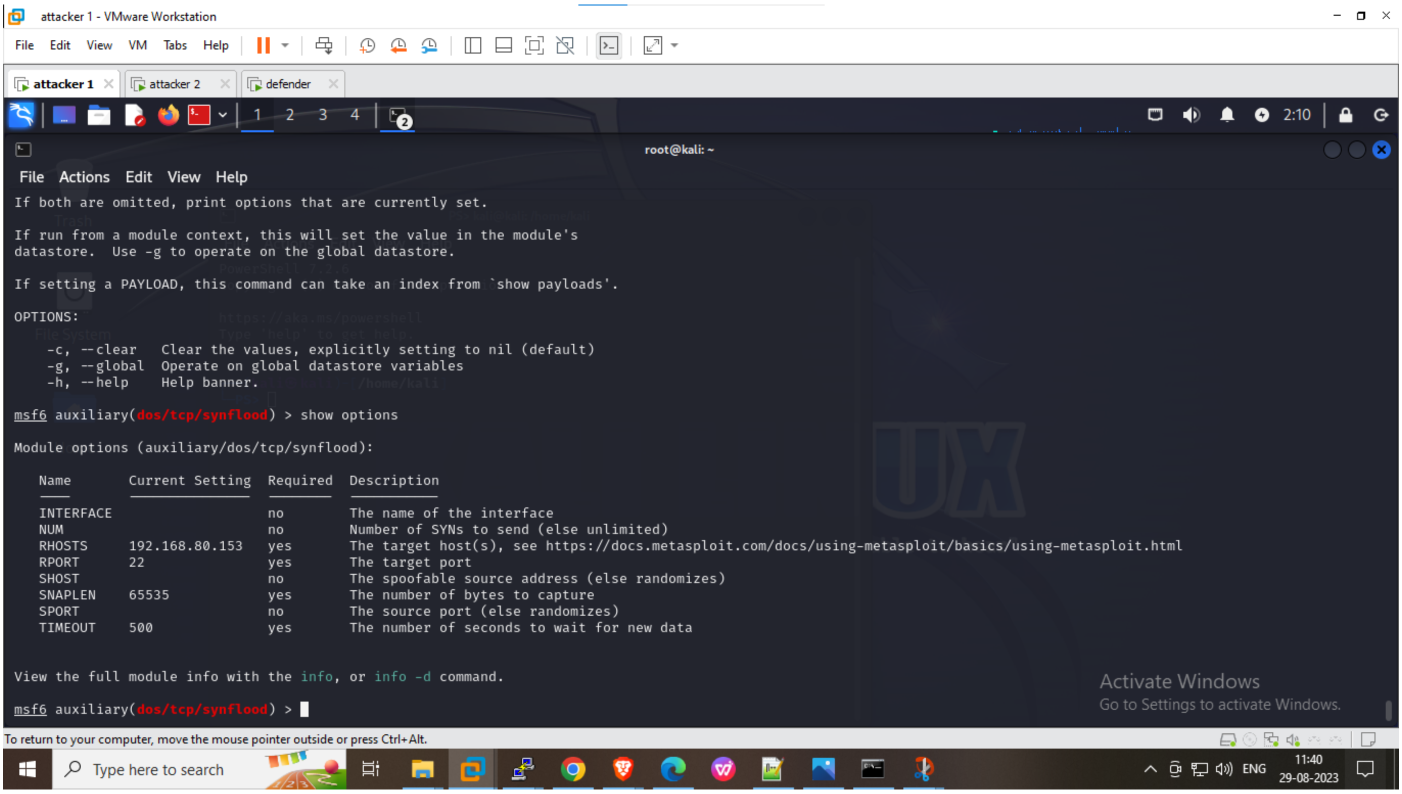
Randomize target order:

```
nmap --randomize-hosts -iL targets.txt
```

# Syn flood :-

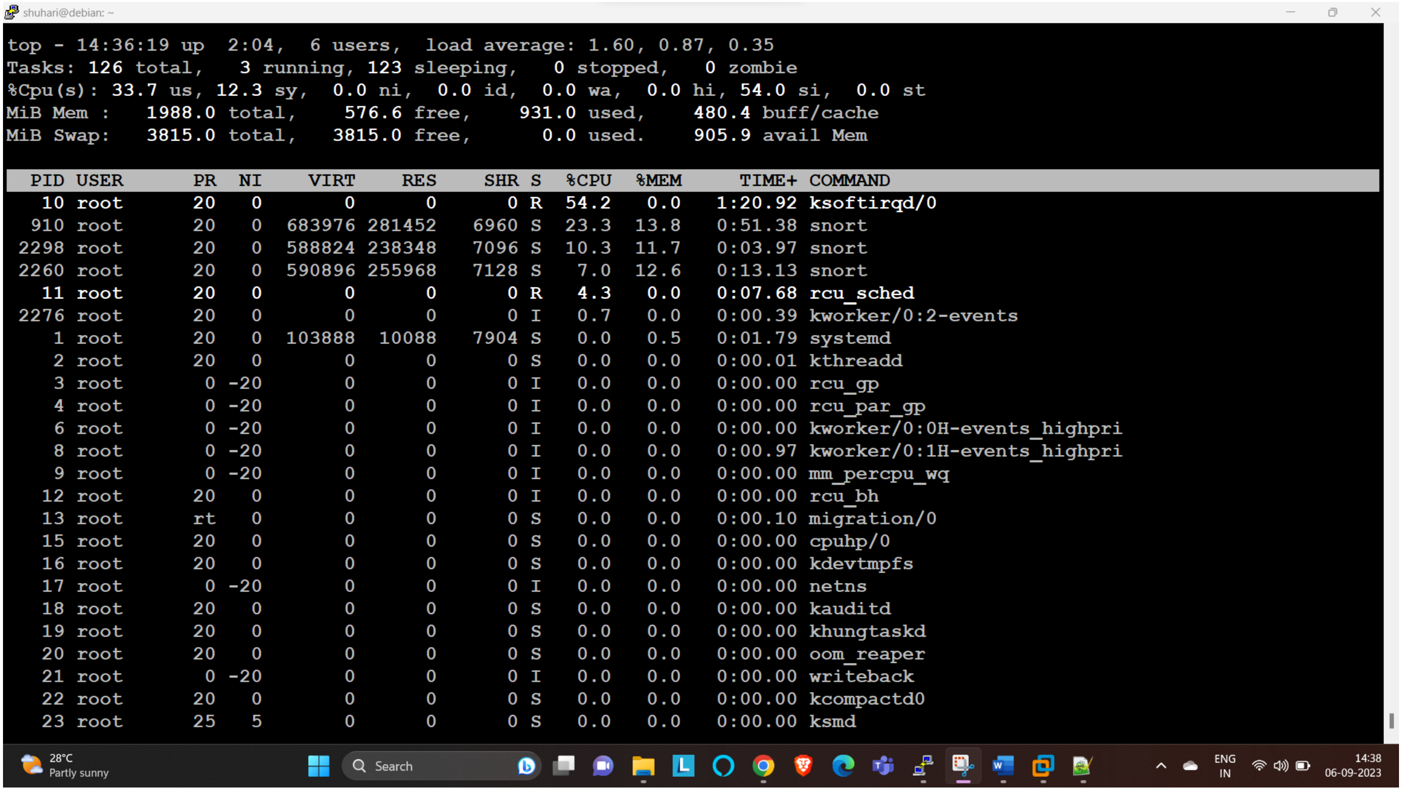
Using metasploit :-

Flooding on port 22


attacker 1 - VMware Workstation
File Edit View VM Tabs Help
attacker 1
attacker 2
defender
1 2 3 4
2:10
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Type here to search
ENG
11:40
29-08-2023

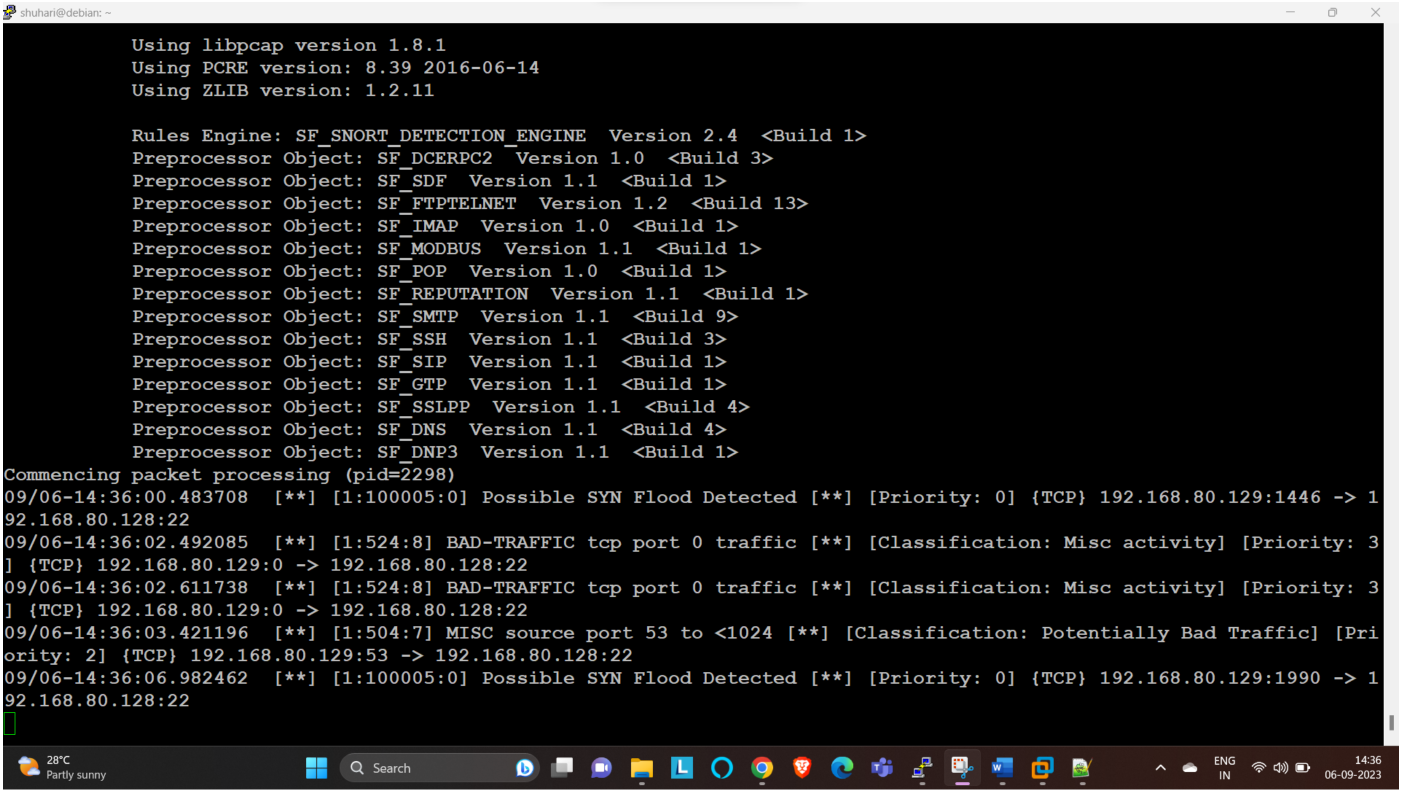
```
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.

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     192.168.80.153   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      22               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


View the full module info with the info, or info -d command.

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

Top command to see cpu utilization



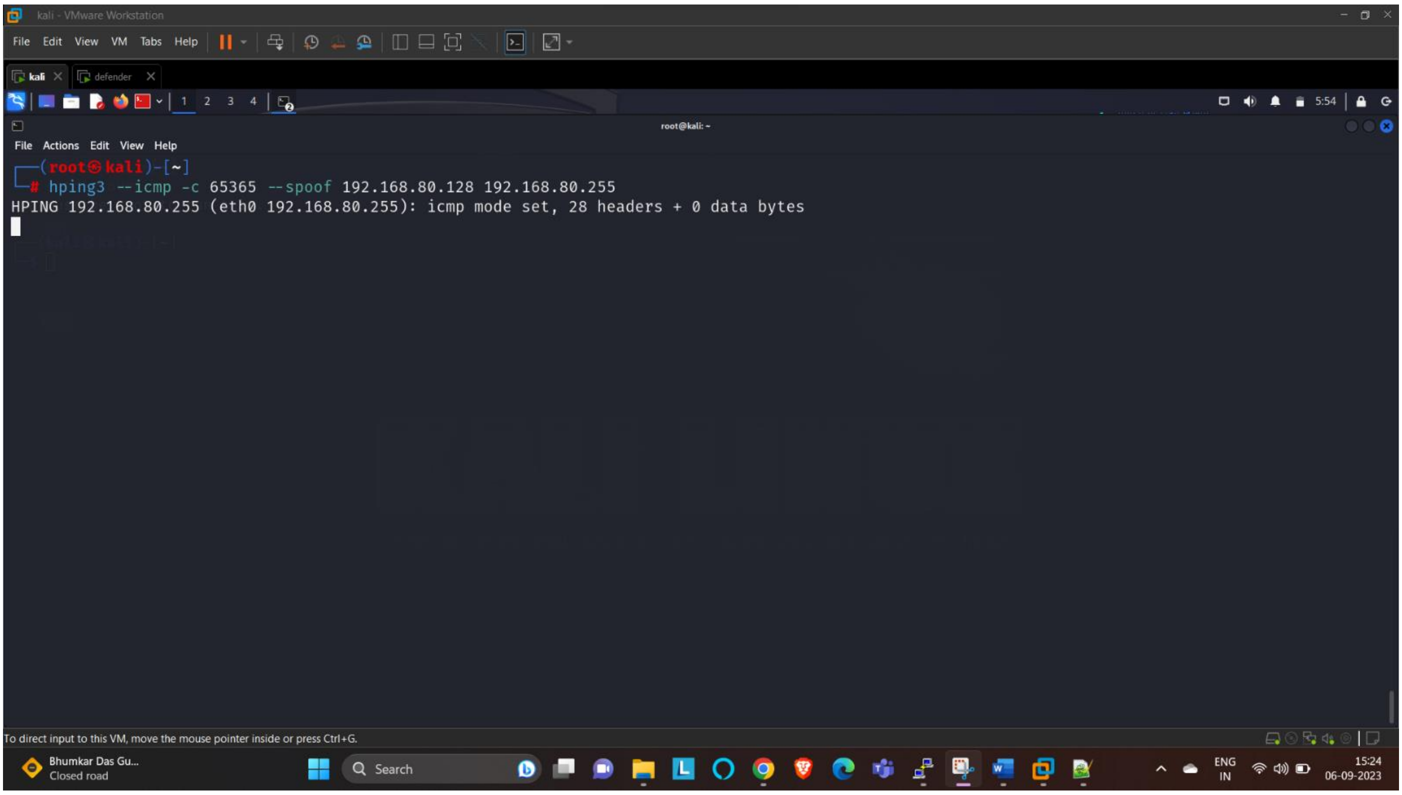
```
top - 14:36:19 up  2:04,  6 users,  load average: 1.60, 0.87, 0.35
Tasks: 126 total,   3 running, 123 sleeping,   0 stopped,   0 zombie
%Cpu(s): 33.7 us, 12.3 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi, 54.0 si,  0.0 st
MiB Mem :   1988.0 total,    576.6 free,    931.0 used,    480.4 buff/cache
MiB Swap:   3815.0 total,   3815.0 free,      0.0 used.    905.9 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   10 root      20   0       0      0      0 R  54.2   0.0   1:20.92 ksoftirqd/0
  910 root      20   0  683976 281452   6960 S  23.3  13.8   0:51.38 snort
 2298 root      20   0  588824 238348   7096 S  10.3  11.7   0:03.97 snort
 2260 root      20   0  590896 255968   7128 S   7.0  12.6   0:13.13 snort
   11 root      20   0       0      0      0 R   4.3   0.0   0:07.68 rcu_sched
 2276 root      20   0       0      0      0 I   0.7   0.0   0:00.39 kworker/0:2-events
    1 root      20   0  103888  10088   7904 S   0.0   0.5   0:01.79 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.97 kworker/0:1H-events_highpri
    9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_bh
   13 root      rt   0       0      0      0 S   0.0   0.0   0:00.10 migration/0
   15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   16 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
   17 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
   18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
   19 root      20   0       0      0      0 S   0.0   0.0   0:00.00 khungtaskd
   20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
   21 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 writeback
   22 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kcompactd0
   23 root      25   5       0      0      0 S   0.0   0.0   0:00.00 ksmd
```

## Snort detection  syn flood



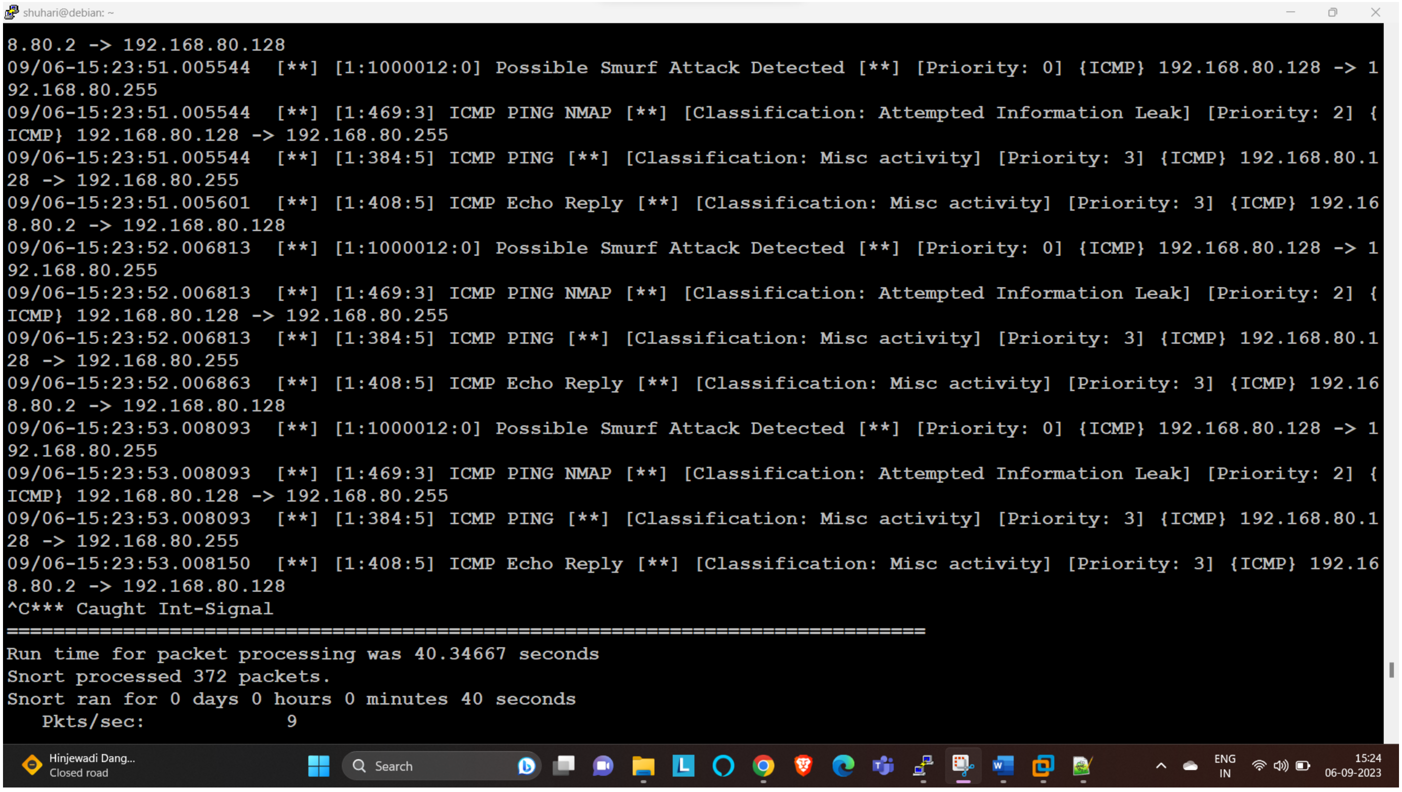
```
           Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=2298)
09/06-14:36:00.483708  [**] [1:100005:0] Possible SYN Flood Detected [**] [Priority: 0] {TCP} 192.168.80.129:1446 -> 1
92.168.80.128:22
09/06-14:36:02.492085  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity] [Priority: 3
] {TCP} 192.168.80.129:0 -> 192.168.80.128:22
09/06-14:36:02.611738  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity] [Priority: 3
] {TCP} 192.168.80.129:0 -> 192.168.80.128:22
09/06-14:36:03.421196  [**] [1:504:7] MISC source port 53 to <1024 [**] [Classification: Potentially Bad Traffic] [Pri
ority: 2] {TCP} 192.168.80.129:53 -> 192.168.80.128:22
09/06-14:36:06.982462  [**] [1:100005:0] Possible SYN Flood Detected [**] [Priority: 0] {TCP} 192.168.80.129:1990 -> 1
92.168.80.128:22
```

## Smurf attack :-



```
┌──(root㉿kali)-[~]
└─# hping3 --icmp -c 65365 --spoof 192.168.80.128 192.168.80.255
HPING 192.168.80.255 (eth0 192.168.80.255): icmp mode set, 28 headers + 0 data bytes
```

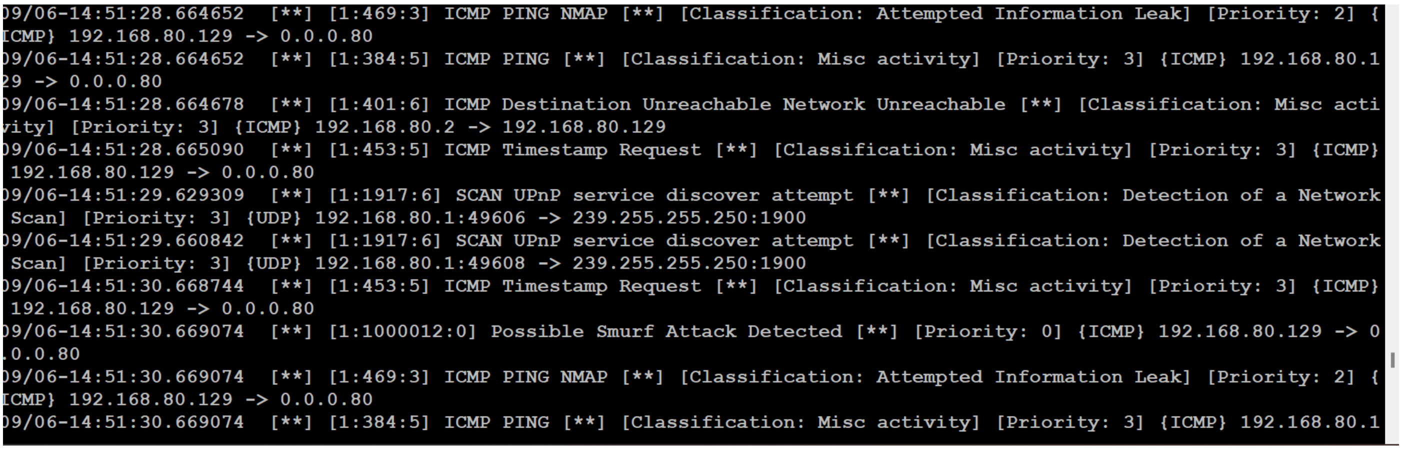
# Snort detection smurf attack



```
8.80.2 -> 192.168.80.128
09/06-15:23:51.005544  [**] [1:1000012:0] Possible Smurf Attack Detected [**] [Priority: 0] {ICMP} 192.168.80.128 -> 1
92.168.80.255
09/06-15:23:51.005544  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.80.128 -> 192.168.80.255
09/06-15:23:51.005544  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.80.1
28 -> 192.168.80.255
09/06-15:23:51.005601  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.16
8.80.2 -> 192.168.80.128
09/06-15:23:52.006813  [**] [1:1000012:0] Possible Smurf Attack Detected [**] [Priority: 0] {ICMP} 192.168.80.128 -> 1
92.168.80.255
09/06-15:23:52.006813  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.80.128 -> 192.168.80.255
09/06-15:23:52.006813  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.80.1
28 -> 192.168.80.255
09/06-15:23:52.006863  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.16
8.80.2 -> 192.168.80.128
09/06-15:23:53.008093  [**] [1:1000012:0] Possible Smurf Attack Detected [**] [Priority: 0] {ICMP} 192.168.80.128 -> 1
92.168.80.255
09/06-15:23:53.008093  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.80.128 -> 192.168.80.255
09/06-15:23:53.008093  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.80.1
28 -> 192.168.80.255
09/06-15:23:53.008150  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.16
8.80.2 -> 192.168.80.128
^C*** Caught Int-Signal
===============================================================================
Run time for packet processing was 40.34667 seconds
Snort processed 372 packets.
Snort ran for 0 days 0 hours 0 minutes 40 seconds
   Pkts/sec:            9
```

# Snort port scanning detection

# Port 80



```
09/06-14:51:28.664652  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.80.129 -> 0.0.0.80
09/06-14:51:28.664652  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.80.1
29 -> 0.0.0.80
09/06-14:51:28.664678  [**] [1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc acti
vity] [Priority: 3] {ICMP} 192.168.80.2 -> 192.168.80.129
09/06-14:51:28.665090  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP}
 192.168.80.129 -> 0.0.0.80
09/06-14:51:29.629309  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network
 Scan] [Priority: 3] {UDP} 192.168.80.1:49606 -> 239.255.255.250:1900
09/06-14:51:29.660842  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network
 Scan] [Priority: 3] {UDP} 192.168.80.1:49608 -> 239.255.255.250:1900
09/06-14:51:30.668744  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP}
 192.168.80.129 -> 0.0.0.80
09/06-14:51:30.669074  [**] [1:1000012:0] Possible Smurf Attack Detected [**] [Priority: 0] {ICMP} 192.168.80.129 -> 0
.0.0.80
09/06-14:51:30.669074  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {
ICMP} 192.168.80.129 -> 0.0.0.80
09/06-14:51:30.669074  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.80.1
```

All attacks prevented by firewall iptables .