Cover sheet for submission of work for assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

UNIT DETAILS

Unit name	Secure Network			Class day/time	
Unit code	TNE80006	Assignment no.		Due date	
Name of lecturer/teacher					
Tutor/marker's name					

Office use only

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/**

Lecture 1

Talking about history of telecommunication, in 1969 ARPNET 4 node network was connected and by year 1983 host were increased to 213. In 1983 ARPNET was replaced by TCP/IP.

IP network stack

OSI layer consists of 7 layers. And TCP/IP consists of 5 layers.

Physical layer

Physical medium such as wire are attached to this layer. Data encoding and decoding take place at this layer.

Data link layer

Frames are transferred to physical layer. Link establishment, transmission and error checking take place. Protocols in this layer is ethernet.

Network

3rd layer which consists of IP packets. Function of this layer are data encapsulated with source IP address and destination IP address for routing purposes, frame fragmentation etc. Ipv4 and IPv6 protocols.

Transport layer.

Protocols are TCP UDP

In this layer data is segmented. Function are delivering error free messages, Message acknowledgement etc.

Session layer

Functions are session establishment between process, termination and maintenance of session.

Presentation layer

Data conversion, formatting data, encryption are function s of this layer

Application layer

Serve window to users, file access remotely, email, directing services are some functions of this layer.

Answers

1. When domain name http://www.swin.edu.au/ is entered in browser it checks different cache including browser and OS cache for corresponding IP. If not found, it checks router cache. If not found it searches for ISP cache which maintain records to find IP address. In this cache DNS server is in the campus so it holds the ip address of the web server. Once

IP address of the server is retrieved it starts TCP connection through port 80. Once session is established the webserver send webpage which is displayed on browser.

2. Data is vulnerable to attack at each layer in OSI model as data is encapsulated or decapsulated at sending or receiving end. Detailed study of these layers is needed to implement network security. So OSI model is important to implement network security.
3. TCP operates at layer 4 transport layer of OSI model.

Lab1

1. Setting IP address on Linux centOS machine using command system-config-network.
2. Checking IPs implemented using ifconfig.
3. Pinging nearby PC with command ping <IP>.
4. Changing directory using command CD in terminal.
5. Ls to list all files in locating directory.
6. Make directory using mkdir <name> command.
7. Copying and moving the files between directories using Command cp <source path> <destination path> and mv cp <source path> <destination path>.

Lecture 2

Layer 1 defense

As our network is in danger of attack from outsiders i.e. outside of the network. The network is in danger within the perimeter too. So, to protect the data servers, router rack etc. Only the authorized individual should be granted entry or use of RFID i.e. radio frequency identification, locks such as pin tumbler, tubular locks, keys etc.

On using active element ball bearing on keys, copying of keys can be prevented.

RFIDs can also be cloneable using promark3 devices so cards like HID class E and HID smart ID mifire/defire) can be used which is yet to hijack.

If hacker success or layer 1 compromise than hackers will go for

I) Console authentication
II) Drop/switch USB drives
III) Plug/ boot from usb / lock the bios
IV) Can clone hard drives (have disk encryption)

Answers:

1. Ip spoofing is sending the packets by an attacker which consist of Source address of another host/victim at its IP header.
2. If the packets are examined, it contains IP address of the attacker at its IP header, so attacker spoof the source address to hide the identity.
3. Port mirroring is the method of monitoring network traffic. With enabling mirroring, it sends the network traffic from on switchport to another port to be analyzed [1].

4. BCP38 prevents incoming spoofed packets with Ingress filtering which is filtering method where spoofed packets are drop and logged [2], so John Smith attack is unsuccessful.

Lab 2

1. Changing IP address using command system-config-network.
2. Create lab1.txt file and copy using cp <source path> <destination path>.
3. Verify permissions of lab1.txt using command ls -l lab1.txt. Remove all user permission by chmod a-rw lab1.txt. Assign read permission as chmod a+rw lab1.txt.
4. To find word in file use grep -i name lab1.txt. for count of word command as grep -ic name lab1.txt

Answers:

1. Unix is a computer OS which was developed by the AT&T group in 1969 while Unix-like OS is that behaves in a similar manner to Unix OS without complying with the rules of Unix specifications.
2. Linux was created by young Linus Torvalds on 1991 to use his computer hardware better and with fewer restrictions [3].
3. Distros is OS made from collection of software's based on Linux kernel and Package management system. Some families are OpenSUSE, fedora, Red Hat, Ubuntu.
4. Nowadays every Linux come with guis but formerly only Shell was the user interface available on Linux. Shell is program that takes command from keyboards and provide to OS to perform.

Lecture 3

Taking Layer 2 Ethernet layer in which switch consist of CAM table (Linking ports and MAC entries). Hackers can fill CAM table with MAC flooding. Proper port security implementation with limiting number of hosts per port can mitigate this.

IP address and corresponding MAC address are in ARP table. Prior this entry, arp request is broadcast and thus attacker can first attack to this, receive their packets, look, change and return to the host. This is ARP spoofing. Mitigation is implementation of static ARP entries which is hard to manage. Dynamic ARP inspection can be implemented.

Data received while monitoring or logging network traffic should properly examine and never be ignored.

For Wi-Fi network only use WPA and WPA2 encryption wireless security.

Creating Access points with same SSID as original network in intension of stealing other credentials after users try to login to that network are Rouge AP attacks. Placing wireless sniffer can help in detection of rouge APS.

Lab 3

1. To extract .tar.gz file, tar xzvf x.tar.gz command can be used.
2. To install wireshark, inside Tools directory tar xzvf wireshark-0.99.5.tar.gz is used to extract. Using cd wireshark-0.99.5 to move inside wireshark-0.99.5 directory. Now use ./configure;make install;make to install.
3. To capture packets, connect to eth0 and click promiscuous mode (to monitor whole network) and click to start capture tab to start capturing packets.
4. Filter tab can be used to capture specific packets only.

Answers:

1. Sofwares as source code are written in form of codes which is transformed to machine readable by compiler whereas binary is precompiled ready to install.
2. .tar.gz is standard extension for zipped source code I.e. tar file.
3. To extract .tar.gz file, tar xzvf x.tar.gz command can be used.
4. Eth0 is ethernet interface and Lo0 is loopback interface to ping its own network.

Lecture 4

Routers forward the packets as routing tables determine where to forward the packets.

Ip source address spoofing: Root user can generate any packets. 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.

Fragmentation: Packets are fragmented to transfer to the destination with. As the fragmented packet reach the destination, these fragmented packets are kept on hold for all fragmented packets to arrive on memory. An attack can be done to exploit such as Tinny fragment attack and Fragment overlap attack. Best practice to drop every fragmented packet at firewall.

Path MTU discovery: It is the mechanism to avoid the fragmentation as it tests the path to send larger packets. Ip header has DF (do not fragment) set if any router in path cannot accommodate the packets size.

Nmap: is used to scan the layer 3 and 4 on the network. It is used to generate some reports about TCP/UDP ports which is vulnerable. Sends series of packets/cmd to guess the OS of the system which is called Fingerprinting.

ACLs (Access control lists) can be implemented to permit, deny any packets.

Answers:

1. Layer 2 have different MTU (Maximum transmission unit), which is largest packet size that can be transferred through the link. So the larger packets are fragmented and transferred though the same link with different MF flag in IP header.
2. If MF flag is set it means more fragments yet to follow in destination. At destination the fragments are stored in memory until all the fragments arrives and reassembles them.
3. When these packets are at memory attack can be mounted to exploit them this leads to Tiny fragmentation attack which is implementing packets with size small enough to induce them into the header fields of a second datagram so that it doesn't match the filter rules and passes through the filter. As the filtering implementation doesn't include minimum fragment size, spoofed packets might be forwarded. Best practice to avoid these attacks is to drop packets at the firewall.
4. Path MTU discovery is the mechanism to avoid the fragmentation as it tests the path to send larger packets. IP header has DF (do not fragment) set if any router in path cannot accommodate the packets size.

Lecture 5

Ports: Endpoint of Communication where services/Process can be implemented.

Services: network application such as HTTP, HTTPS, DNS etc.

Protocols: Rule of communication such as TCP and UDP.

TCP is connection oriented and 3way handshake. Attacking host with many tcp data and confusing host is session hijacking.

Firewall are built in OS. They are:

Static: Allow or deny traffic silently or ICMP "Destination Unreachable". Separate rules for incoming and outgoing traffic.

Dynamic: Outbound packet to server return packet automatically. But incoming Packet without corresponding outgoing packet is dropped.

Deep packet inspection: inspect payload and understands application protocols.

DNS: Contains IP corresponding domain name.

DNS queries are of two types:

1. Recursive: Server responds with answer or error
2. Iterative: Server responds with answer or it refers to another server

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.

Answers:

1. Nmap send many TCP packets to host based on the reply it predicts the OS of the system. It compares these responses to nmap-os-db database and sends the details of that OS.
2. Nmap can only predict OS if it is on nmap-os-db database.

Lab 5

1. To install Apache, inside Tools /tools directory tar xzvf httpd_2.0.52.tar.gz is used to extract. Using cd httpd_2.0.52 to move inside httpd_2.0.52 directory. Now use ./configure;make install;make to install.
2. To change the index.html.en file on htdocs command used is nano /usr/local/apache2/htdocs/index.html.en.
3. To run server: /usr/local/apache2/bin/apachectl start.check entering the IP on browser. Proper webpage displaying Apache installed.
4. tail -f /usr/local/apache2/logs/access_log is a command to observe logs 'live'.
5. Install nmap with command tar xjvf nmap.tar.bz2 in /tools.
6. Command nmap -O <ip> can be used to find running OS in the machine.

Answers

1. Access log contains list of successful requests of file in the server whereas Error logs are information about error trying accessing those files.

Lecture 6

There are two main security issues in application layer. They are:

- 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.
- 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.

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.

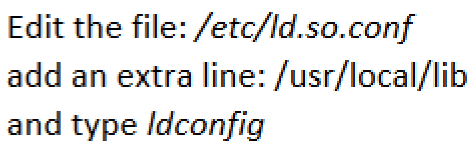
It is mainly used to give security to apache server from attacks such as XSS and SQL injections.

Answers:

1. WAF can filter contents of specific web applications while deep packet inspection firewall can serve as safety gate between servers.
2. Both can understand application protocols and inspect incoming traffic.
3. IDS monitor malicious activities and firewall do inspect incoming packets but is not able to prevent attacks such as SQL injection and XSS so I will apply WAF to protect the server.

Lab 6

1. Installing Firestarter from /tools.
2. Go to policy tab and make policies to allow HTTP service from port 80 and HTTPS from port 443 for everyone.
3. Click apply policies and nmap your centOS machine with nmap -sT <ip>.
4. Observe live events in events tab.
5. Nessus can be installed with help of four set of files nessus-libraries, libnasl, nessus-core and nessus-plugins. summary for installations are:
6. 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*

7. Making certificate: /usr/local/sbin/nessus-mkcert.
8. Adding user: /usr/local/sbin/nessus-adduser.
9. Start nessus server with nessusd command.
10. Start nessus gui with nessus command in another terminal.
11. Ps -f | grep nessusd to check if nessus server is running or not.

Answers:

1. Net filter is inbuilt Linux software which Performs translation of network address and Filters traffic whereas Iptables are rules set to configure IPv4 and V6 frameworks.

Lecture 7

Rouge DHCP server offers address with wrong gateways.

Mitigation: DHCP snooping binding table is build by snooping DHCP reply.

Unauthorized client: Any client is given ip from DHCP server. To mitigate it layer 2 authentications i.e.801. x can be implemented.

Malicious Client: A client in a network who takes all IP address and randomizes MAC address. Fill all CAM table with cmd.

To mitigate proper port security should be implemented.

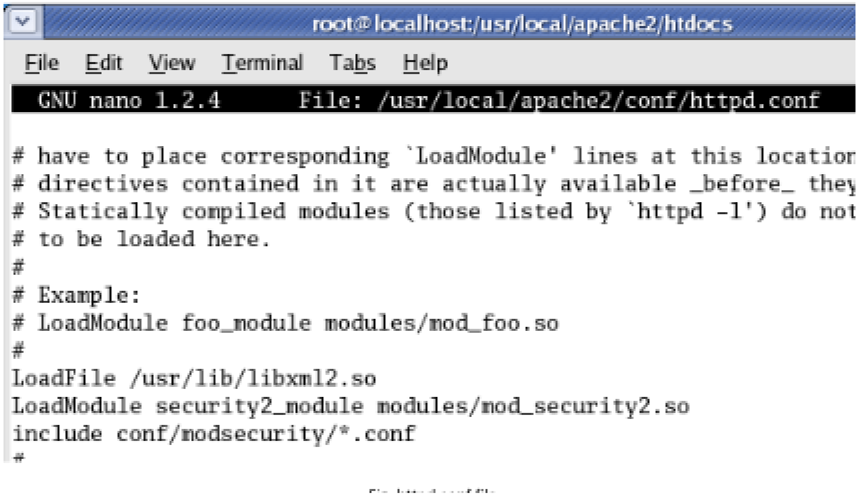
Answers:

1. Forward proxy masks internal resources and outbound filtering. Reverse proxy terminates client connections to the server and created gap to inspect incoming traffic.
2. As proxy cache contains all the requests made from clients on network. And retrieving attachments is easy as they are cached.

Lab 7

1. 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.



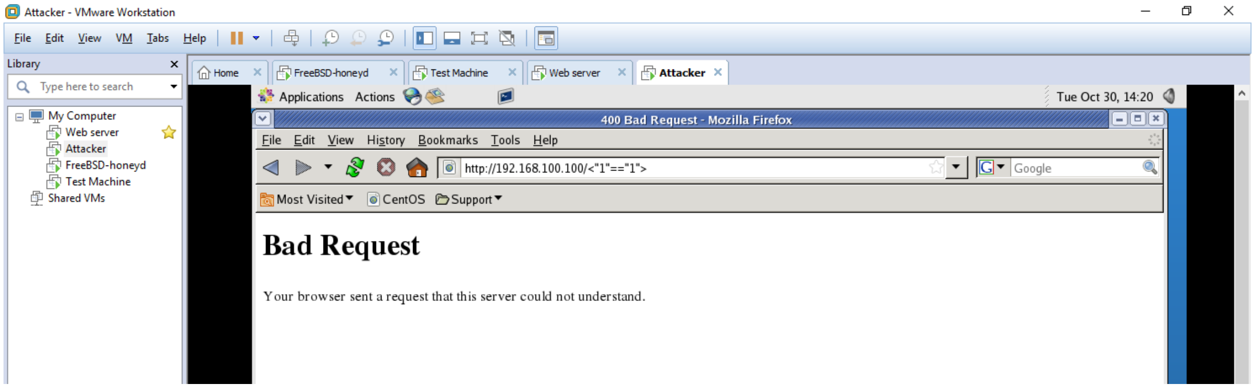
root@localhost:/usr/local/apache2/htdocs
File Edit View Terminal Tabs Help

```
  GNU nano 1.2.4        File: /usr/local/apache2/conf/httpd.conf

# have to place corresponding `LoadModule' lines at this locatior
# 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
#
```

Fig. httpd.conf file

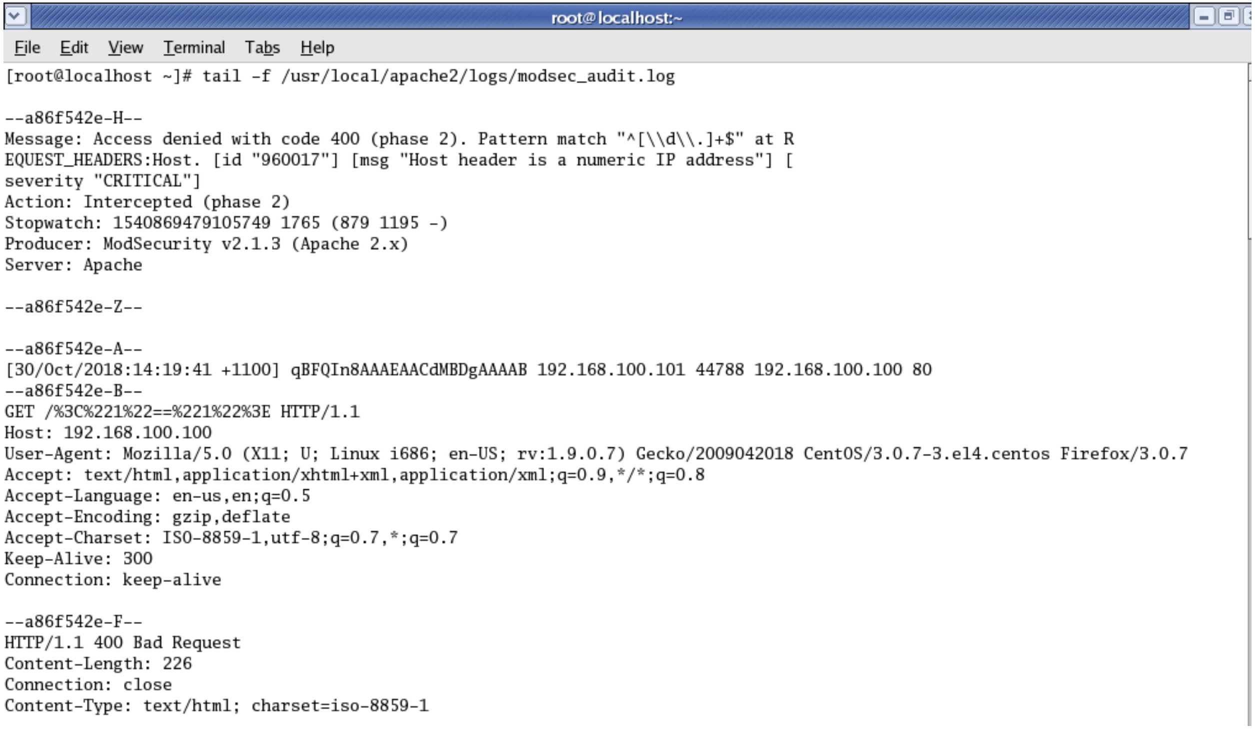
Trying scripting entering <”1”==”1”> at end of Ipsddress as xx.xx.xx.xx/<”1”==”1”>



Bad Request

Your browser sent a request that this server could not understand.

Monitoring with modsecurity.in tail -f /usr/local/apache2/logs/modsec_audit.log.



```
[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
```

Lecture 8

- 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.

  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.

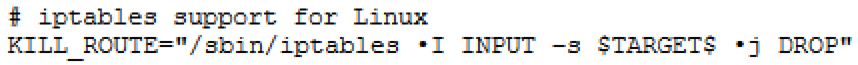
Answers

1. Two main problem of buffer overflow where data overwrites adjacent memory are :
   a) Service to crash
   b) Remote execution of code with root privileges.

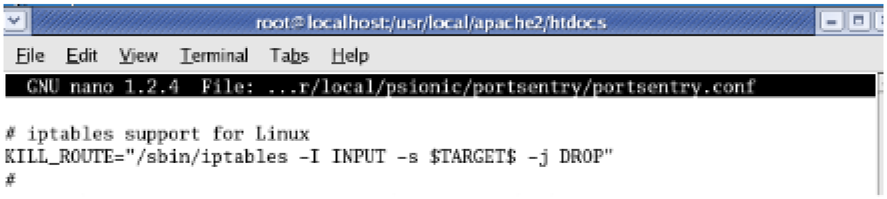
Lab 8

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.



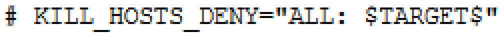
```
# iptables support for Linux
KILL_ROUTE="/sbin/iptables •I INPUT –s $TARGET$ •j DROP"
```



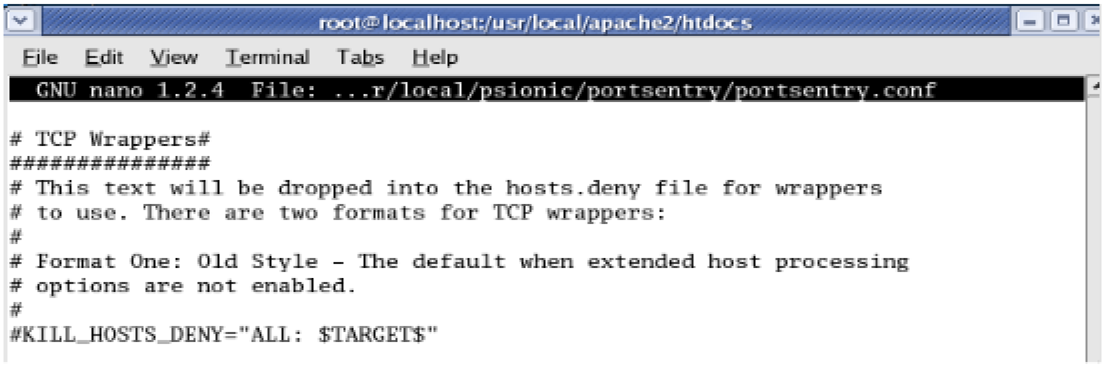
```
  GNU nano 1.2.4   File: ...r/local/psionic/portsentry/portsentry.conf

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

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



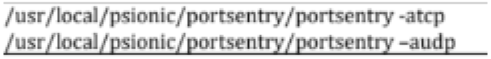
```
# KILL_HOSTS_DENY="ALL: $TARGET$"
```



```
 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
```

Lecture 9

IDS (Intrusion Detection system): Takes data and distinguished between good and bad using various methods. It is of four broad types: signature (any layer), Anomaly (any layer), darknet (layer 3 & 4) and honeypot (layer 7).

Encryption: Use keys to encode/decode a message.

Two types: Symmetric: Need a same key to encrypt/decrypt the message

Asymmetric: 2 keys Private keys used to decrypt the message and public key to encrypt the message.

VPN: used to communicate two networks, common encryption is made in a public

network.

Defense in depth: Implement security at each layer and analyzing impact of each layer attack.

Lecture 10

This lecture describes User Accounts, Authentication and password cracking.

• User Accounts: must have naming conventions, passwords policies, accounts expiry, limiting

Password attempts.

• Multi factor authentication: Identifying users via username and password. And additionally, with knowledge, possession like RFID and Inherence like retina scan, fingerprint scan, Face ID etc

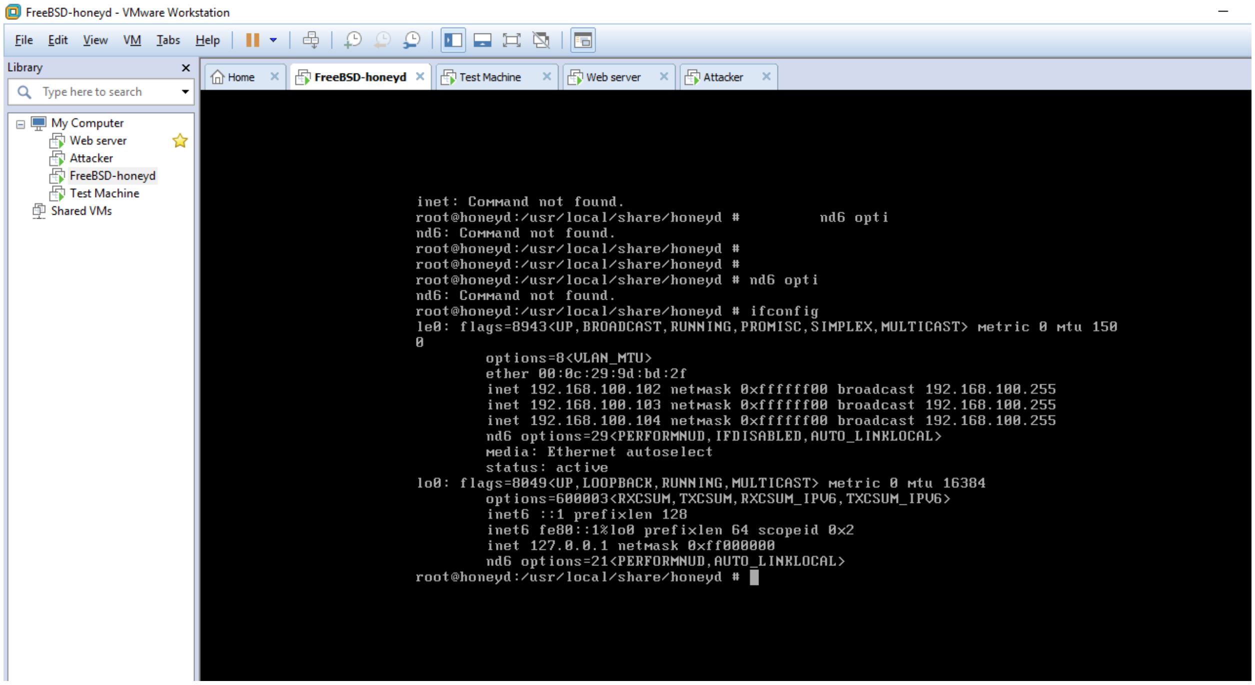
• Password Cracking: John the Ripper tries all the possible combinations of passwords and usernames and cracks the passwords. GPUs are deployed to fasten the cracking of passwords.

Lab 10

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.

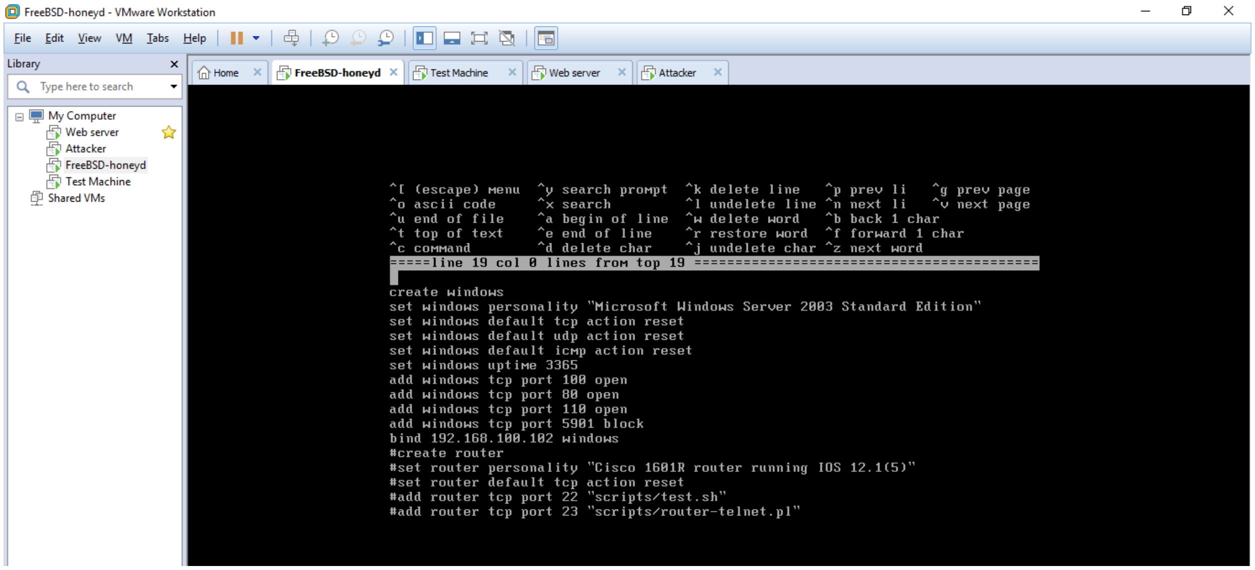
To config IP address to FreeBSD ifconfig le0 inet <ip>/24

To crate alias ifconfig le0 inet <ip>/24 alias.



```
inet: Command not found.
root@honeyd:/usr/local/share/honeyd #         nd6 opti
nd6: Command not found.
root@honeyd:/usr/local/share/honeyd #
root@honeyd:/usr/local/share/honeyd #
root@honeyd:/usr/local/share/honeyd # nd6 opti
nd6: Command not found.
root@honeyd:/usr/local/share/honeyd # ifconfig
le0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 150
0
        options=8<VLAN_MTU>
        ether 00:0c:29:9d:bd:2f
        inet 192.168.100.102 netmask 0xffffff00 broadcast 192.168.100.255
        inet 192.168.100.103 netmask 0xffffff00 broadcast 192.168.100.255
        inet 192.168.100.104 netmask 0xffffff00 broadcast 192.168.100.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
root@honeyd:/usr/local/share/honeyd #
```

Config.sample has been configured with following template. To open this file ee /usr/locsl/share/honeyd.



```
^[ (escape) menu  ^y search prompt  ^k delete line   ^p prev li    ^g prev page
^o ascii code     ^x search         ^l undelete line ^n next li    ^v next page
^u end of file    ^a begin of line  ^w delete word   ^b back 1 char
^t top of text    ^e end of line    ^r restore word  ^f forward 1 char
^c command        ^d delete char    ^j undelete char ^z next word
=====line 19 col 0 lines from top 19 ==========================================

create windows
set windows personality "Microsoft Windows Server 2003 Standard Edition"
set windows default tcp action reset
set windows default udp action reset
set windows default icmp action reset
set windows uptime 3365
add windows tcp port 100 open
add windows tcp port 80 open
add windows tcp port 110 open
add windows tcp port 5901 block
bind 192.168.100.102 windows
#create router
#set router personality "Cisco 1601R router running IOS 12.1(5)"
#set router default tcp action reset
#add router tcp port 22 "scripts/test.sh"
#add router tcp port 23 "scripts/router-telnet.pl"
```

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

Lecture 11

- IANA: Manages the IP assignment worldwide.
- Interior gateway protocol is implemented using protocols such as EIGRP, RIP, OSPF.
- Exterior gateway protocols are inter-AS.
- BGP is a Path-vector routing protocol that uses TCP where EIGRP and OSPF uses IP.
- BGP verifies the identity of the destination and authenticates to communicate preventing hijacking the communication BGP provides unaltered conversations.

Lecture 12

Summary of all lectures and exam paper discussion.

References:

1. MiaRec, What is port mirroring?, 2017, https://www.miarec.com/faq/what-is-port-mirroring
2. DNS made easy, Implementing BCP 38 To Reduce Spoofed-Packet DDoS Attacks, April,2017, http://social.dnsmadeeasy.com/blog/implementing-bcp-38-to-reduce-spoofed-packet-ddos-attacks/
3. FOSSMint, When and why was Linux created, Martins D.okoi , https://www.fossmint.com/when-and-why-was-linux-created/