Cover sheet for submission of work for assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

UNIT DETAILS

Unit name	Secure Network		Class day/time		Office use only
Unit code	TNE80006	Assignment no.		Due date	
Name of lecturer/teacher					
Tutor/marker's name					Faculty or school date stamp

STUDENT(S)

	Family Name(s)	Given Name(s)	Student ID Number(s)
(1)	Khanal	Bikesh Nath	101985810
(2)			
(3)			
(4)			
(5)			
(6)			

DECLARATION AND STATEMENT OF AUTHORSHIP

1. I/we have not impersonated, or allowed myself/ourselves to be impersonated by any person for the purposes of this assessment.
2. This assessment is my/our original work and no part of it has been copied from any other source except where due acknowledgement is made.
3. No part of this assessment has been written for me/us by any other person except where such collaboration has been authorised by the lecturer/teacher concerned.
4. I/we have not previously submitted this work for this or any other course/unit.
5. I/we give permission for my/our assessment response to be reproduced, communicated, compared and archived for plagiarism detection, benchmarking or educational purposes.

I/we understand that:

6. Plagiarism is the presentation of the work, idea or creation of another person as though it is your own. It is a form of cheating and is a very serious academic offence that may lead to exclusion from the University. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited.

Student signature/s

I/we declare that I/we have read and understood the declaration and statement of authorship.

(1)	Bikesh Nath Khanal	(4)	
(2)		(5)	
(3)		(6)	

Further information relating to the penalties for plagiarism, which range from a formal caution to expulsion from the University is contained on the Current Students website at **www.swin.edu.au/student/**

Contents

Introduction

Scenario Discussion

SportClothes-IT-ALL is emerging textile company which is planning to execute an online shopping portal to manage the customers demand. For this the company is planning to host the popular and open source web server known as Apache-2 web server on Linux based environment (CentOS machine). After some testing's and with very little knowledge about network security the new system administrator trainee has launched the web server to the internet with no internet security which is vulnerable to many possible threats and attacks from outside and inside attackers (within organizations). After somedays of monitoring it was noticed that some PCS with trusted IP has been scanning for open TCP ports. This shows that the company's web server is in possible threat of attack.

As a senior network systems administrator, I am proposing the possible threats to the company's network with the appropriate security solutions.

Possible threats to Linux server and their solutions

- Root login (login with administrative privilege)
  The person wise enough to scan the TCP ports from within a system if able to root access the system than this attacker can easily modify the device configuration and can generate any type of packet from the system or can find details such as Source or MAC address from packets. Free Password cracking software such as John the Ripper which combines many other password crackers into one package can be used for cracking the password.
  The solution for this threat is to disable the root login or giving an administrative permission to another administrative user.
- Secure shell (SSH) login with root privilege
  SSH is remotely accessing the system through the secure authentication procedures. If hacker gain remote root access to the system with brute force attack than the system is no more trustworthy. The best practice is disabling the root login as well as SSH access.
- Internet Control Message Protocol (ICMP)
  Attacker initiates the attack with discovering the devices and server with ping. So, using application such as Firestarter with ICMP filtering ticked can help to hide the server from unnecessary pinging.
- USB ports
  The attacker gaining access to the system or workstations can easily plugin the USB to the any of the PCS accessible and leave malicious software or can copy the confidential information of the system such as network structures. Disabling the USB port in any user PC can mitigate this problem
- Unused ports and services
  There are 65535 ports and different services running on them. Such as HTTP on port 80, 23 telnet, 22 SSH, 53 DNS etc. All the ports and services are not in use. Examining the unused ports and services and shutting them down can be the best option to protect the system.

Possible threats to Apache web server and their solutions

- Server Fingerprinting
  Using software such as NMAP where attacker can easily find the information like open ports, server type, running OS etc.
  Using honeyd can mislead the attacker and can help to trap them.

- Input validation
  The web application should properly handle the data which is received from clients and users. Always validate the user data before using on server otherwise it may be cause for cross-site scripting, Sql injection or buffer overflow.

- Daniel service of attack (DOS)
  Attackers send too many syn packets to the server in which the server ran out of memory, RAM, CPU, Bandwidth etc. and finally server crashes.

- Distributed service of attack (DDOS)
  DDOS attack is the most common attack happening in the world in which the attacker can flood the system or server with help of other compromised system at same time. The attacker sends the traffic from multiple compromised systems as server and shut the server down.

- Reflected DDOS
  In reflected DDOS many public servers such as Yahoo, google are sent a TCP sun such as victims IP is source IP address in that packet so as in response to that the servers sent the TCP ack/syn packets to the server at the same time. In which the victim server cannot handle much packets eventually server crashes.

- Buffer overflow
  Improper coding techniques may lead to overrun the memory buffer or writing data into adjacent memory eventually causing service crash. In worst case it allows remote execution of code with admin privileges which has full control over the system. Proper coding techniques can eradicate this threat.

  <u>Mitigation</u>

- Checking and cleaning the inputs from the web applications.
- Implementing web application firewall such as ModSecurity, Firestarter etc.
- Making sure there is enough RAM, CPU and memory for operating server.
- If possible, use cloud-based scrubbing to filter the unwanted traffic out.
- Using more than one server acting as one with distributed services such as load sharing and fail over.
- Allow server to keep minimal state during 3-way handshake.

Possible threats to Network and their solutions

- Ip spoofing
  When attacker uses the IP address of the host as source address, sending the spoofed packet to another host and the receiving host can send response to the real host. It is base for initiating DoS attack.
  Implementing BCP48 or letting packets exit the network with valid source address can prevent attackers.

- Content Addressable Memory (CAM table Poisoning)
  Switches have CAM table where ports to Mac addresses are stored. Attacker fill CAM table with bogus MAC addresses so as switch act like hub. This leads to MAC flooding.
  Implementing proper port security with limiting the MAC addresses per port can help mitigating this problem.

- Secure Socket Layer (SSL) attack
  SSL is used for encrypted connection between browser and web server. This link is also vulnerable to attackers as they can access cookies, Passwords and other data.

- Domain Name System (DNS) attack:
  DNS can have IP address to domain name stored. Attacker can poison the DNS server and redirect the traffic to where the attacker designed to mislead the victims. This way customers can be redirect to attacker website and attacker can get personal and bank details of customers.

- Network Scanning
  First thing Attackers can scan the whole network with tools such as NMAP, NESSUS, Hping, etc. They acquire every detail about network infrastructures which help them in attacking. So, minimizing those threats and hiding those details which are displayed is the first things which should be considered.

Network drawing

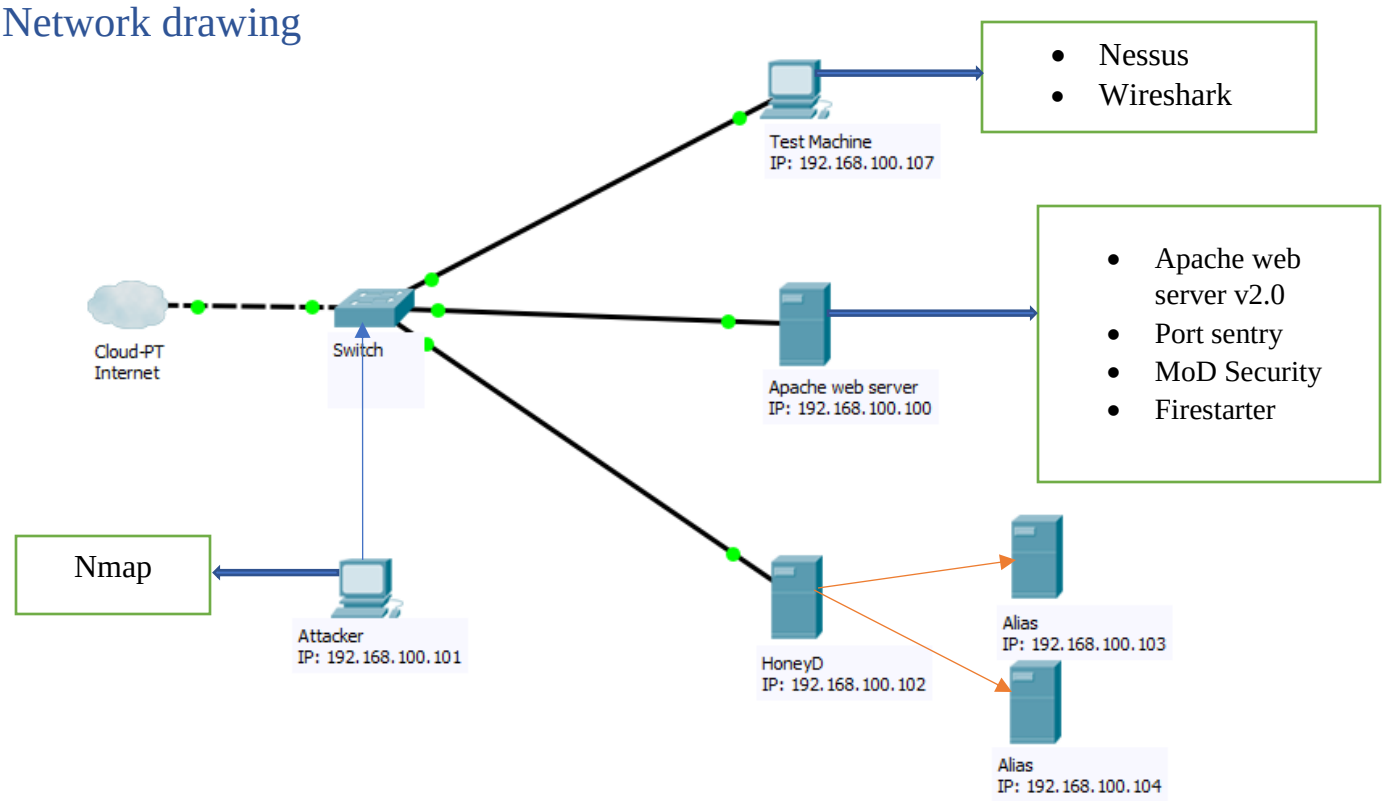


Fig: Network Diagram

Design Discussion

As above diagram stated that I have used four main machines.

1. Test Machine
2. Web server with apache server installed
3. Attacker and
4. Honeyd Server hosting multiple honeypots

Devices	Tool installed	Ip address
Web server	Apache web server v2.0 Port sentry MoDSecurity Firestarter	192.168.100.100
Attacker	Nmap	192.168.100.101
Test Machine	Nessus Wireshark	192.168.100.107
FreeBSD (Honeyd)	Honeyd	192.168.100.102 192.168.100.103(alias) 192.168.100.104(alias)

As above table show I have implemented Apache web server and some security tools to protect it. Details about security Tools used are described below.

Apache web server v2.0

It is the most successful and commonly used server with flexible modular architectures.

MoD Security

It is open source free web application firewall. It provides additional security to which helps in finding the attack prior to reaching web applications. Its importance is Real-time monitoring, access control and Hardening rules for web application.

It is mainly used to give security to apache server from attacks such as XSS and SQL injections.

Port sentry

It is a program implemented on a single host which listens to the TCP synchronizations packets send to the unused ports of the host. It works on two mode Basic for normal TCP and UDP port monitoring and Stealth mode for other types such as synchronizations.

I have used this tool in a web server machine to monitor the real time port scanning of the TCP/UDP ports by tools such as NMAP.

Nessus

This tool is the network vulnerabilities scanner and it is used to detect the weakness in any system setting the appropriate system.

I have installed Nessus in Test machine to detect the weakness in a server.

Wireshark

Wireshark is used to analyze the packet movement in a network. While set on promiscuous mode, Wireshark can scan the traffic of whole network.

I have installed Wireshark in Test machine to monitor the traffic in and out of the network.

Firestarter

Firestarter is a tool to manipulate the inbuild firewall in a system. It can be used to allow or deny the specific network traffic setting policies.

I have used Firestarter to manipulate the firewall and used to control ICMP broadcasting and allowing only HTTP request in a server.

NMAP (Network Mapper)

Nmap is the free tool used to identify network host, what services host are offering through different ports, which OS versions host are Using etc.

I have installed this tool as an attacker to find out necessary details about server OS, unused ports etc. which are helpful to plan the attack.

HoneyD

It is a free server that is capable of creating multiple other alias with other IP addresses on same subnet.

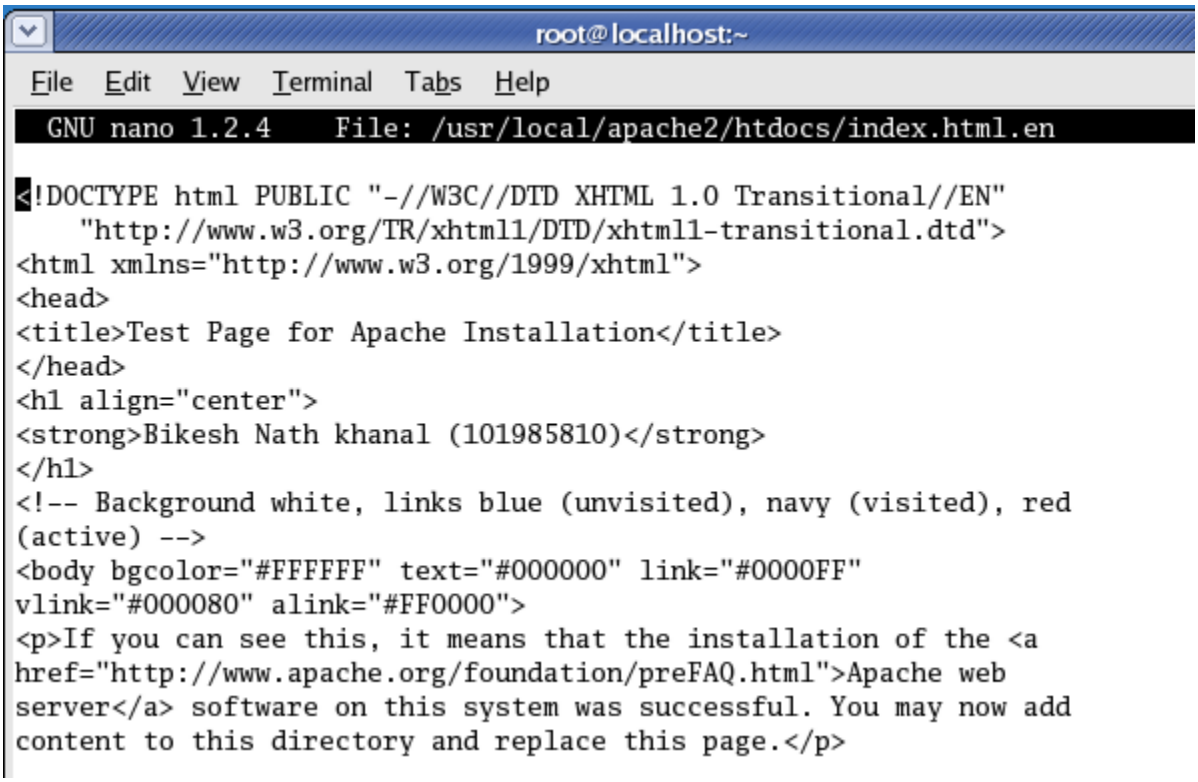
I have installed this server to mislead the attacker with unnecessary and irrelevant information.

Device configuration summary

Apache web server V2.0

Successful installation of this web server will host SportClothes-IT-All company website under /usr/local/apache2/htdocs. For prototyping, I have used the index.html webpage under htdocs to implement webpage with my Name and Student ID with company name. To change the index.html.en file on htdocs command used is nano /usr/local/apache2/htdocs/index.html.en.

To run server: /usr/local/apache2/bin/apachectl start.



Mod security

First running server need to be stopped with command /usr/local/apache2/bin/apachectl stop.

Then reconfigure apache with command ./configure –enable-unique-id ; make; make install. Install modsecurity by adding line top_dir = /usr/local/apache2 to MakeFile located in modsecurity/apache2. Now install without ./configure. At last add 3 line as shown below in httpd.conf file.

```
root@localhost:/usr/local/apache2/htdocs
File  Edit  View  Terminal  Tabs  Help
  GNU nano 1.2.4      File: /usr/local/apache2/conf/httpd.conf

# have to place corresponding `LoadModule' lines at this location
# directives contained in it are actually available _before_ they
# Statically compiled modules (those listed by `httpd -l') do not
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadFile /usr/lib/libxml2.so
LoadModule security2_module modules/mod_security2.so
include conf/modsecurity/*.conf
#
```

Portsentry

It is installed in a different way using command as make; make Linux; make install.

After this slight modification to file portsentry.conf located in /usr/local/psionic/portsentry in iptables section.

```
# iptables support for Linux
KILL_ROUTE="/sbin/iptables •I INPUT -s $TARGET$ •j DROP"
```

```
root@localhost:/usr/local/apache2/htdocs
File  Edit  View  Terminal  Tabs  Help
  GNU nano 1.2.4  File: ...r/local/psionic/portsentry/portsentry.conf

# iptables support for Linux
KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"
#
```

And adding # in following line on TCP wrappers section as.

```
# KILL_HOSTS_DENY="ALL: $TARGET$"
```

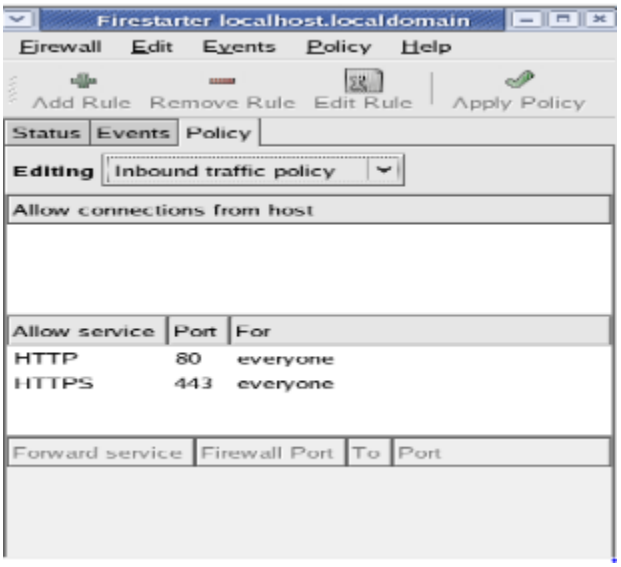
```
root@localhost:/usr/local/apache2/htdocs
File  Edit  View  Terminal  Tabs  Help
  GNU nano 1.2.4  File: ...r/local/psionic/portsentry/portsentry.conf

# TCP Wrappers#
###############
# This text will be dropped into the hosts.deny file for wrappers
# to use. There are two formats for TCP wrappers:
#
# Format One: Old Style - The default when extended host processing
# options are not enabled.
#
#KILL_HOSTS_DENY="ALL: $TARGET$"
```

Now running Portsentry in stealth detection mode:

```
/usr/local/psionic/portsentry/portsentry -atcp
/usr/local/psionic/portsentry/portsentry -audp
```

Firestarter

Firestarter is installed on Linux web server with policies allowing all HTTP and HTTPS services via port 80 and 443.



Nmap

Nmap is installed using same commands as ./configure;make;make install.

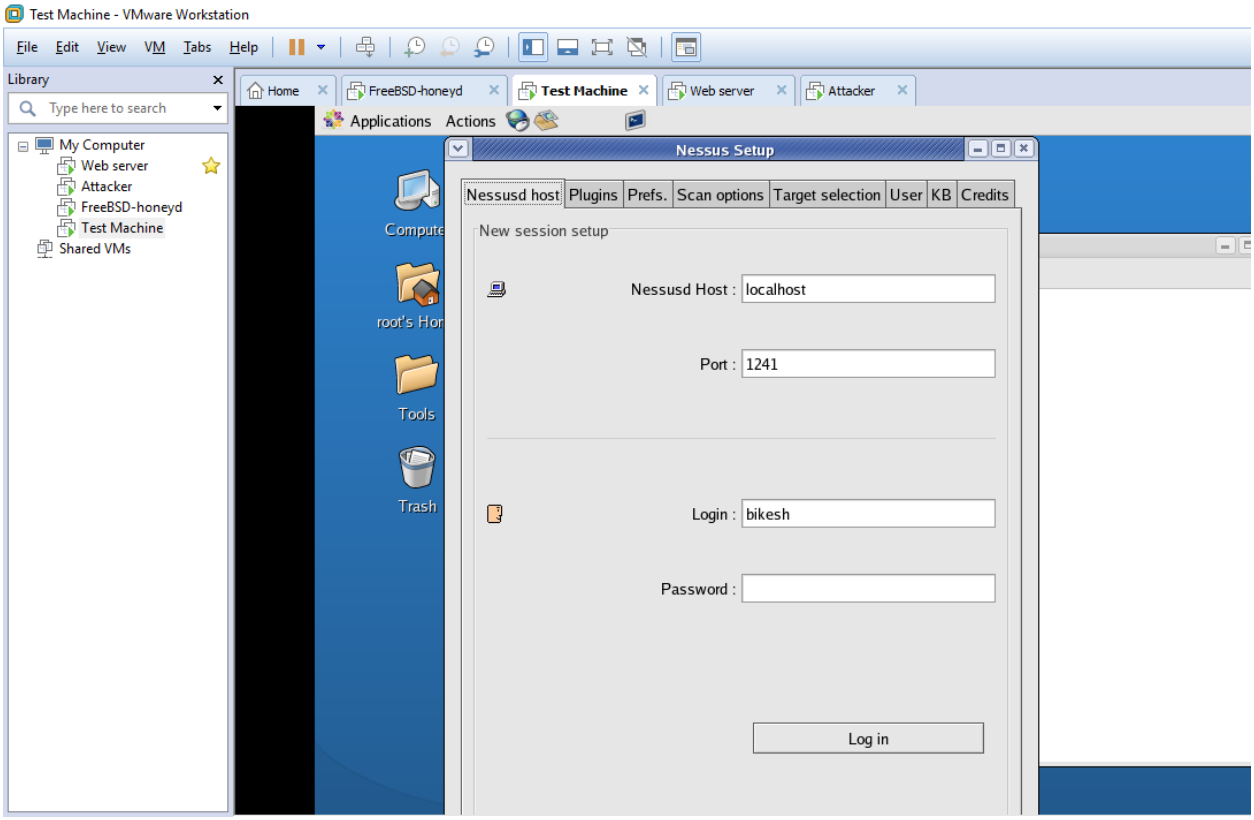
Nessus

Nessus can be installed with help of four set of files nessus-libraries, libnasl, nessus-core and nessus-plugins. summary for installations are:

1. Extract all four set of files and installing them with ./configure;make;make install except for libraries. For libraries following editing should be done at first before compiling others.

   Edit the file: */etc/ld.so.conf*
   add an extra line: /usr/local/lib
   and type *ldconfig*

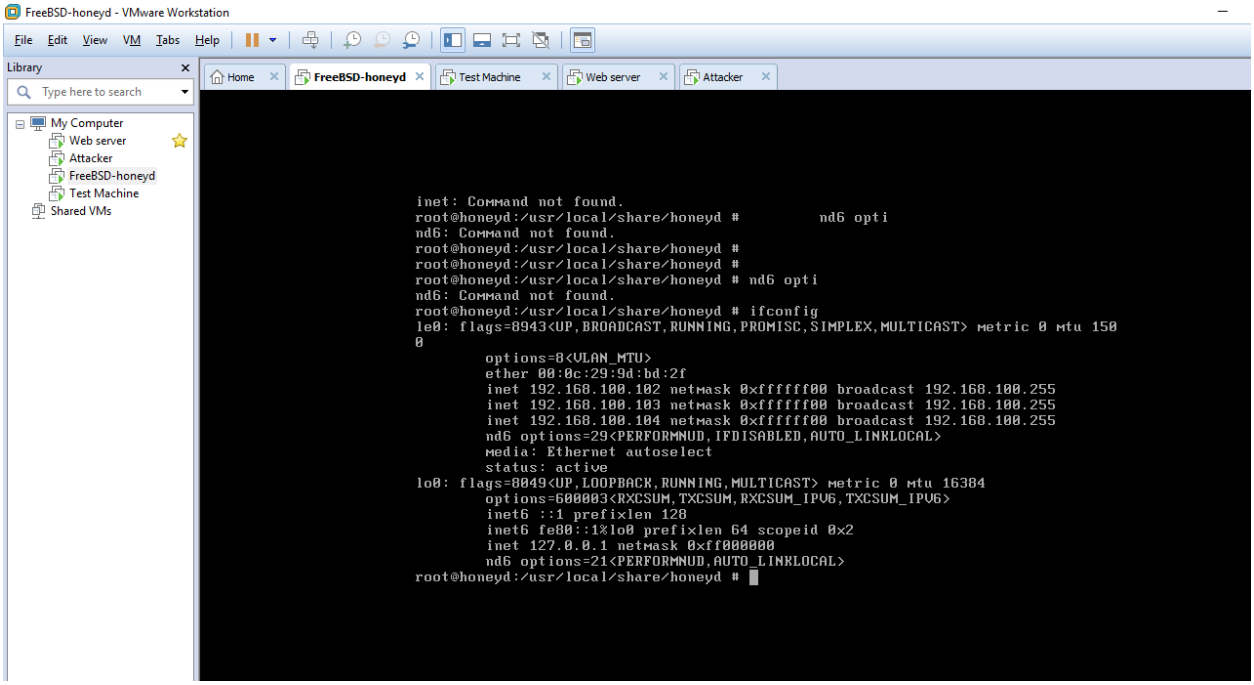
2. Making certificate: /usr/local/sbin/nessus-mkcert.
3. Adding user: /usr/local/sbin/nessus-asduser.
4. Start nessus server with nessusd command.
5. Start nessus gui with nessus command.



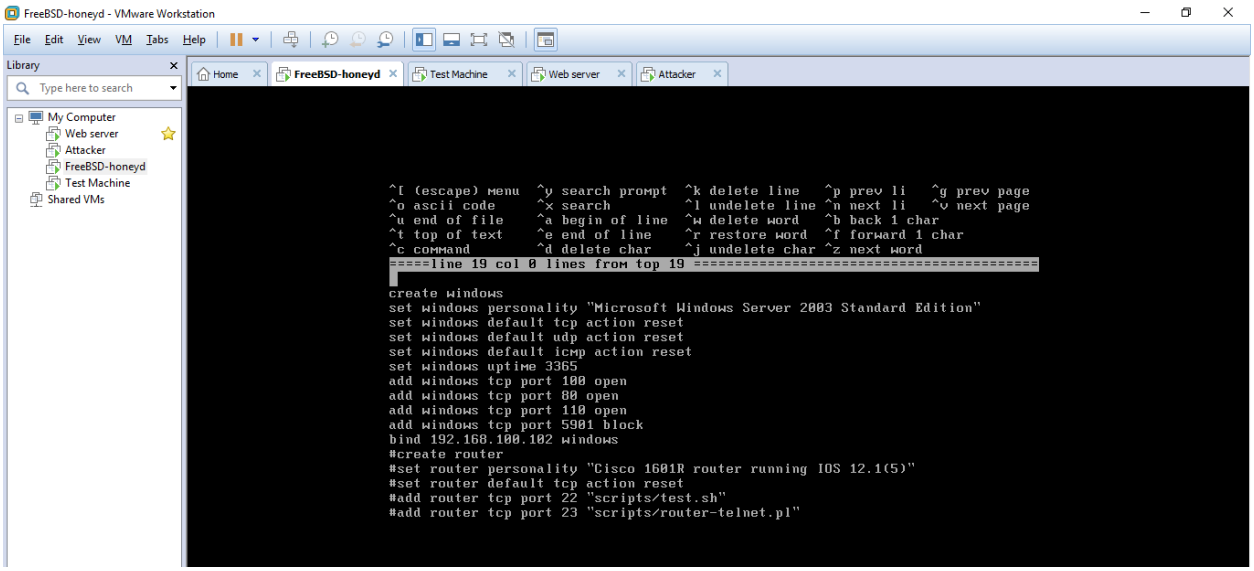
Wireshark and NMAP can be installed with same command as ./comfigure;make ;make install.

Honeyd

I have set FreeBSD ip address to 192.168.100.102 and two alias with ip address 192.168.100.103 and 192.168.100.104 as shown in figure.



Config.sample has been configured with following template.



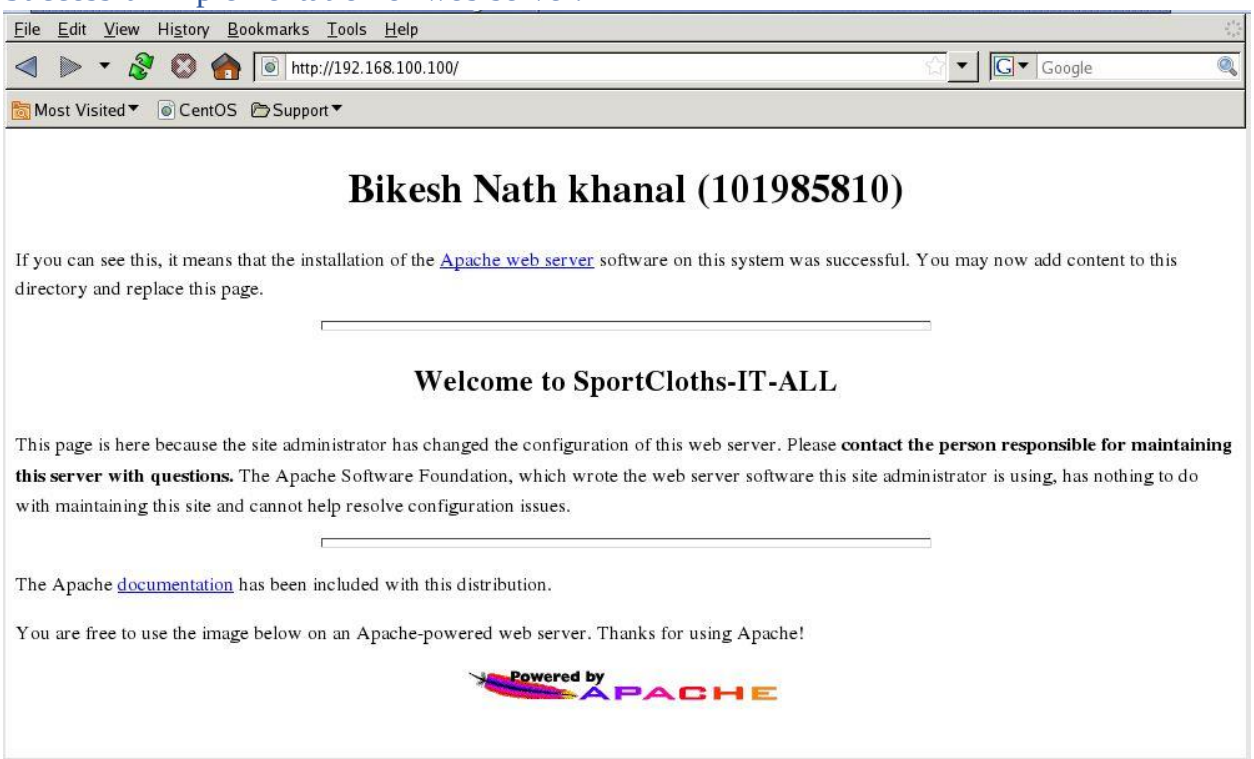
For running honeyd command honeyd -d -i le0 -f config.sample is used.

Testing Plan

Threats	Mitigation	Device configured	Commands
Fingerprinting	Portsentry, Honeyd	Web server Machine	honey -d -I le0 -f confing.sample to run Honeyd Portsentry in stealth scan detection /usr/local/psionic/portsentry/portsentry -atcp /usr/local/psionic/portsentry/portsentry –audp
SQL injection and Cross-site Scripting	Modsecurity	Web server Machine	ModSecurity Rules
Buffer Overflow,	ModSecurity	Web server Machine	ModSecurity Rules
DDOS, DoS, RDos	Firestarter,portsentry	Web server Machine	Allow TCP Port 80 and HTTPS service from Port 443 Portsentry in stealth scan detection /usr/local/psionic/portsentry/portsentry -atcp /usr/local/psionic/portsentry/portsentry –audp
IP spoofing	Wireshark	Test machine	Run wireshark in promiscuous mode to monitor all network traffic
CAM table and ARP poisoning	Port security	Ports (Switches)	Portsecurity command as: switchport portsecurity mac-address max N switchport portsecurity violation shutdown
Network Scan	Portsentry, honeyd	Web server Machine	honey -d -I le0 -f confing.sample to run Honeyd Portsentry in stealth scan detection /usr/local/psionic/portsentry/portsentry -atcp /usr/local/psionic/portsentry/portsentry –audp
ICMP broadcast	Firestarter	Web server Machine	ICMP filtering in Firestarter tcked.

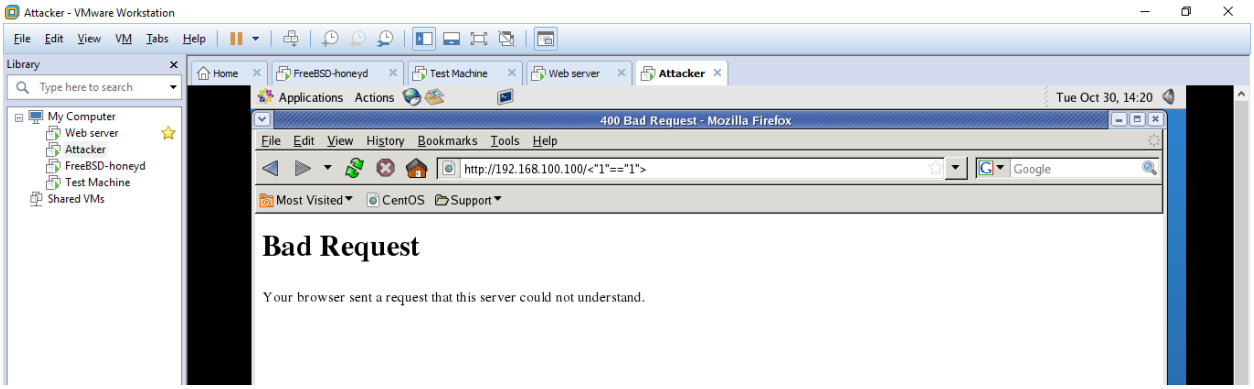
Unused Ports	Switch security, Nessus	Switch, Test Machine	Run “nessusd” daemon, and “nessus” client and scan for vulnerabilities.
Root login/ SSH login	Policies	Host	Implement policies while setting passwords

Successful implementation of web server.



After installing mod security.

Trying scripting.



Monitoring with modsecurity.

```
root@localhost:~
File  Edit  View  Terminal  Tabs  Help
[root@localhost ~]# tail -f /usr/local/apache2/logs/modsec_audit.log

--a86f542e-H--
Message: Access denied with code 400 (phase 2). Pattern match "^[\\d\\.]+$" at R
EQUEST_HEADERS:Host. [id "960017"] [msg "Host header is a numeric IP address"] [
severity "CRITICAL"]
Action: Intercepted (phase 2)
Stopwatch: 1540869479105749 1765 (879 1195 -)
Producer: ModSecurity v2.1.3 (Apache 2.x)
Server: Apache

--a86f542e-Z--

--a86f542e-A--
[30/Oct/2018:14:19:41 +1100] qBFQIn8AAAEAACdMBDgAAAAB 192.168.100.101 44788 192.168.100.100 80
--a86f542e-B--
GET /%3C%221%22==%221%22%3E HTTP/1.1
Host: 192.168.100.100
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.7) Gecko/2009042018 CentOS/3.0.7-3.el4.centos Firefox/3.0.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

--a86f542e-F--
HTTP/1.1 400 Bad Request
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Nmap Web server from attacker.

```
root@localhost:~/Desktop/Tools/nmap-4.00
File  Edit  View  Terminal  Tabs  Help
[2]+  Stopped                 man nmap
[root@localhost nmap-4.00]# nmap -sV 192.168.100.100

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2018-10-17 21:15 EST
Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nm
ap-services for security and consistency reasons.  set NMAPDIR=. to give priorit
y to files in your local directory (may affect the other data files too).
Interesting ports on 192.168.100.100:
(The 1668 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 3.9p1 (protocol 1.99)
80/tcp  open  http    Apache httpd
111/tcp open  rpcbind  2 (rpc #100000)
777/tcp open  status   1 (rpc #100024)
MAC Address: 00:0C:29:CB:B0:1D (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 29.620 seconds
[root@localhost nmap-4.00]# nmap -sP 192.168.100.100

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2018-10-17 21:16 EST
Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nm
ap-services for security and consistency reasons.  set NMAPDIR=. to give priorit
y to files in your local directory (may affect the other data files too).
Host 192.168.100.100 appears to be up.
```

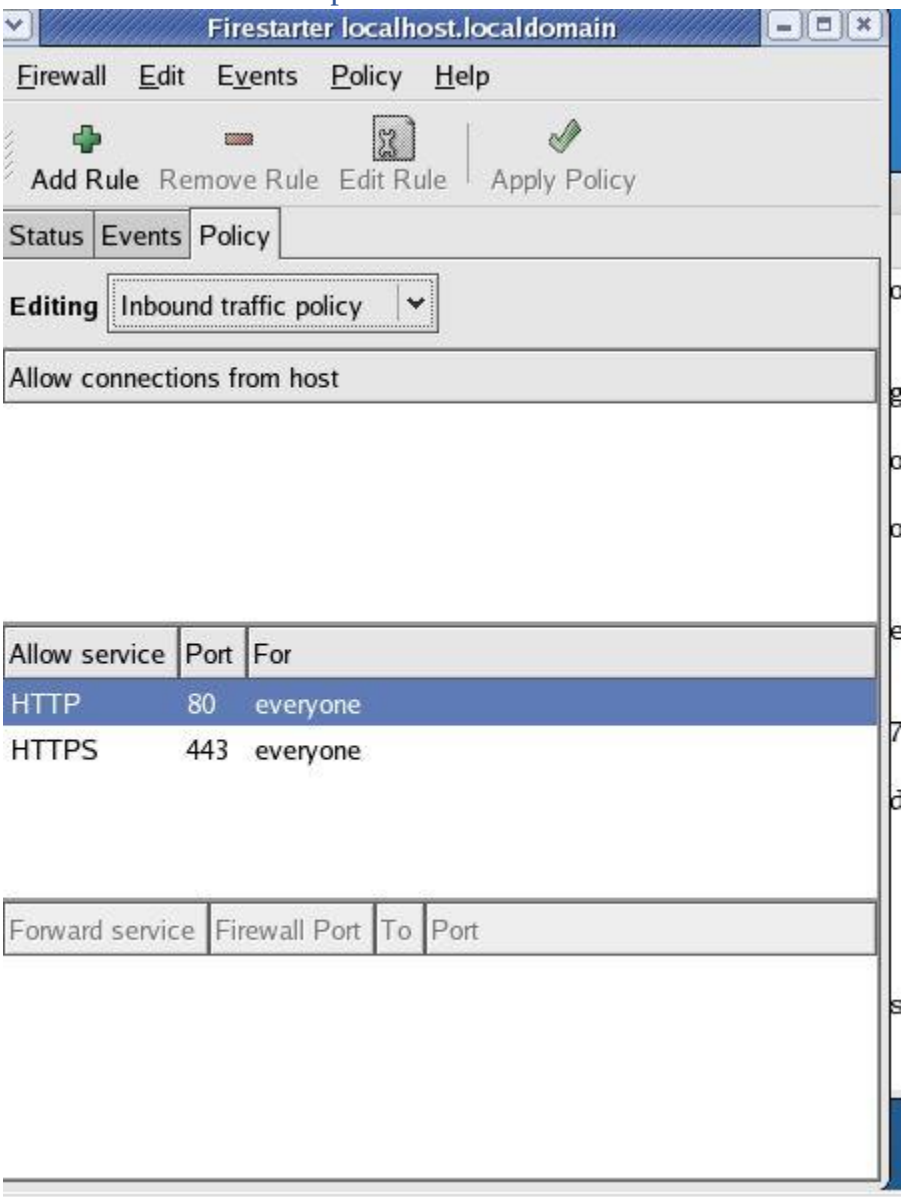
OS detection of web server

```
root@localhost:~/Desktop/Tools/nmap-4.00
File  Edit  View  Terminal  Tabs  Help

Nmap finished: 1 IP address (1 host up) scanned in 17.254 seconds
[root@localhost nmap-4.00]# nmap -O 192.168.100.100
Warning: File ./nmap-os-fingerprints exists, but Nmap is using /usr/local/share/
nmap/nmap-os-fingerprints for security and consistency reasons.  set NMAPDIR=. t
o give priority to files in your local directory (may affect the other data file
s too).

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2018-10-17 21:36 EST
Interesting ports on 192.168.100.100:
(The 1668 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
777/tcp open  unknown
MAC Address: 00:0C:29:CB:B0:1D (VMware)
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11
Uptime 0.050 days (since Wed Oct 17 20:23:52 2018)

Nmap finished: 1 IP address (1 host up) scanned in 19.352 seconds
[root@localhost nmap-4.00]#
```

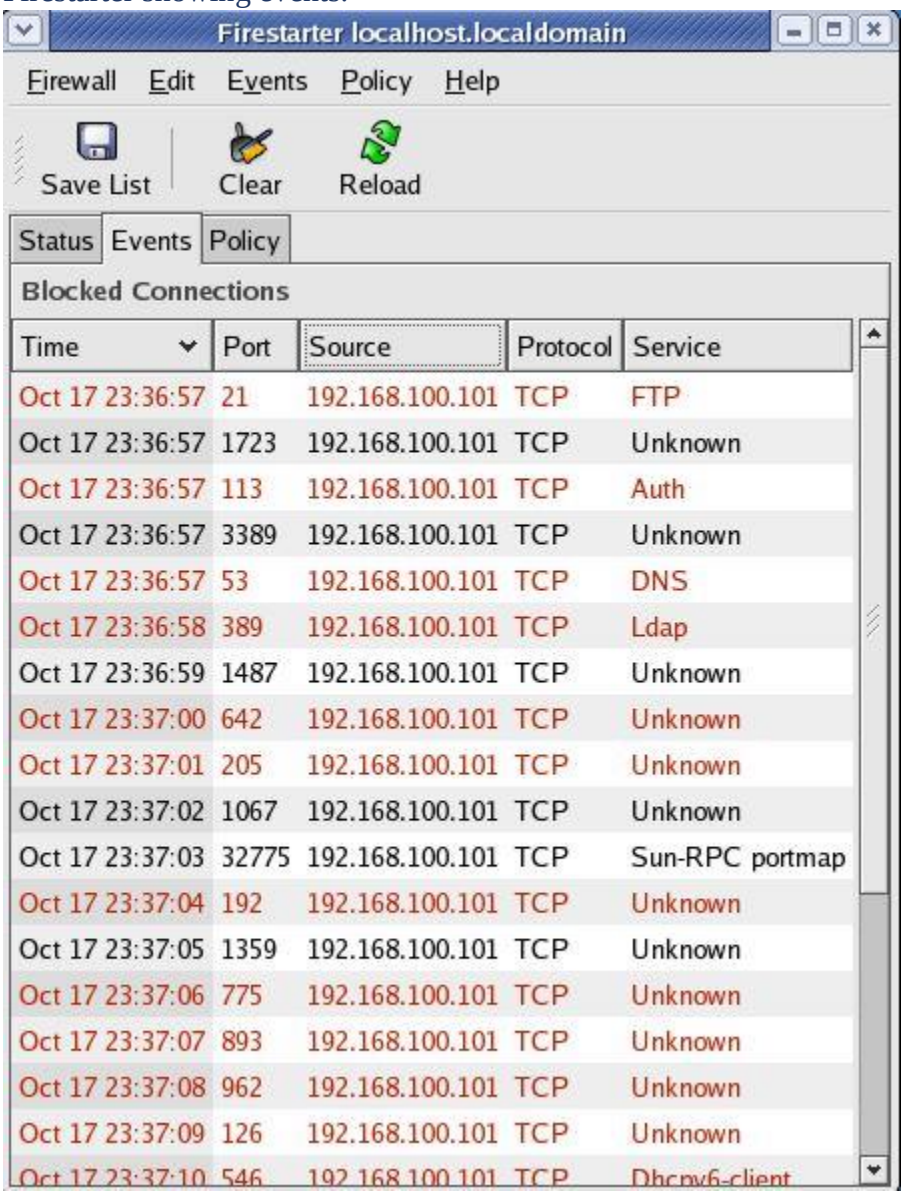
Portsentry dropping packet from attacker.

```
root@localhost:/usr/local/psionic/portsentry
File  Edit  View  Terminal  Tabs  Help
Oct 18 01:29:32 localhost kernel: Inbound IN=eth0 OUT= MAC=00:0c:29:cb:b0:1d:00:0c:29:2
f:09:fe:08:00 SRC=192.168.100.101 DST=192.168.100.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64
ID=48680 DF PROTO=TCP SPT=36379 DPT=1723 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 18 01:29:32 localhost kernel: Inbound IN=eth0 OUT= MAC=00:0c:29:cb:b0:1d:00:0c:29:2
f:09:fe:08:00 SRC=192.168.100.101 DST=192.168.100.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64
ID=43487 DF PROTO=TCP SPT=36381 DPT=389 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 18 01:29:32 localhost kernel: Inbound IN=eth0 OUT= MAC=00:0c:29:cb:b0:1d:00:0c:29:2
f:09:fe:08:00 SRC=192.168.100.101 DST=192.168.100.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64
ID=16860 DF PROTO=TCP SPT=36382 DPT=636 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 18 01:29:32 localhost kernel: Inbound IN=eth0 OUT= MAC=00:0c:29:cb:b0:1d:00:0c:29:2
f:09:fe:08:00 SRC=192.168.100.101 DST=192.168.100.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64
ID=61350 DF PROTO=TCP SPT=36383 DPT=256 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 18 01:29:33 localhost kernel: Inbound IN=eth0 OUT= MAC=00:0c:29:cb:b0:1d:00:0c:29:2
f:09:fe:08:00 SRC=192.168.100.101 DST=192.168.100.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64
ID=30536 DF PROTO=TCP SPT=36384 DPT=256 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 18 01:29:33 localhost kernel: Inbound IN=eth0 OUT= MAC=00:0c:29:cb:b0:1d:00:0c:29:2
f:09:fe:08:00 SRC=192.168.100.101 DST=192.168.100.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64
ID=51239 DF PROTO=TCP SPT=36385 DPT=636 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 18 01:29:33 localhost portsentry[3199]: attackalert: TCP SYN/Normal scan from host:
 192.168.100.101/192.168.100.101 to TCP port: 443
Oct 18 01:29:33 localhost portsentry[3199]: attackalert: Host 192.168.100.101 has been
blocked via dropped route using command: "/sbin/iptables -I INPUT -s 192.168.100.101 -j
 DROP"
```

Installation of Firestarter with policies.

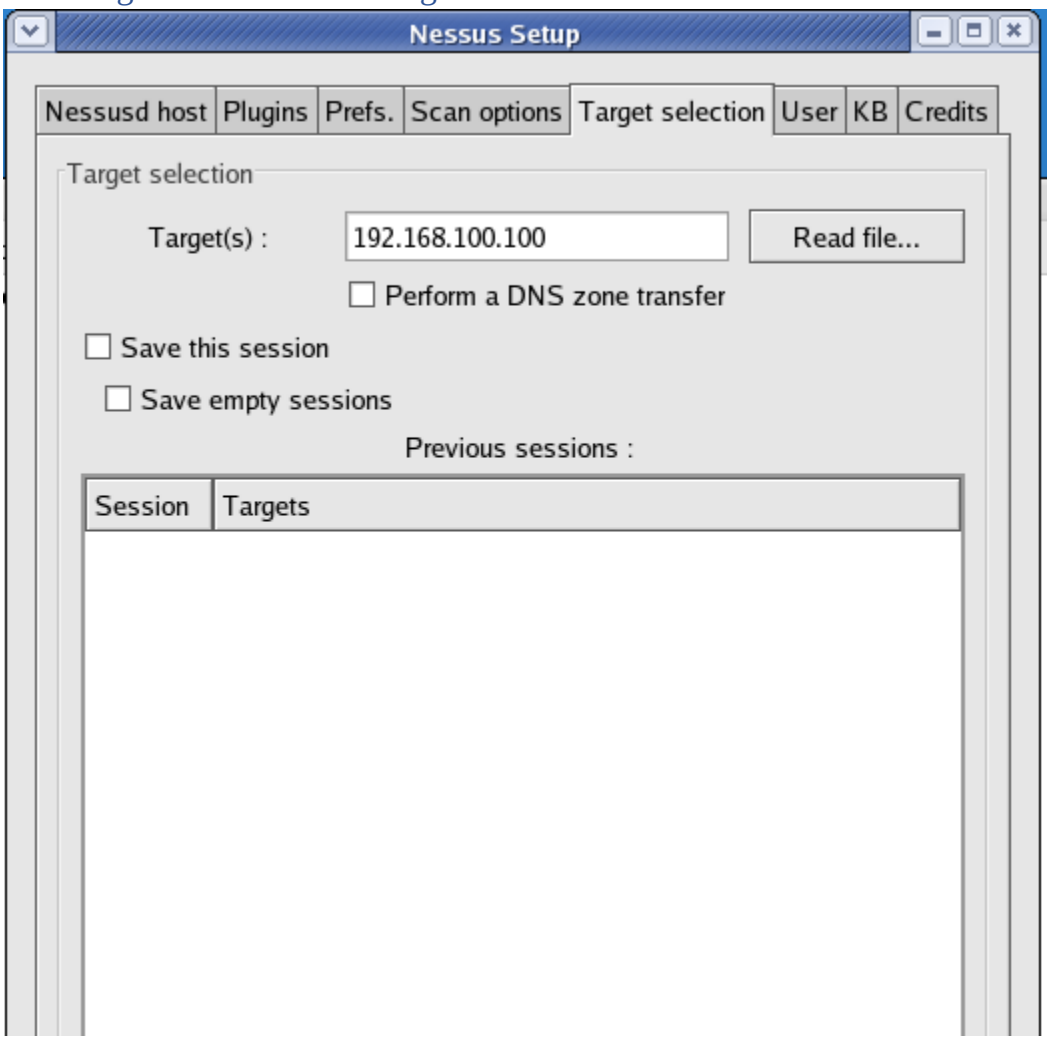


Firestarter showing events.



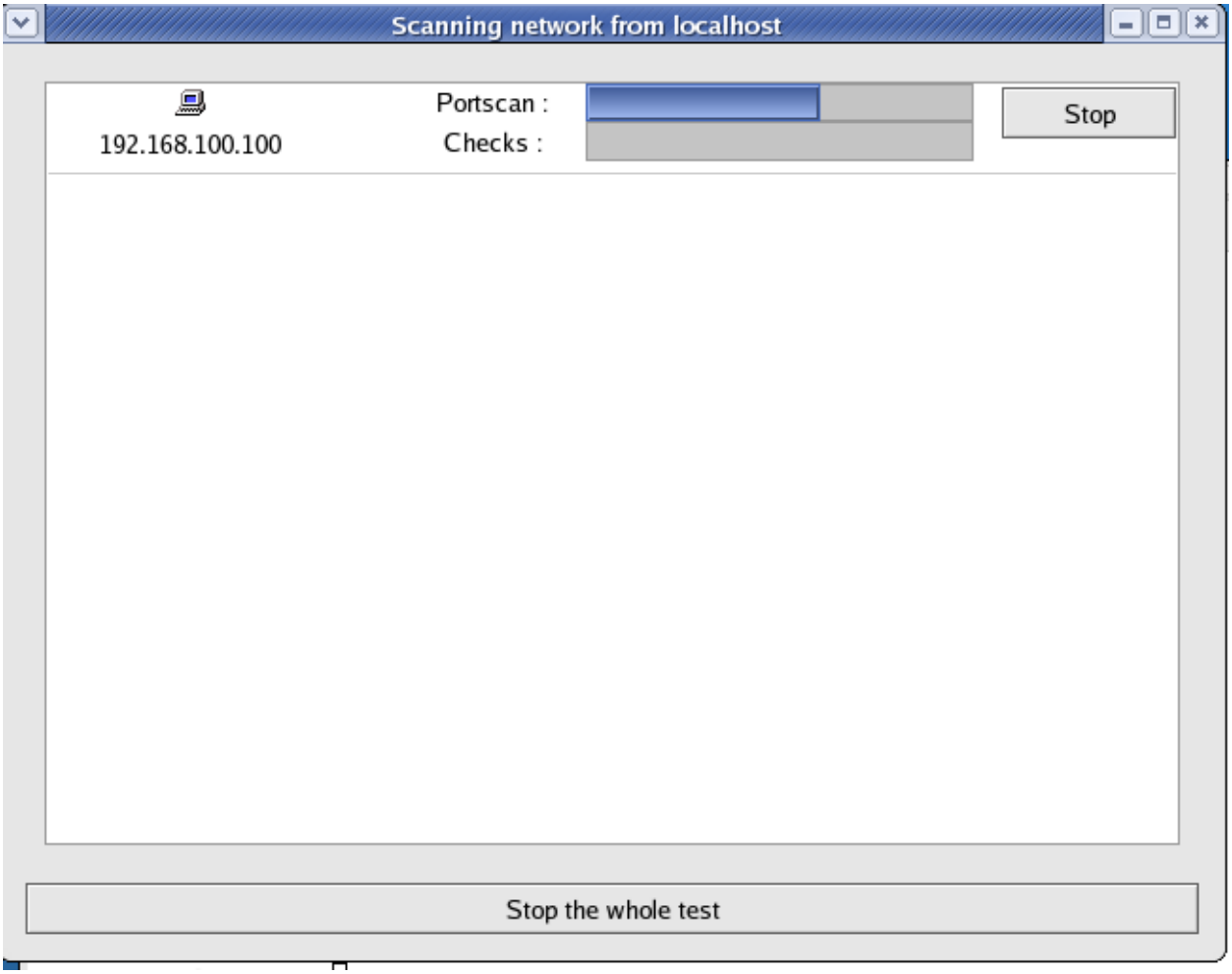
Time	Port	Source	Protocol	Service
Oct 17 23:36:57	21	192.168.100.101	TCP	FTP
Oct 17 23:36:57	1723	192.168.100.101	TCP	Unknown
Oct 17 23:36:57	113	192.168.100.101	TCP	Auth
Oct 17 23:36:57	3389	192.168.100.101	TCP	Unknown
Oct 17 23:36:57	53	192.168.100.101	TCP	DNS
Oct 17 23:36:58	389	192.168.100.101	TCP	Ldap
Oct 17 23:36:59	1487	192.168.100.101	TCP	Unknown
Oct 17 23:37:00	642	192.168.100.101	TCP	Unknown
Oct 17 23:37:01	205	192.168.100.101	TCP	Unknown
Oct 17 23:37:02	1067	192.168.100.101	TCP	Unknown
Oct 17 23:37:03	32775	192.168.100.101	TCP	Sun-RPC portmap
Oct 17 23:37:04	192	192.168.100.101	TCP	Unknown
Oct 17 23:37:05	1359	192.168.100.101	TCP	Unknown
Oct 17 23:37:06	775	192.168.100.101	TCP	Unknown
Oct 17 23:37:07	893	192.168.100.101	TCP	Unknown
Oct 17 23:37:08	962	192.168.100.101	TCP	Unknown
Oct 17 23:37:09	126	192.168.100.101	TCP	Unknown
Oct 17 23:37:10	546	192.168.100.101	TCP	Dhcpv6-client

Installing Nessus and Scanning network vulnerabilities for server.

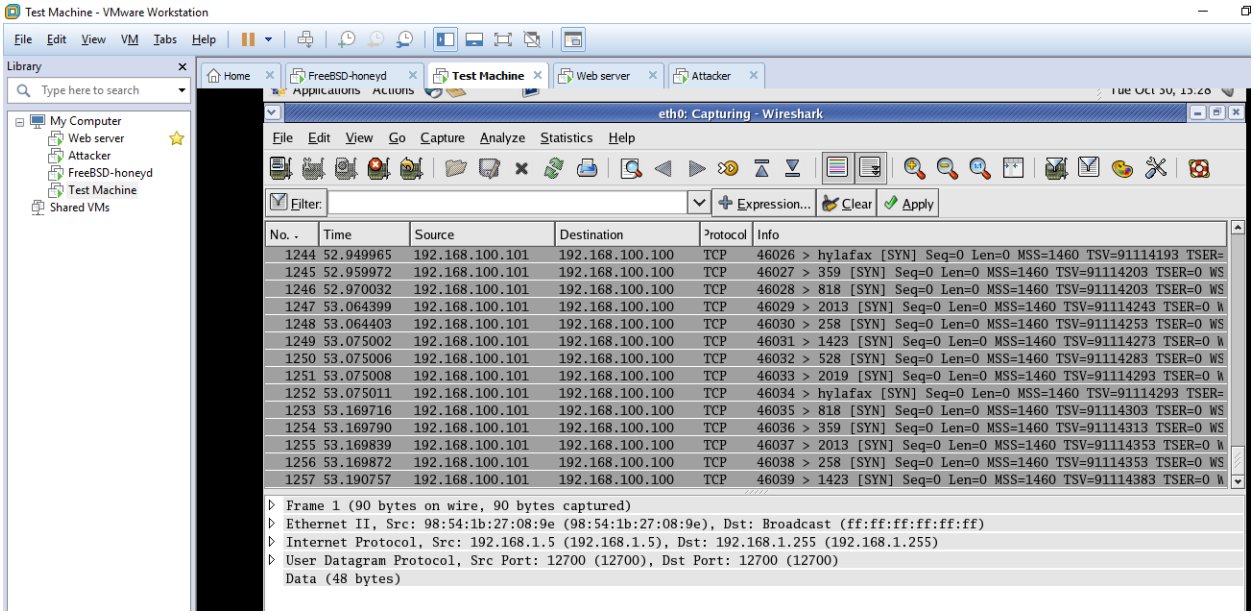


\

Scanning for network vulnerabilities.



Running wire shark on promiscuous mode.



Running Honeyd.

Nmaping alias.

```
root@localhost:~
File  Edit  View  Terminal  Tabs  Help
          RX bytes:498 (498.0 b)  TX bytes:336 (336.0 b)
          Interrupt:185 Base address:0x1424

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1549562 (1.4 MiB)  TX bytes:1549562 (1.4 MiB)

[root@localhost ~]# nmap -sT 192.168.100.103

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2018-10-30 20:45 EST
Interesting ports on 192.168.100.103:
(The 1670 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
180/tcp open  ris
MAC Address: 00:0C:29:E1:54:18 (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 17.998 seconds
[root@localhost ~]#
```

```
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34455 - 192.168.
100.103:1662)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34456 - 192.168.
100.103:2065)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34457 - 192.168.
100.103:1661)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34458 - 192.168.
100.103:894)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34459 - 192.168.
100.103:313)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34460 - 192.168.
100.103:140)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34461 - 192.168.
100.103:398)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34462 - 192.168.
100.103:585)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34463 - 192.168.
100.103:597)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34464 - 192.168.
100.103:1537)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34465 - 192.168.
100.103:1431)
honeyd[967]: Killing attempted connection: tcp (192.168.100.101:34466 - 192.168.
100.103:261)
```

References

1. Nmap, Introduction, https://nmap.org/.