

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:

1. 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 1](#_Toc528703559)

[Scenario Discussion 1](#_Toc528703560)

[Possible threats to Linux server and their solutions 1](#_Toc528703561)

[Possible threats to Apache web server and their solutions 2](#_Toc528703562)

[Possible threats to Network and their solutions 3](#_Toc528703563)

[Network drawing 4](#_Toc528703564)

[Design Discussion 4](#_Toc528703565)

[Apache web server v2.0 5](#_Toc528703566)

[MoD Security 5](#_Toc528703567)

[Port sentry 5](#_Toc528703568)

[Nessus 5](#_Toc528703569)

[Wireshark 5](#_Toc528703570)

[Firestarter 5](#_Toc528703571)

[NMAP (Network Mapper) 5](#_Toc528703572)

[HoneyD 5](#_Toc528703573)

[Device configuration summary 6](#_Toc528703574)

[Apache web server V2.0 6](#_Toc528703575)

[Mod security 6](#_Toc528703576)

[Portsentry 7](#_Toc528703577)

[Firestarter 8](#_Toc528703578)

[Nmap 8](#_Toc528703579)

[Nessus 8](#_Toc528703580)

[Honeyd 10](#_Toc528703581)

[Testing Plan 11](#_Toc528703582)

[Successful implementation of web server. 12](#_Toc528703583)

[After installing mod security. 12](#_Toc528703584)

[Trying scripting. 12](#_Toc528703585)

[Monitoring with modsecurity. 13](#_Toc528703586)

[Nmap Web server from attacker. 14](#_Toc528703587)

[OS detection of web server 15](#_Toc528703588)

[Portsentry dropping packet from attacker. 16](#_Toc528703589)

[Installation of Firestarter with policies. 17](#_Toc528703590)

[Firestarter showing events. 18](#_Toc528703591)

[Installing Nessus and Scanning network vulnerabilities for server. 19](#_Toc528703592)

[Scanning for network vulnerabilities. 20](#_Toc528703593)

[Running wire shark on promiscuous mode. 21](#_Toc528703594)

[Running Honeyd. 22](#_Toc528703595)

[References 23](#_Toc528703596)

# 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.

Mitigation

* 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:

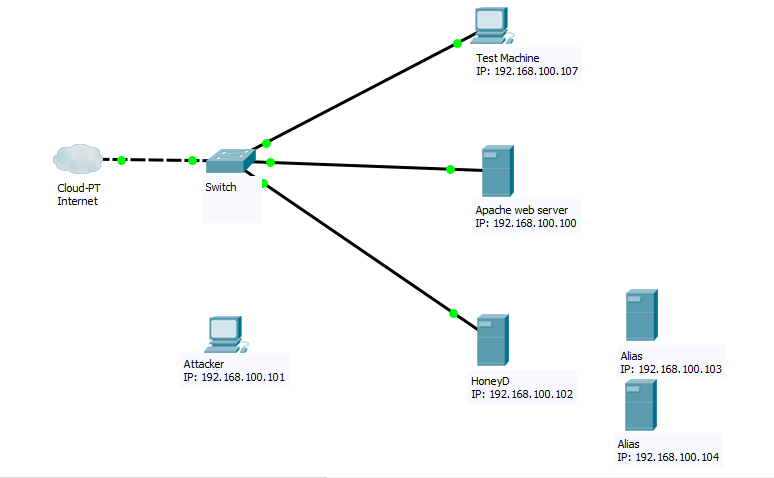
DNS can have IP address to domain name stored. Attacker can poison the DNS server and redirect the traffic to where the attacker designed to mislead the victims. This way customers can be redirect to attacker website and attacker can get personal and bank details of customers.

* 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

* Nessus
* Wireshark



Nmap

* Apache web server v2.0
* Port sentry
* MoD Security
* Firestarter

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.

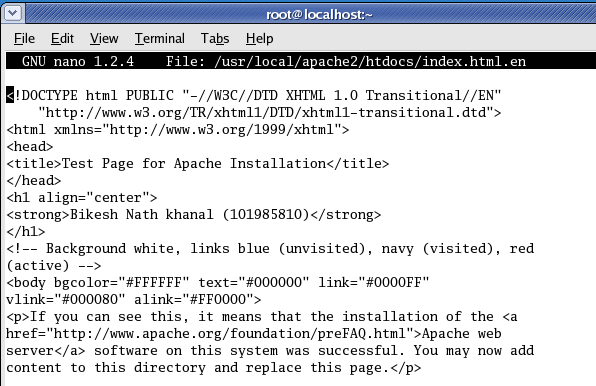
I have installed this server to mislead the attacker with unnecessary and irrelevant information.

# 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.

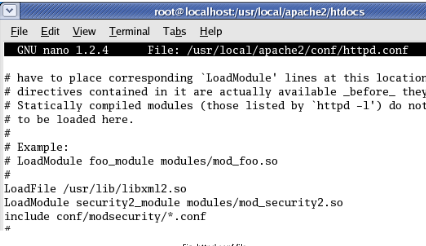
To run server: /usr/local/apache2/bin/apachectl start.



## 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.

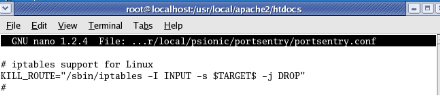


## Portsentry

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

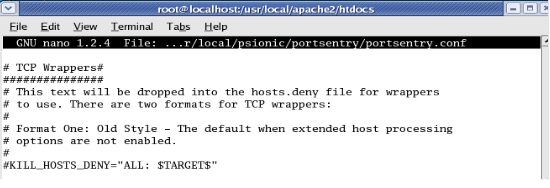
After this slight modification to file portsentry.conf located in /usr/local/psionic/portsentry in iptables section.





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



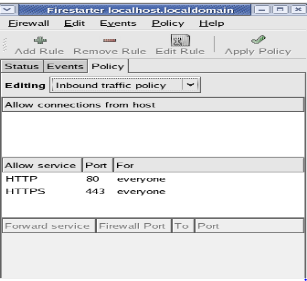


Now running Portsentry in stealth detection mode:



## Firestarter

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

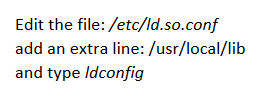


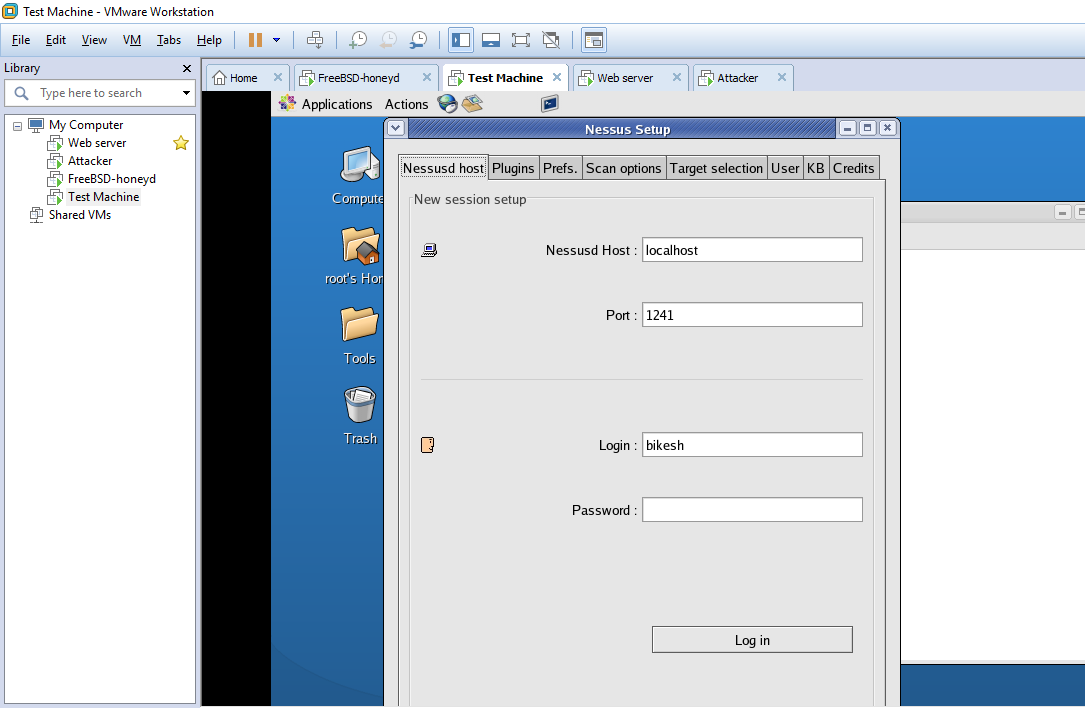
## Nmap

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

## Nessus

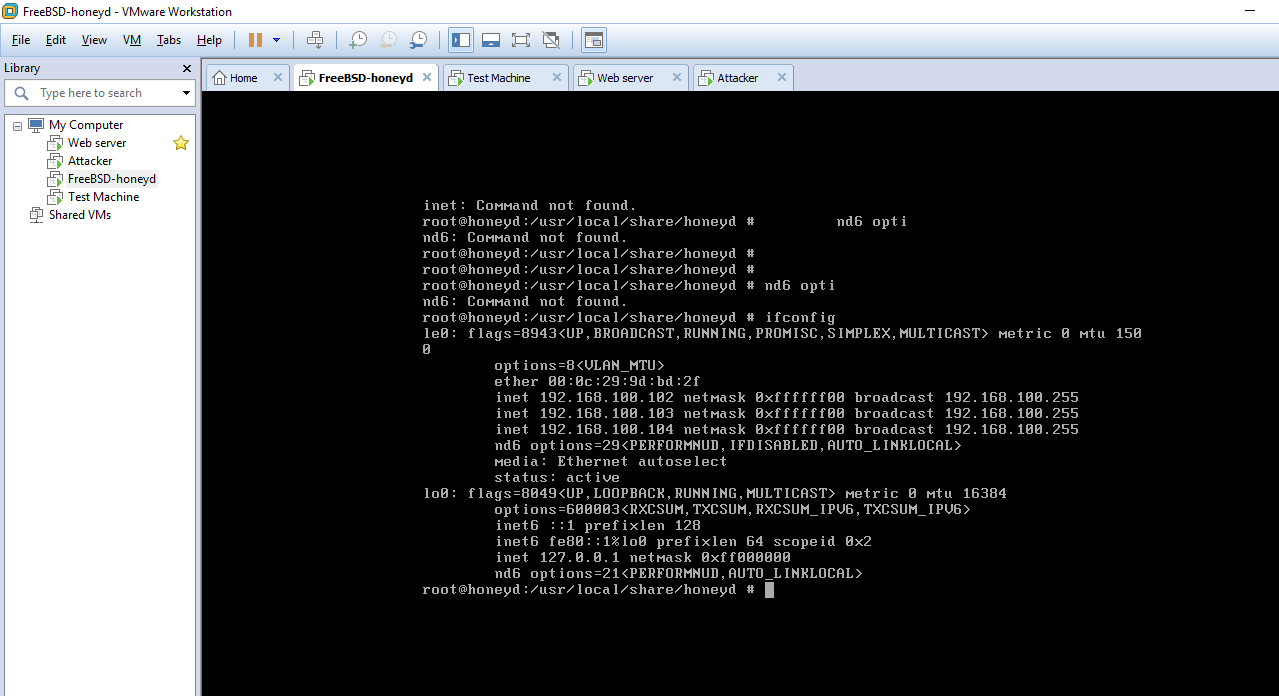
Nessus can be installed with help of four set of files nessus-libraries, libnasl, nessus-core and nessus-plugins. summary for installations are:

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. 
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.

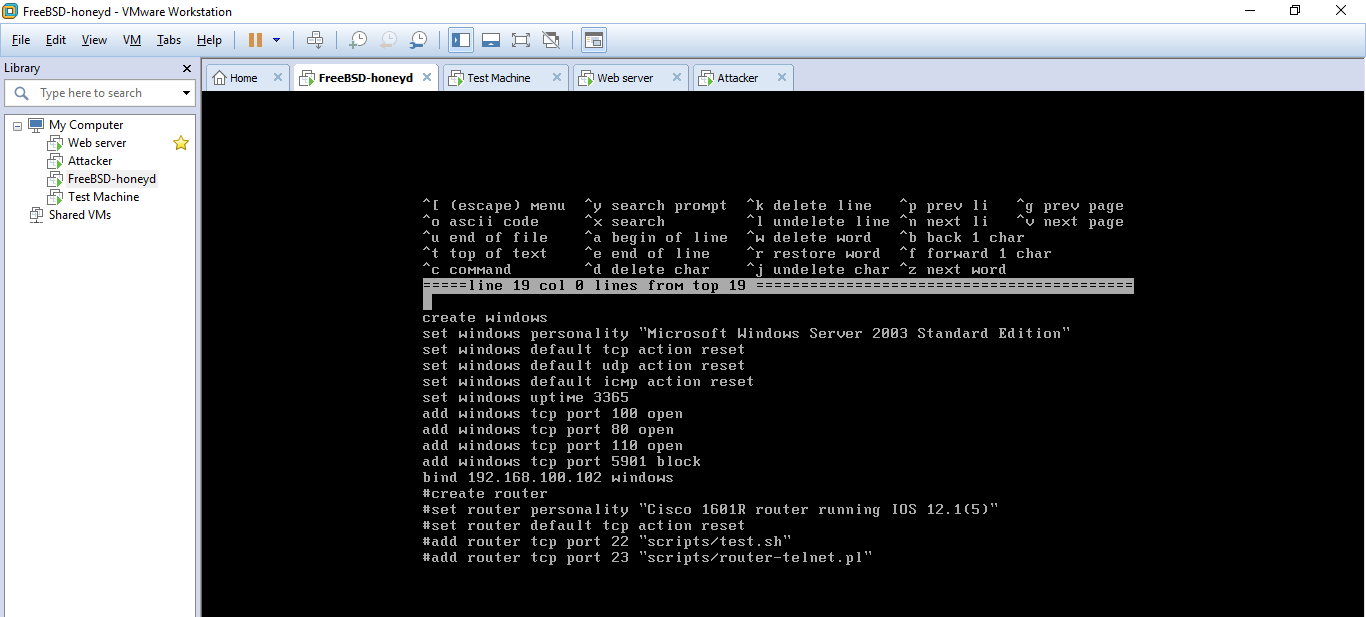


Wireshark and NMAP can be installed with same command as ./comfigure;make ;make install.

## 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.

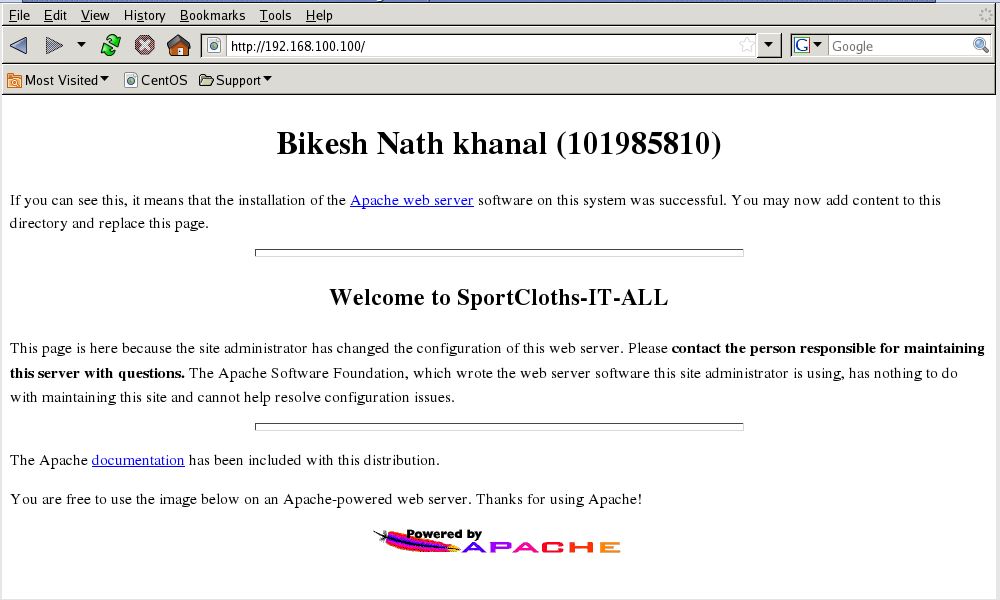


For running honeyd command honeyd -d -i le0 -f config.sample is used.

# Testing Plan

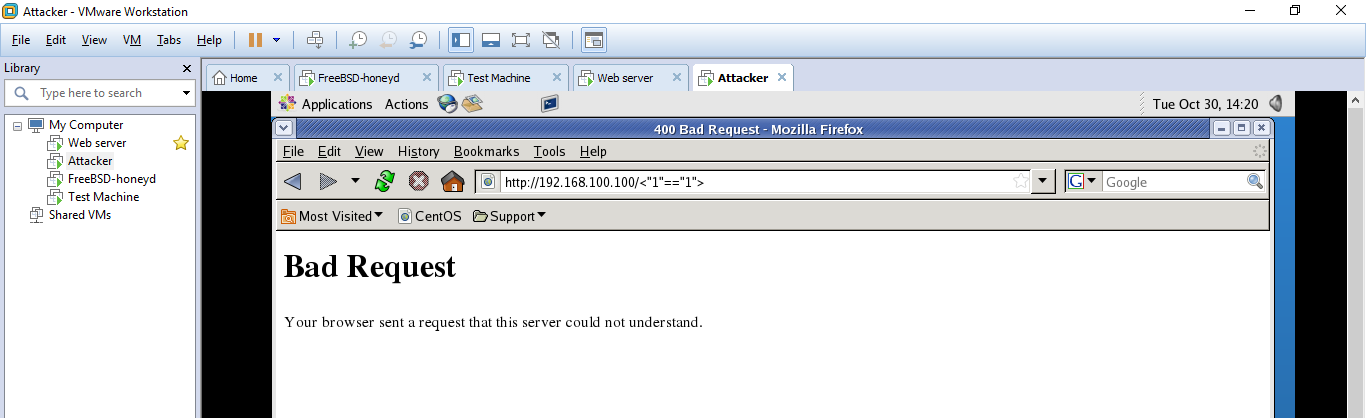
|  |  |  |  |
| --- | --- | --- | --- |
| Threats | Mitigation | Device configured | Commands |
| Fingerprinting | Portsentry, Honeyd | Web server Machine | honey -d -I le0 -f confing.sample to run  Honeyd  Portsentry in stealth scan detection  /usr/local/psionic/portsentry/portsentr  y -atcp  /usr/local/psionic/portsentry/portsentr  y –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/portsentr  y -atcp  /usr/local/psionic/portsentry/portsentr  y –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/portsentr  y -atcp  /usr/local/psionic/portsentry/portsentr  y –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.

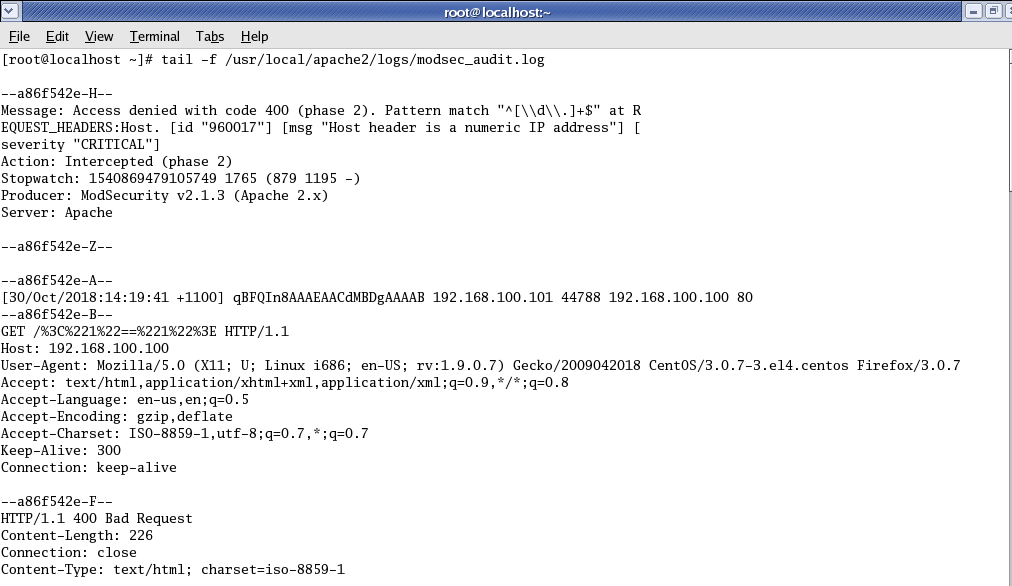


## After installing mod security.

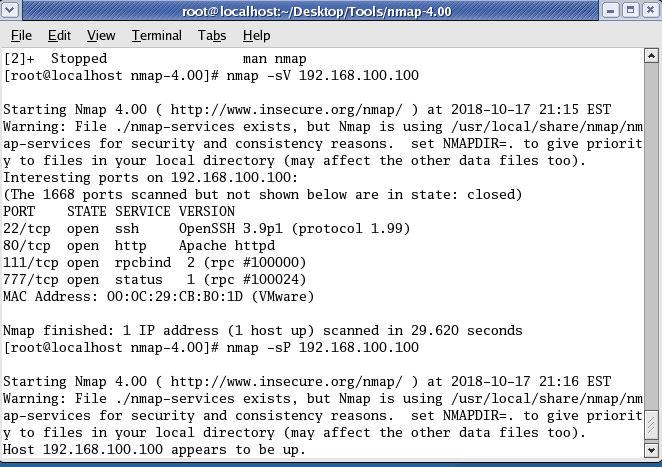
### Trying scripting.



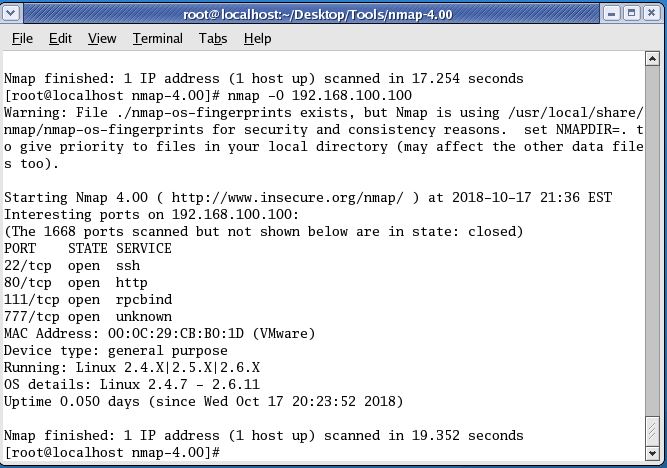
### Monitoring with modsecurity.



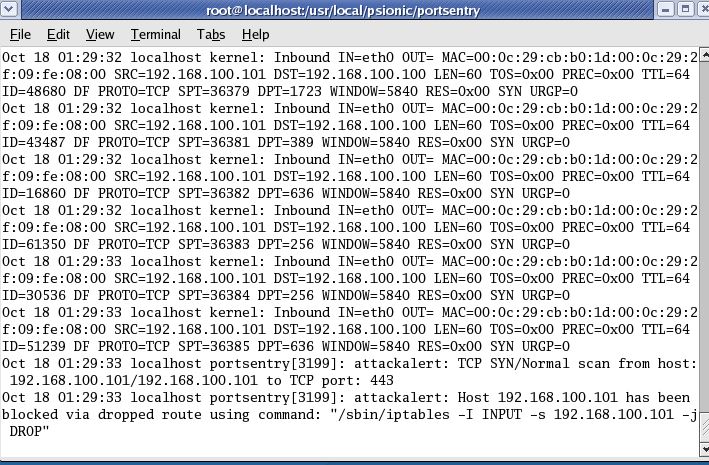
## Nmap Web server from attacker.



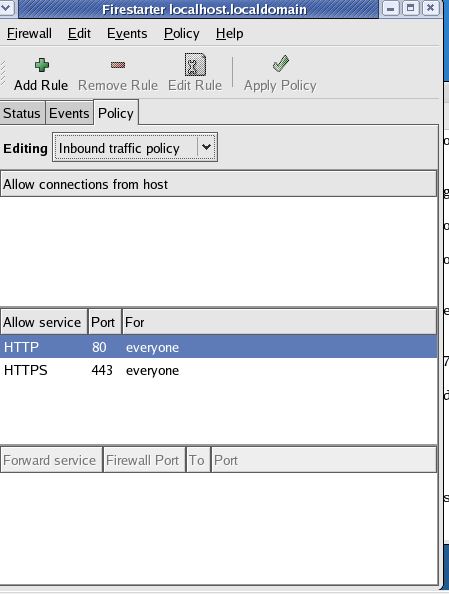
### OS detection of web server



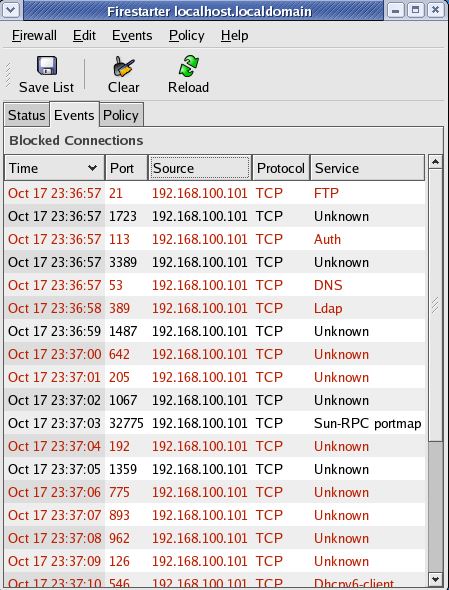
## Portsentry dropping packet from attacker.



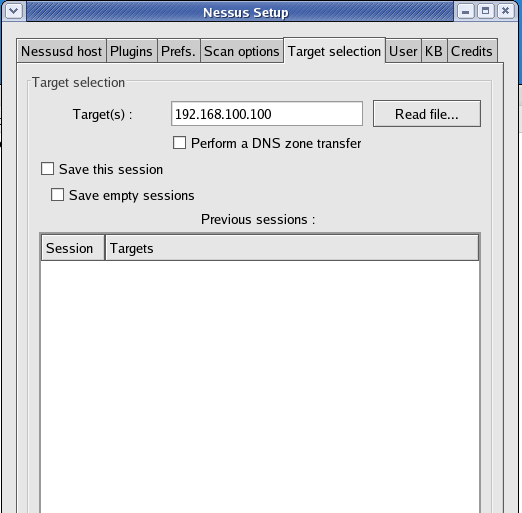
## Installation of Firestarter with policies.



### Firestarter showing events.

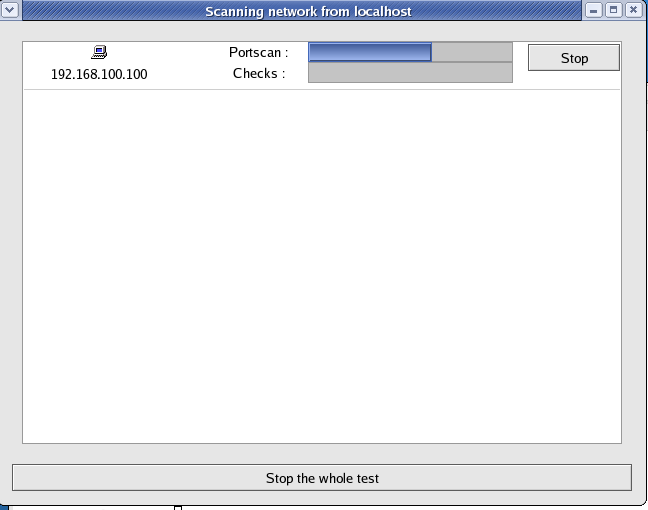


## Installing Nessus and Scanning network vulnerabilities for server.

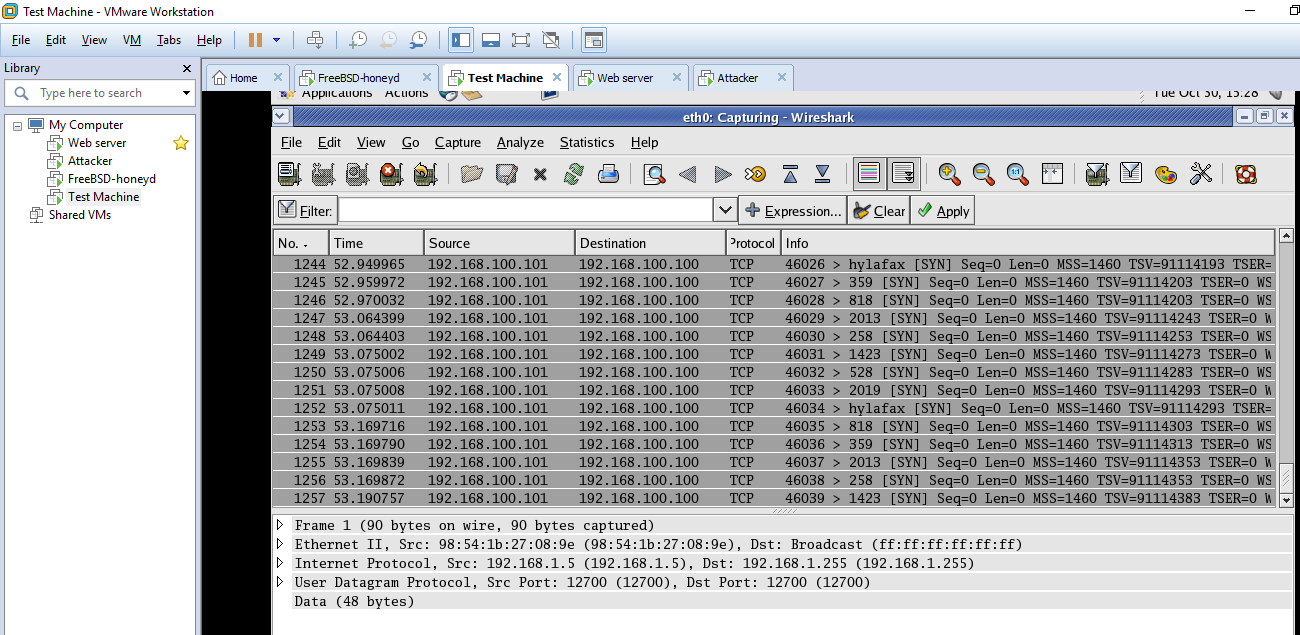


\

### Scanning for network vulnerabilities.

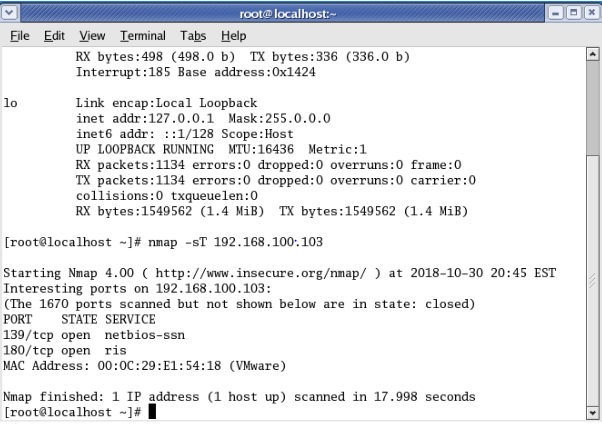


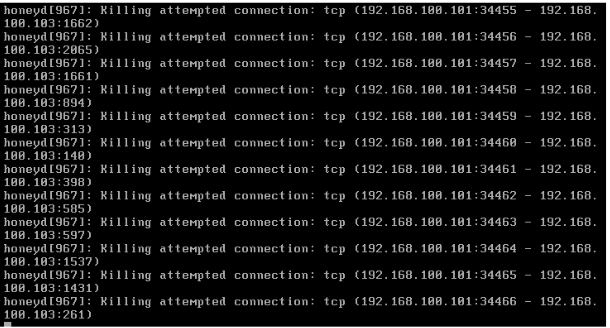
## Running wire shark on promiscuous mode.



## Running Honeyd.

Nmaping alias.





# References

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