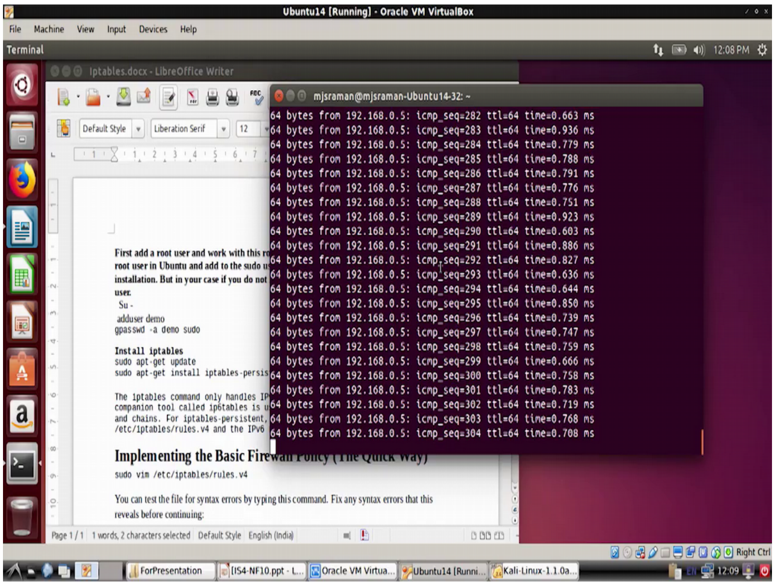
Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 55
Logs, Rules and Automated Tools

Welcome to this session on network security and forensics. We will now show a small demo configuration of firewall ah. So, what we have done is; so, we have a actually got a set up of two machines running on a oracle virtual v m.

(Refer Slide Time: 00:28)



First add a root user and work with this ro
root user in Ubuntu and add to the sudo u
installation. But in your case if you do not
user.

```
 Su -
 adduser demo
gpasswd -a demo sudo
```

Install iptables

```
sudo apt-get update
sudo apt-get install iptables-persis
```

```
The iptables command only handles IP
companion tool called ip6tables is u
and chains. For iptables-persistent,
/etc/iptables/rules.v4 and the IPv6
```

Implementing the Basic Firewall Policy (The Quick Way)

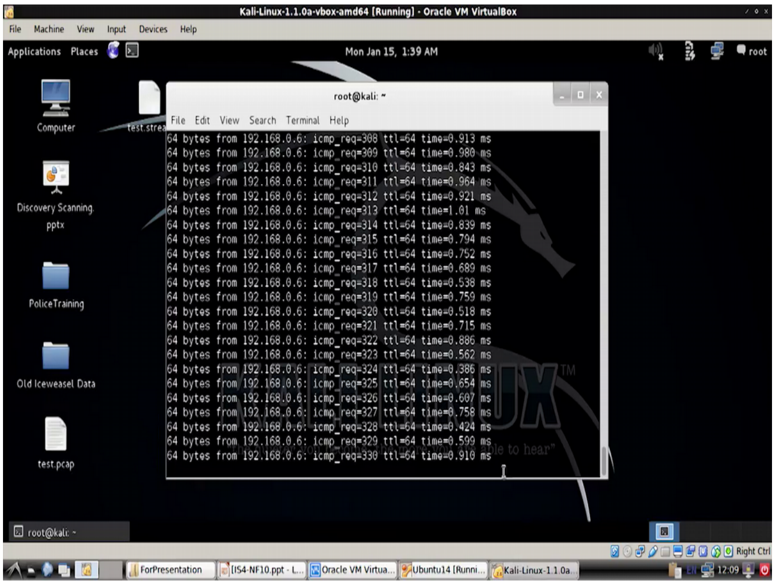
```
sudo vim /etc/iptables/rules.v4
```

You can test the file for syntax errors by typing this command. Fix any syntax errors that this reveals before continuing:

```
64 bytes from 192.168.0.5: icmp_seq=282 ttl=64 time=0.663 ms
64 bytes from 192.168.0.5: icmp_seq=283 ttl=64 time=0.936 ms
64 bytes from 192.168.0.5: icmp_seq=284 ttl=64 time=0.779 ms
64 bytes from 192.168.0.5: icmp_seq=285 ttl=64 time=0.788 ms
64 bytes from 192.168.0.5: icmp_seq=286 ttl=64 time=0.791 ms
64 bytes from 192.168.0.5: icmp_seq=287 ttl=64 time=0.776 ms
64 bytes from 192.168.0.5: icmp_seq=288 ttl=64 time=0.751 ms
64 bytes from 192.168.0.5: icmp_seq=289 ttl=64 time=0.923 ms
64 bytes from 192.168.0.5: icmp_seq=290 ttl=64 time=0.603 ms
64 bytes from 192.168.0.5: icmp_seq=291 ttl=64 time=0.886 ms
64 bytes from 192.168.0.5: icmp_seq=292 ttl=64 time=0.827 ms
64 bytes from 192.168.0.5: icmp_seq=293 ttl=64 time=0.636 ms
64 bytes from 192.168.0.5: icmp_seq=294 ttl=64 time=0.644 ms
64 bytes from 192.168.0.5: icmp_seq=295 ttl=64 time=0.850 ms
64 bytes from 192.168.0.5: icmp_seq=296 ttl=64 time=0.739 ms
64 bytes from 192.168.0.5: icmp_seq=297 ttl=64 time=0.747 ms
64 bytes from 192.168.0.5: icmp_seq=298 ttl=64 time=0.759 ms
64 bytes from 192.168.0.5: icmp_seq=299 ttl=64 time=0.666 ms
64 bytes from 192.168.0.5: icmp_seq=300 ttl=64 time=0.758 ms
64 bytes from 192.168.0.5: icmp_seq=301 ttl=64 time=0.783 ms
64 bytes from 192.168.0.5: icmp_seq=302 ttl=64 time=0.719 ms
64 bytes from 192.168.0.5: icmp_seq=303 ttl=64 time=0.768 ms
64 bytes from 192.168.0.5: icmp_seq=304 ttl=64 time=0.708 ms
```

So, we have got one Ubuntu 14 that is running and this is internally connected to a Kali Linux machine.

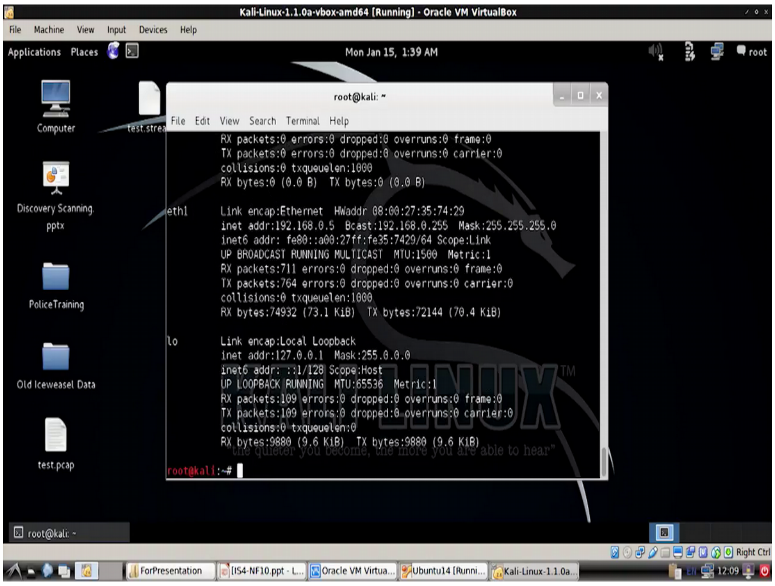
(Refer Slide Time: 00:42)



```
64 bytes from 192.168.0.6: icmp_req=308 ttl=64 time=0.913 ms
64 bytes from 192.168.0.6: icmp_req=309 ttl=64 time=0.980 ms
64 bytes from 192.168.0.6: icmp_req=310 ttl=64 time=0.843 ms
64 bytes from 192.168.0.6: icmp_req=311 ttl=64 time=0.964 ms
64 bytes from 192.168.0.6: icmp_req=312 ttl=64 time=0.921 ms
64 bytes from 192.168.0.6: icmp_req=313 ttl=64 time=1.01 ms
64 bytes from 192.168.0.6: icmp_req=314 ttl=64 time=0.839 ms
64 bytes from 192.168.0.6: icmp_req=315 ttl=64 time=0.794 ms
64 bytes from 192.168.0.6: icmp_req=316 ttl=64 time=0.752 ms
64 bytes from 192.168.0.6: icmp_req=317 ttl=64 time=0.689 ms
64 bytes from 192.168.0.6: icmp_req=318 ttl=64 time=0.538 ms
64 bytes from 192.168.0.6: icmp_req=319 ttl=64 time=0.759 ms
64 bytes from 192.168.0.6: icmp_req=320 ttl=64 time=0.518 ms
64 bytes from 192.168.0.6: icmp_req=321 ttl=64 time=0.715 ms
64 bytes from 192.168.0.6: icmp_req=322 ttl=64 time=0.886 ms
64 bytes from 192.168.0.6: icmp_req=323 ttl=64 time=0.562 ms
64 bytes from 192.168.0.6: icmp_req=324 ttl=64 time=0.386 ms
64 bytes from 192.168.0.6: icmp_req=325 ttl=64 time=0.654 ms
64 bytes from 192.168.0.6: icmp_req=326 ttl=64 time=0.607 ms
64 bytes from 192.168.0.6: icmp_req=327 ttl=64 time=0.758 ms
64 bytes from 192.168.0.6: icmp_req=328 ttl=64 time=0.424 ms
64 bytes from 192.168.0.6: icmp_req=329 ttl=64 time=0.599 ms
64 bytes from 192.168.0.6: icmp_req=330 ttl=64 time=0.910 ms
```

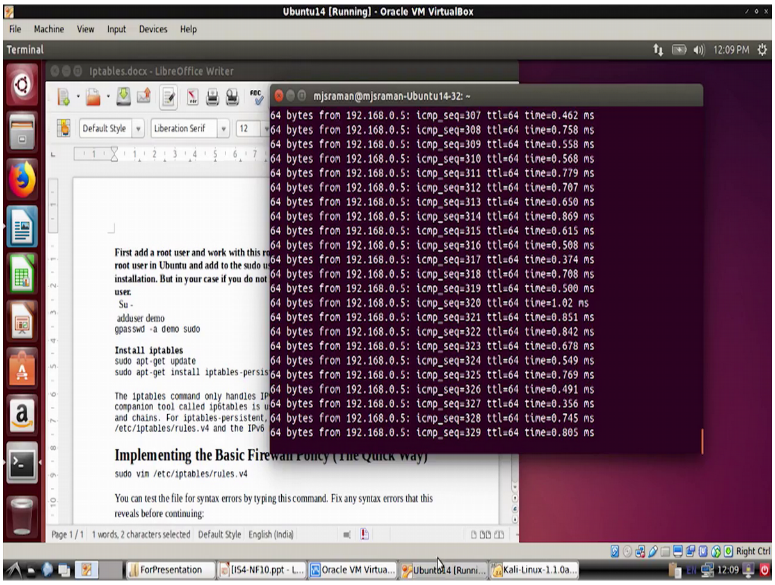
With the IP address for this Kali Linux machine is 192 dot 168 dot 0 dot 5 and the IP address for our Ubuntu machine is as you can see is 192 dot 168 dot 0 dot 6.

(Refer Slide Time: 00:49)



```
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth1      Link encap:Ethernet  HWaddr 08:00:27:35:74:29
          inet addr:192.168.0.5  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe35:7429/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:711 errors:0 dropped:0 overruns:0 frame:0
          TX packets:764 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:74932 (73.1 KiB)  TX bytes:72144 (70.4 KiB)

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:65536  Metric:1
          RX packets:109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9880 (9.6 KiB)  TX bytes:9880 (9.6 KiB)

root@kali:~#
```

(Refer Slide Time: 00:54)


Ubuntu14 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:09 PM
Iptables.docx - LibreOffice Writer
Default Style
Liberation Serif
12
mjsraman@mjsraman-Ubuntu14-32: ~
Page 1 / 1 1 words, 2 characters selected Default Style English (India)
Right Ctrl
ForPresentation
[IS4-NF10.ppt - L...
Oracle VM Virtua...
Ubuntu14 [Runni...
Kali-Linux-1.1.0a...
12:09

First add a root user and work with this ro
root user in Ubuntu and add to the sudo u
installation. But in your case if you do not
user.

```
 Su -
 adduser demo
gpasswd -a demo sudo
```

Install iptables

```
sudo apt-get update
sudo apt-get install iptables-persis
```

```
The iptables command only handles IP
companion tool called ip6tables is u
and chains. For iptables-persistent,
/etc/iptables/rules.v4 and the IPv6
```

Implementing the Basic Firewall Policy (The Quick Way)

```
sudo vim /etc/iptables/rules.v4
```

You can test the file for syntax errors by typing this command. Fix any syntax errors that this reveals before continuing:

```
64 bytes from 192.168.0.5: icmp_seq=307 ttl=64 time=0.462 ms
64 bytes from 192.168.0.5: icmp_seq=308 ttl=64 time=0.758 ms
64 bytes from 192.168.0.5: icmp_seq=309 ttl=64 time=0.558 ms
64 bytes from 192.168.0.5: icmp_seq=310 ttl=64 time=0.568 ms
64 bytes from 192.168.0.5: icmp_seq=311 ttl=64 time=0.779 ms
64 bytes from 192.168.0.5: icmp_seq=312 ttl=64 time=0.707 ms
64 bytes from 192.168.0.5: icmp_seq=313 ttl=64 time=0.650 ms
64 bytes from 192.168.0.5: icmp_seq=314 ttl=64 time=0.869 ms
64 bytes from 192.168.0.5: icmp_seq=315 ttl=64 time=0.615 ms
64 bytes from 192.168.0.5: icmp_seq=316 ttl=64 time=0.508 ms
64 bytes from 192.168.0.5: icmp_seq=317 ttl=64 time=0.374 ms
64 bytes from 192.168.0.5: icmp_seq=318 ttl=64 time=0.708 ms
64 bytes from 192.168.0.5: icmp_seq=319 ttl=64 time=0.500 ms
64 bytes from 192.168.0.5: icmp_seq=320 ttl=64 time=1.02 ms
64 bytes from 192.168.0.5: icmp_seq=321 ttl=64 time=0.851 ms
64 bytes from 192.168.0.5: icmp_seq=322 ttl=64 time=0.842 ms
64 bytes from 192.168.0.5: icmp_seq=323 ttl=64 time=0.678 ms
64 bytes from 192.168.0.5: icmp_seq=324 ttl=64 time=0.549 ms
64 bytes from 192.168.0.5: icmp_seq=325 ttl=64 time=0.769 ms
64 bytes from 192.168.0.5: icmp_seq=326 ttl=64 time=0.491 ms
64 bytes from 192.168.0.5: icmp_seq=327 ttl=64 time=0.356 ms
64 bytes from 192.168.0.5: icmp_seq=328 ttl=64 time=0.745 ms
64 bytes from 192.168.0.5: icmp_seq=329 ttl=64 time=0.805 ms
```

So, what we are able to do right now is I can do a ping to find out whether the Kali machine is in the network. So, I try 192 dot 168 dot 0 dot 5; so, I am able to ping this machine similarly I will also try to ping from the kali machine to this machine.

So, if you look at the this ping 192 dot 168 dot 0 dot 6. So, this now this shows that these two machines are connected to each other ok. Now what we will do is we will have to now find out or will explain how to install IP tables. Now we already done this install this IP tables in this machine, but then this is the step that we have to do the first thing we need to be very careful is if you are logged in as root into your Ubuntu machine, please do not go ahead and use the same login to install firewalls.

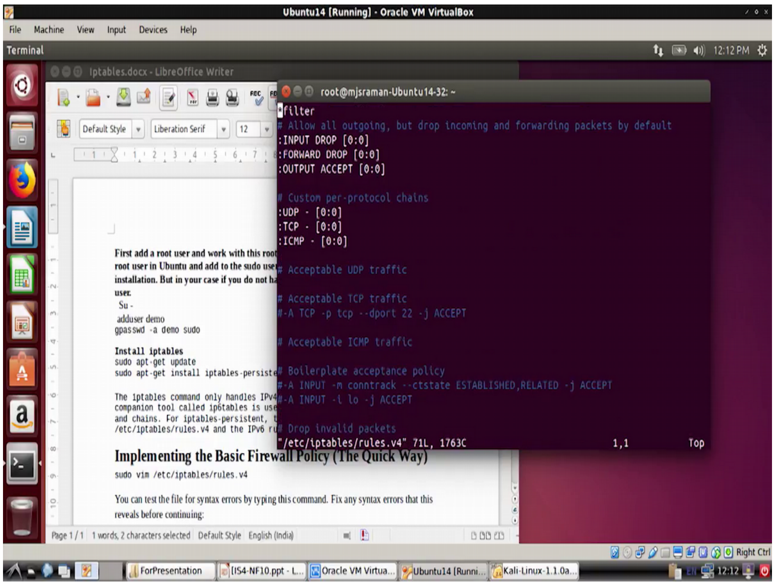
Because if you get blocked and there is a problem I mean you will not be able to recover unless you put otherwise recovering by it is a long process. So, do not go into that problem you have to create a root user with special root permission. So, this is the way to create the root user with permissions if it is a Ubuntu machine then you put a s u minus then you give the password what are the password you have given to the machines; so, you become a root user.

Then you can use this term something known as add users see and I have already added this user. So, you do not have to worry about it at least in the demo and then what you have to do is the next line says that this route user whatever user you have you have created must be added as a pseudo user I mean. So, that you gets all the permissions then you can actually install IP tables ok. So, you can use the commands pseudo apt get update then you can get install IP tables persistent ok.

So, once you do that ok; so, in my case I already installed it. So, it says otherwise its goes and it should be connected to the internet of course, ah. So, then it goes and gets all the packages and then gets installed the next step that you have to do is you have to look at the rules that are there ok. So, for this what you do is you can go to the rules are actually given in two places one is I can just do a edit of the rule.

So, e t c slash IP tables rules dot this is for v 4 IP v 4.

(Refer Slide Time: 03:39)


Ubuntu14 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:12 PM
iptables.docx - LibreOffice Writer
Default Style
Liberation Serif
12
Page 1 / 1 1 words, 2 characters selected Default Style English (India)
ForPresentation
[IS4-NF10.ppt - L...
Oracle VM Virtua...
Ubuntu14 [Runni...
Kali-Linux-1.1.0a...
Right Ctrl
12:12

root@mjsraman-Ubuntu14-32: ~

```
*filter
# Allow all outgoing, but drop incoming and forwarding packets by default
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

# Custom per-protocol chains
:UDP - [0:0]
:TCP - [0:0]
:ICMP - [0:0]

# Acceptable UDP traffic

# Acceptable TCP traffic
#-A TCP -p tcp --dport 22 -j ACCEPT

# Acceptable ICMP traffic

# Boilerplate acceptance policy
#-A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
#-A INPUT -i lo -j ACCEPT

# Drop invalid packets
"/etc/iptables/rules.v4" 71L, 1763C                          1,1           Top
```

First add a root user and work with this root
root user in Ubuntu and add to the sudo user
installation. But in your case if you do not ha
user.

Su -
adduser demo
gpasswd -a demo sudo

```
Install iptables
sudo apt-get update
sudo apt-get install iptables-persiste

The iptables command only handles IPv4
companion tool called ip6tables is use
and chains. For iptables-persistent, t
/etc/iptables/rules.v4 and the IPv6 ru
```

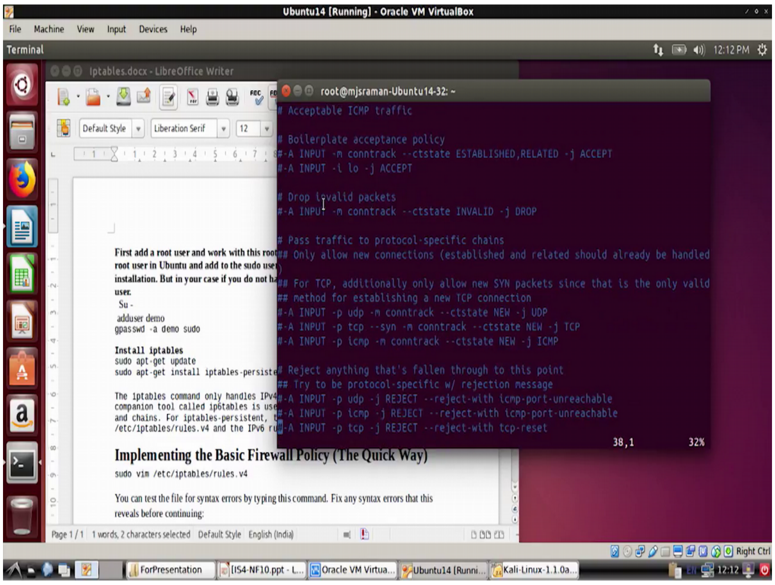
Implementing the Basic Firewall Policy (The Quick Way)

sudo vim /etc/iptables/rules.v4

You can test the file for syntax errors by typing this command. Fix any syntax errors that this reveals before continuing:

So, these are all the bunch of rules that you have for IP v 4 as I told you there is this filter then what to do input drop and all those things.

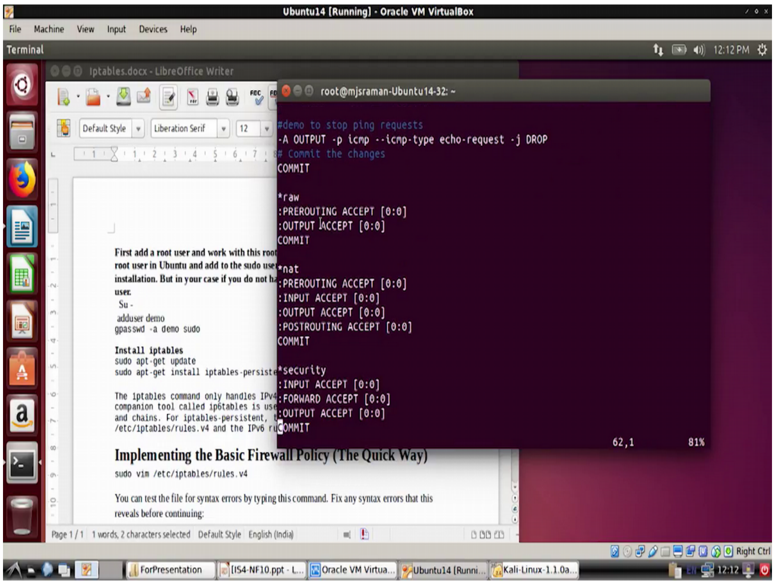
(Refer Slide Time: 03:48)



```
# Acceptable ICMP traffic

# Boilerplate acceptance policy
#-A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
#-A INPUT -i lo -j ACCEPT

# Drop invalid packets
#-A INPUT -m conntrack --ctstate INVALID -j DROP

# Pass traffic to protocol-specific chains
## Only allow new connections (established and related should already be handled
)
## For TCP, additionally only allow new SYN packets since that is the only valid
## method for establishing a new TCP connection
#-A INPUT -p udp -m conntrack --ctstate NEW -j UDP
#-A INPUT -p tcp --syn -m conntrack --ctstate NEW -j TCP
#-A INPUT -p icmp -m conntrack --ctstate NEW -j ICMP

# Reject anything that's fallen through to this point
## Try to be protocol-specific w/ rejection message
#-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
#-A INPUT -p icmp -j REJECT --reject-with icmp-port-unreachable
#-A INPUT -p tcp -j REJECT --reject-with tcp-reset
                                                       38,1          32%
```

So, if you look at this configuration file it has bunch of rules ok.

(Refer Slide Time: 03:54)

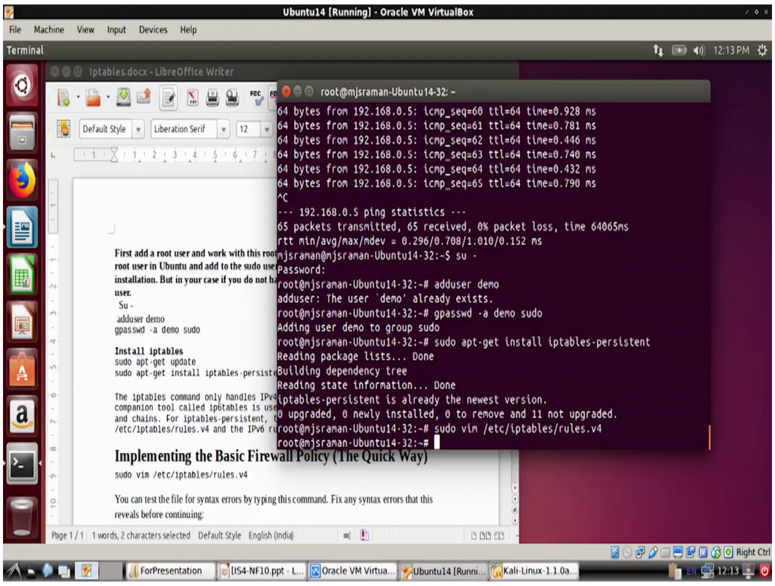


```
#demo to stop ping requests
-A OUTPUT -p icmp --icmp-type echo-request -j DROP
# Commit the changes
COMMIT

*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT

*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT

*security
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
                                                       62,1          81%
```

And what we could do is. we could add I mean in this demo I am just going to add a one rule here is a rule that I have added that if I send out from my Ubuntu machine an ICMP packet and if the packet is of echo request then the rule says that do not send the packet just drop it ok; it is a very simple rule there are other ways for example, there is a NAT table here is a security table you can have a raw packet table etcetera, but I blocked all of the things just for the demo purposes if you actually install it you will get bunch of rules how to do track the connections and all those things.

So, let us not complicate I mean the if as initially it is it is a very simple rule to block someone to ping from my machine to the other machine only thing I have to check is that ok. So, here is the rule minus A output minus p ICMP, ICP type echo request minus j drop.

(Refer Slide Time: 04:53)


Ubuntu14 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:13 PM
Iptables.docx - LibreOffice Writer
Default Style
Liberation Serif
12
root@mjsraman-Ubuntu14-32: ~
Page 1 / 1 1 words, 2 characters selected Default Style English (India)
ForPresentation
[IS4-NF10.ppt - L...
Oracle VM Virtua...
Ubuntu14 [Runni...
Kali-Linux-1.1.0a...
Right Ctrl
12:13

First add a root user and work with this root
root user in Ubuntu and add to the sudo use
installation. But in your case if you do not ha
user.

Su -
adduser demo

```
gpasswd -a demo sudo
```

Install iptables

```
sudo apt-get update
sudo apt-get install iptables-persiste

The iptables command only handles IPv4
companion tool called ip6tables is use
and chains. For iptables-persistent, t
/etc/iptables/rules.v4 and the IPv6 ru
```

Implementing the Basic Firewall Policy (The Quick Way)

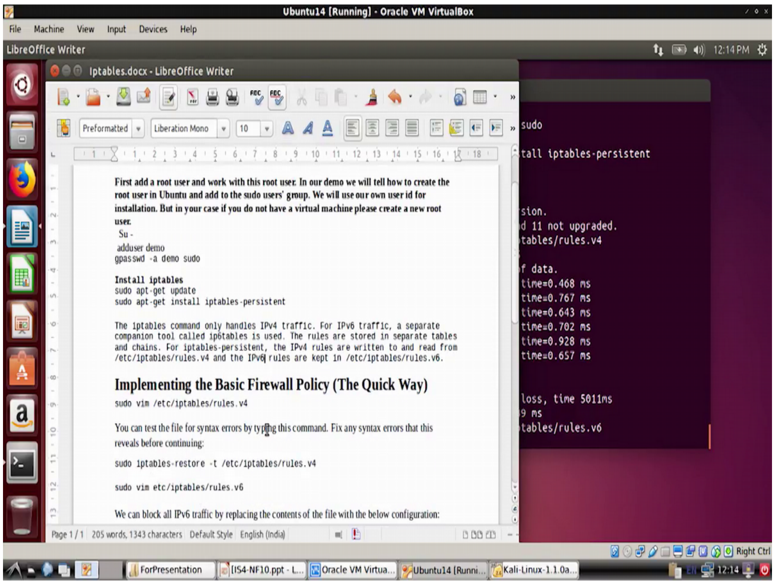
```
sudo vim /etc/iptables/rules.v4
```

You can test the file for syntax errors by typing this command. Fix any syntax errors that this reveals before continuing:

```
64 bytes from 192.168.0.5: icmp_seq=60 ttl=64 time=0.928 ms
64 bytes from 192.168.0.5: icmp_seq=61 ttl=64 time=0.781 ms
64 bytes from 192.168.0.5: icmp_seq=62 ttl=64 time=0.446 ms
64 bytes from 192.168.0.5: icmp_seq=63 ttl=64 time=0.740 ms
64 bytes from 192.168.0.5: icmp_seq=64 ttl=64 time=0.432 ms
64 bytes from 192.168.0.5: icmp_seq=65 ttl=64 time=0.790 ms
^C
--- 192.168.0.5 ping statistics ---
65 packets transmitted, 65 received, 0% packet loss, time 64065ms
rtt min/avg/max/mdev = 0.296/0.708/1.010/0.152 ms
mjsraman@mjsraman-Ubuntu14-32:~$ su -
Password:
root@mjsraman-Ubuntu14-32:~# adduser demo
adduser: The user `demo' already exists.
root@mjsraman-Ubuntu14-32:~# gpasswd -a demo sudo
Adding user demo to group sudo
root@mjsraman-Ubuntu14-32:~# sudo apt-get install iptables-persistent
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables-persistent is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
root@mjsraman-Ubuntu14-32:~# sudo vim /etc/iptables/rules.v4
root@mjsraman-Ubuntu14-32:~#
```

So,. So, if you look at the rule right now I am able to ping the other machine ok. So, if I do a ping dot 168 dot 0 dot 5; I am able to ping the other machine. So, similarly you also have rules for IP v 6. So, you can also edit the IP v 6 rules and currently I mean just drops all the IP v 6 packets if you look at the drops. So, we are not interested in any IP v 6 traffic right now. So, we are not doing with the IP v 6 traffic now let us one of the things is once you actually write the rules new rules.

(Refer Slide Time: 05:31)



Ubuntu14 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
LibreOffice Writer
12:14 PM
Iptables.docx - LibreOffice Writer
Preformatted
Liberation Mono
10
Page 1 / 1 205 words, 1343 characters Default Style English (India)
ForPresentation
[IS4-NF10.ppt - L...
Oracle VM Virtua...
Ubuntu14 [Runni...
Kali-Linux-1.1.0a...
Right Ctrl
12:14

First add a root user and work with this root user. In our demo we will tell how to create the root user in Ubuntu and add to the sudo users' group. We will use our own user id for installation. But in your case if you do not have a virtual machine please create a new root user.

```
 Su -
 adduser demo
gpasswd -a demo sudo
```

Install iptables

```
sudo apt-get update
sudo apt-get install iptables-persistent
```

The iptables command only handles IPv4 traffic. For IPv6 traffic, a separate companion tool called ip6tables is used. The rules are stored in separate tables and chains. For iptables-persistent, the IPv4 rules are written to and read from /etc/iptables/rules.v4 and the IPv6 rules are kept in /etc/iptables/rules.v6.

Implementing the Basic Firewall Policy (The Quick Way)

```
sudo vim /etc/iptables/rules.v4
```

You can test the file for syntax errors by typing this command. Fix any syntax errors that this reveals before continuing:

```
sudo iptables-restore -t /etc/iptables/rules.v4

sudo vim etc/iptables/rules.v6
```

We can block all IPv6 traffic by replacing the contents of the file with the below configuration:

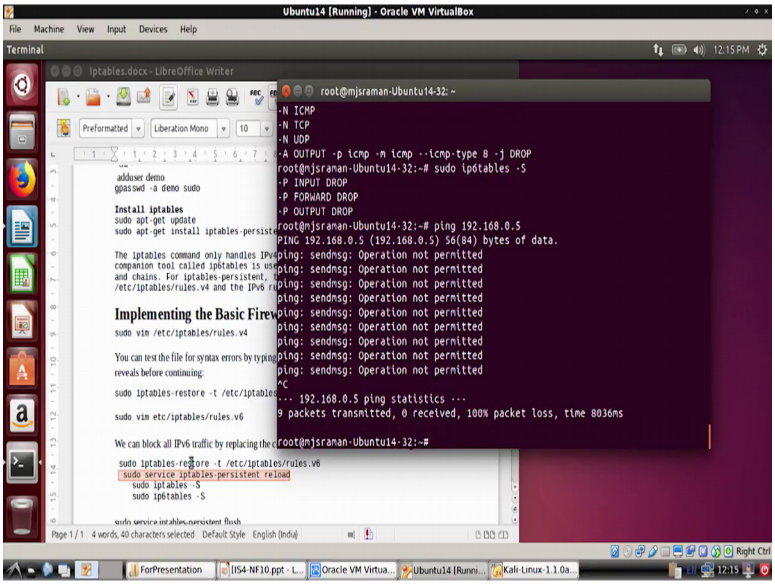
```
sudo

tall iptables-persistent



sion.
d 11 not upgraded.
tables/rules.v4

f data.
time=0.468 ms
time=0.767 ms
time=0.643 ms
time=0.702 ms
time=0.928 ms
time=0.657 ms


loss, time 5011ms
9 ms
tables/rules.v6
```

You can actually a test the rules ok. So, it is; so, there are no syntax errors. So, here is the command that we can do I mean just to ensure that the demo goes very fast as just cutting pasting this command. So, otherwise you might have to type it. So, if you chase that ok. So, everything is fine the rules there is no syntax error or things like that in the rules ok. Now what I will do is I will just go ahead and what I can do is I can just go ahead and load the rules.

So here is what I do now it is loaded the rules and if you want see what rules I have loaded for a IP v 4 I can look at tables minus S. So, it says that I have added one rule it says to drop ICMP packets and if you see IP v 6 what are all the rules that I have added; it just tells you that the everything any IP input packet you just have to drop it IP v 6 packet you have to drop it. So, what will happen?

So, what we expect to happen is that. So, we have been doing a ping and we have told the IP v 6 to stop doing any ping. So, let us try to do a ping and see what happens. So, it clearly says that the operation is not permitted which means our packet is getting filtered now I will flush the rule.

(Refer Slide Time: 07:01)



```
-N ICMP
-N TCP
-N UDP
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j DROP
root@mjsraman-Ubuntu14-32:~# sudo ip6tables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
root@mjsraman-Ubuntu14-32:~# ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.0.5 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8036ms

root@mjsraman-Ubuntu14-32:~#
```

```
adduser demo
gpasswd -a demo sudo

Install iptables
sudo apt-get update
sudo apt-get install iptables-persiste

The iptables command only handles IPv4
companion tool called ip6tables is use
and chains. For iptables-persistent,
/etc/iptables/rules.v4 and the IPv6 ru
```

Implementing the Basic Firew

```
sudo vim /etc/iptables/rules.v4
```

You can test the file for syntax errors by typing
reveals before continuing:

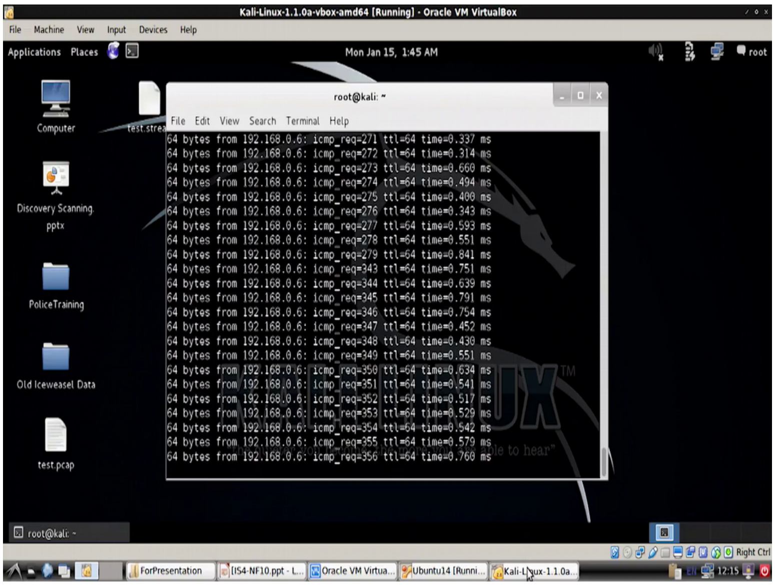
```
sudo iptables-restore -t /etc/iptables

sudo vim etc/iptables/rules.v6
```

We can block all IPv6 traffic by replacing the c

```
sudo iptables-restore -t /etc/iptables/rules.v6
sudo service iptables-persistent reload
   sudo iptables -S
   sudo ip6tables -S

sudo service iptables-persistent flush
```

See what I can do is just to show that our rule is working let me go and flush these rules and let us see what happens ok. So, a flushing the flushing means I am removing the rules ok. And what I now I will do a ping again now the packets are going through straight away. So, this is exactly what IP tables can do and if you want to see one of things next question you might ask.

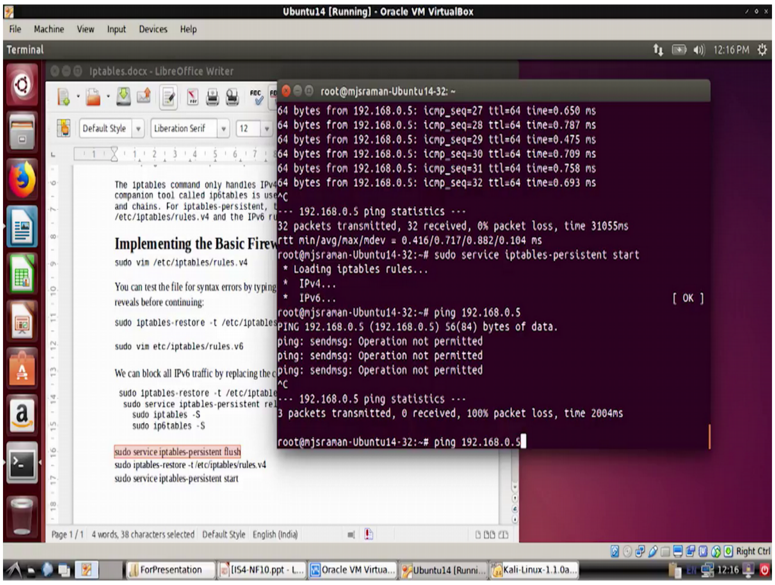
(Refer Slide Time: 07:24)



```
64 bytes from 192.168.0.6: icmp_req=271 ttl=64 time=0.337 ms
64 bytes from 192.168.0.6: icmp_req=272 ttl=64 time=0.314 ms
64 bytes from 192.168.0.6: icmp_req=273 ttl=64 time=0.660 ms
64 bytes from 192.168.0.6: icmp_req=274 ttl=64 time=0.494 ms
64 bytes from 192.168.0.6: icmp_req=275 ttl=64 time=0.400 ms
64 bytes from 192.168.0.6: icmp_req=276 ttl=64 time=0.343 ms
64 bytes from 192.168.0.6: icmp_req=277 ttl=64 time=0.593 ms
64 bytes from 192.168.0.6: icmp_req=278 ttl=64 time=0.551 ms
64 bytes from 192.168.0.6: icmp_req=279 ttl=64 time=0.841 ms
64 bytes from 192.168.0.6: icmp_req=343 ttl=64 time=0.751 ms
64 bytes from 192.168.0.6: icmp_req=344 ttl=64 time=0.639 ms
64 bytes from 192.168.0.6: icmp_req=345 ttl=64 time=0.791 ms
64 bytes from 192.168.0.6: icmp_req=346 ttl=64 time=0.754 ms
64 bytes from 192.168.0.6: icmp_req=347 ttl=64 time=0.452 ms
64 bytes from 192.168.0.6: icmp_req=348 ttl=64 time=0.430 ms
64 bytes from 192.168.0.6: icmp_req=349 ttl=64 time=0.551 ms
64 bytes from 192.168.0.6: icmp_req=350 ttl=64 time=0.634 ms
64 bytes from 192.168.0.6: icmp_req=351 ttl=64 time=0.541 ms
64 bytes from 192.168.0.6: icmp_req=352 ttl=64 time=0.517 ms
64 bytes from 192.168.0.6: icmp_req=353 ttl=64 time=0.529 ms
64 bytes from 192.168.0.6: icmp_req=354 ttl=64 time=0.542 ms
64 bytes from 192.168.0.6: icmp_req=355 ttl=64 time=0.579 ms
64 bytes from 192.168.0.6: icmp_req=356 ttl=64 time=0.760 ms
```

So, sir, but here if you see the ping has been consistently going on; that means, we are only blocking the output packets, the input packets that are sent by the route does not get affected because we have not put a filter on the input chain we have only put the filter on the output chain. So, if you just want to try out just if you. So, now, let us go ahead and reload the rules you can even say IP tables service; it will start and so, it has now reloaded the rules now if you see the operation is not permitted ok.

(Refer Slide Time: 08:02)



Ubuntu14 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:16 PM
Iptables.docx - LibreOffice Writer
Default Style
Liberation Serif
12
Page 1 / 1 4 words, 38 characters selected Default Style English (India)
ForPresentation
[IS4-NF10.ppt - L...
Oracle VM Virtua...
Ubuntu14 [Runni...
Kali-Linux-1.1.0a...
Right Ctrl
12:16

```
The iptables command only handles IPv4
companion tool called ip6tables is use
and chains. For iptables-persistent, t
/etc/iptables/rules.v4 and the IPv6 ru
```

Implementing the Basic Firew

```
sudo vim /etc/iptables/rules.v4
```

You can test the file for syntax errors by typing
reveals before continuing:

```
sudo iptables-restore -t /etc/iptables

sudo vim etc/iptables/rules.v6
```

We can block all IPv6 traffic by replacing the c

```
 sudo iptables-restore -t /etc/iptable
  sudo service iptables-persistent rel
    sudo iptables -S
    sudo ip6tables -S
```

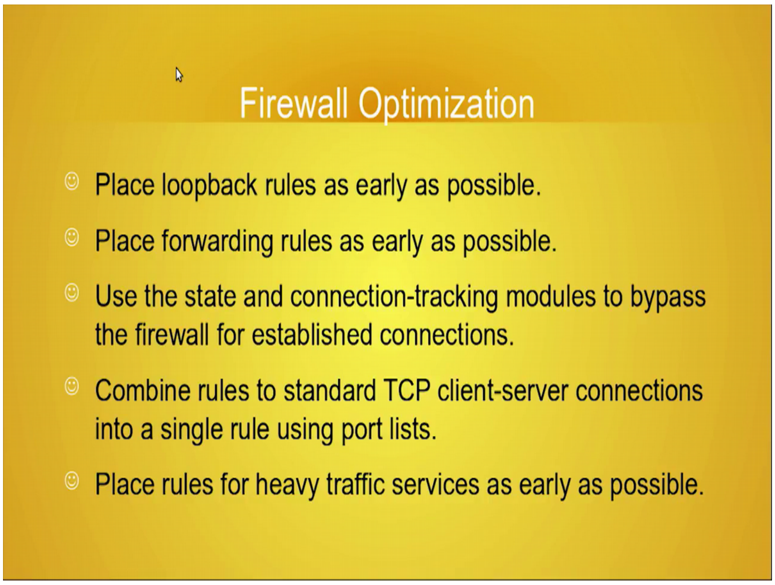
```
sudo service iptables-persistent flush
sudo iptables-restore -t /etc/iptables/rules.v4
sudo service iptables-persistent start
```

root@mjsraman-Ubuntu14-32: ~

```
64 bytes from 192.168.0.5: icmp_seq=27 ttl=64 time=0.650 ms
64 bytes from 192.168.0.5: icmp_seq=28 ttl=64 time=0.787 ms
64 bytes from 192.168.0.5: icmp_seq=29 ttl=64 time=0.475 ms
64 bytes from 192.168.0.5: icmp_seq=30 ttl=64 time=0.709 ms
64 bytes from 192.168.0.5: icmp_seq=31 ttl=64 time=0.758 ms
64 bytes from 192.168.0.5: icmp_seq=32 ttl=64 time=0.693 ms
^C
--- 192.168.0.5 ping statistics ---
32 packets transmitted, 32 received, 0% packet loss, time 31055ms
rtt min/avg/max/mdev = 0.416/0.717/0.882/0.104 ms
root@mjsraman-Ubuntu14-32:~# sudo service iptables-persistent start
 * Loading iptables rules...
 *  IPv4...
 *  IPv6...                                                          [ OK ]
root@mjsraman-Ubuntu14-32:~# ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.0.5 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2004ms

root@mjsraman-Ubuntu14-32:~# ping 192.168.0.5
```

So, what I can do right now. So, if I want to find out what are all the rules that are there IP tables minus S. So, it tells you this drop rule is there; so, if you just converted into input you can actually drop the ping I mean you will not be able to respond to the ping of the input. So, this is very simple and straight forward way of getting this IP tables working and there are very many complications yes ah, but I think this will tell you how to get a simple firewall working in your machine.

(Refer Slide Time: 08:34)



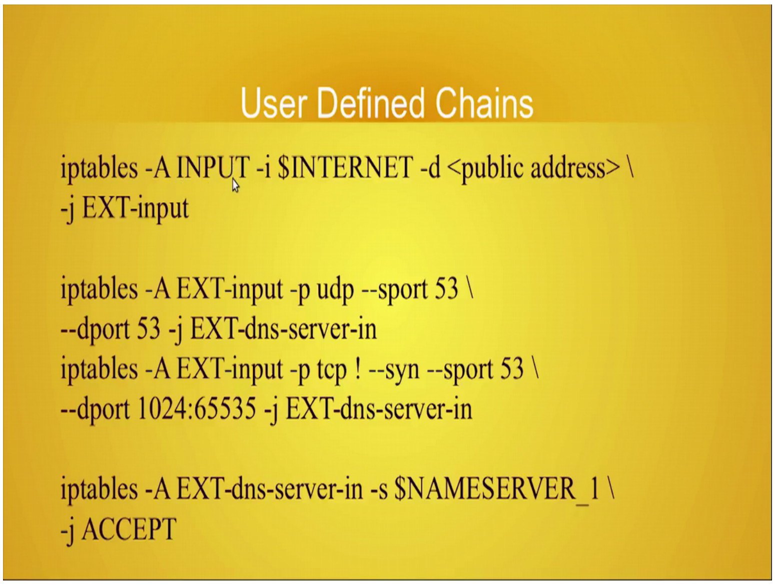
Firewall Optimization

- Place loopback rules as early as possible.
- Place forwarding rules as early as possible.
- Use the state and connection-tracking modules to bypass the firewall for established connections.
- Combine rules to standard TCP client-server connections into a single rule using port lists.
- Place rules for heavy traffic services as early as possible.

So, now let us continue with what we have been discussing and what we have been discussing is that how to place the rule? So, this is the exactly what you have discussing in the previous sections; so how we are planning to place these rule and we just had one rule therefore, we placed it before we just after the in the filter class in the filter table and we were able to filter it.

You can actually have more than see we were having a only one chain the input chain the output chain and the and the forward chain ok. So, you can actually define your own chains ok. So, here is an examples.

(Refer Slide Time: 09:15)



User Defined Chains

```
iptables -A INPUT -i $INTERNET -d <public address> \
-j EXT-input

iptables -A EXT-input -p udp --sport 53 \
--dport 53 -j EXT-dns-server-in
iptables -A EXT-input -p tcp ! --syn --sport 53 \
--dport 1024:65535 -j EXT-dns-server-in

iptables -A EXT-dns-server-in -s $NAMESERVER_1 \
-j ACCEPT
```

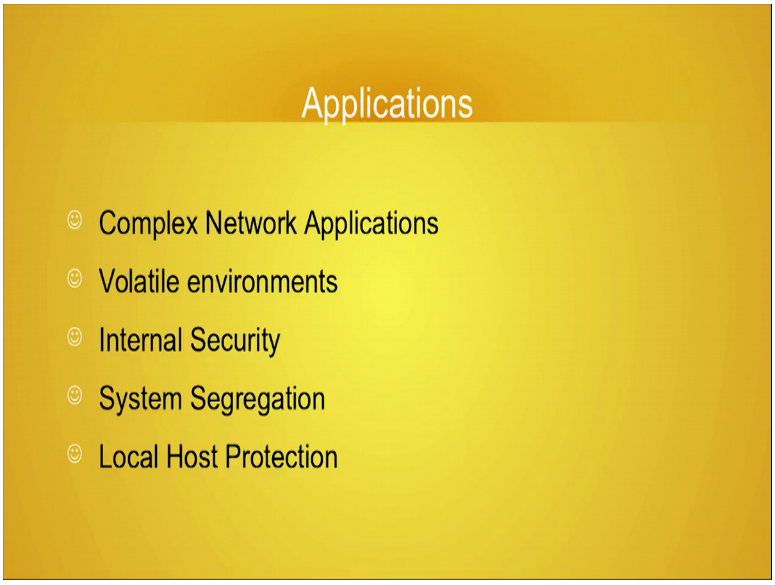
So, what I do is? Here I add something known as external input I jump to a chain called rules called external input. And in the external rule input I jumped to something known as d n s server and in the d n s server I put some more rules.

So, this is the way I can create a user defined chains. So, previously what was happening was that on the output in our example on the outputs. So, let us go back to our example then see we were doing ok. So, in Ubuntu virtual box we were putting it on the output we just use the rule called drop ok. Instead of using this rule called drop I can actually define my own chain that is exactly what we have done.

So, in this case what you have done is this j if you look at this instead of dropping the packet we are trying it up with an external rule. So, once we tied up with this rule this rules starts executing and after this rule; we just go to this chain and we start executing this chain and so, on. So, so in this way I will be able to configure more and more rules to make this work ok.

So, I have this gives you very brief introduction ok.

(Refer Slide Time: 10:26)



Applications

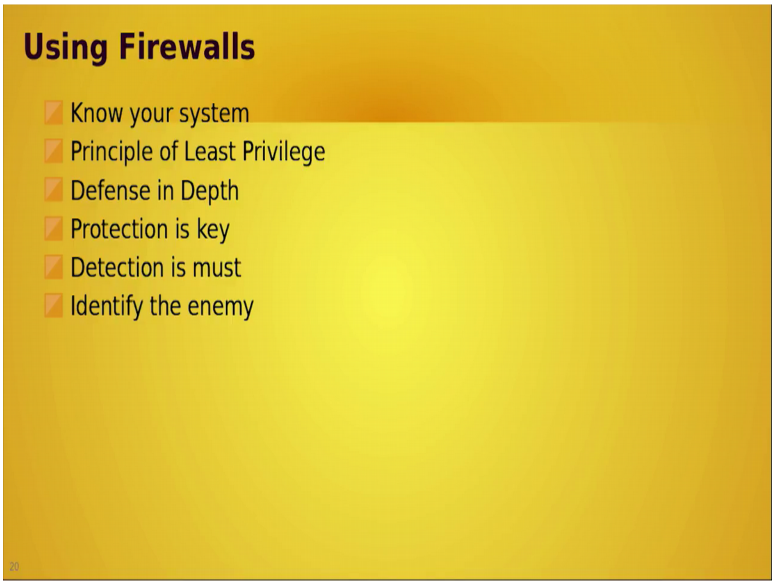
- Complex Network Applications
- Volatile environments
- Internal Security
- System Segregation
- Local Host Protection

Where and where do we apply this kind of firewalls? See you can have complex network and environments where one network does not want to talk to the other network I mean one way is to submit the process, but even if you do submitting if I change the network IP address or I may I may spoof the IP address I will be able to talk to the other person ok.

So, these things can be avoided by using a firewall and it essentially ensures that you can break you can segregate your networks ok. Then there are this volatile environments then it is essentially for internal security and the environments that change where some places you do not want to change see for example, many organizations will change their IP address quite frequently internal IP addresses. Sometimes because they do not want someone to be with the same static IP address for a long time because it is you could actually they could be the vulnerable points in your network.

As I told you can do system segregation. So, you can have partitions. So, that the two partitions do not pack with each other major three partitions with firewall as you know is the demilitarized zone the input and the output networks and you can also protect the local hosts. For example, in our case actually we are more interested in protecting the local host by blocking all the ICMP packets, rather than a opening of the host.

(Refer Slide Time: 11:50)



Using Firewalls

- Know your system
- Principle of Least Privilege
- Defense in Depth
- Protection is key
- Detection is must
- Identify the enemy

One of the things that we should know is that especially with respect to security is when you are using firewalls you should be very aware of what is the system you are using. You should not get blocked by your own system by using certain rules I mean if you apply the rules just for the rules sake like what we do in India you land up with lot of trouble ok.

So, because the rules are created for a particular purpose and you should look at whether you are achieving the purpose rather than looking at the rules alone thus very sacred ok. The intension behind the rule is what we are supposed to look ok. So, here is something known as principle of least privileges it tells you that never open up access to all the people, all the time and make them very independent ok.

So, you should only give the information or the packets that user want it should be least privileged. And if someone wants to get a higher privilege its better they actually apply for it and get it ok. The second thing that you the third thing that you should know is that you should do defense in debt ok. So, it is not a question of just blocking the packets you should also try to lock packets and then try to analyze if you find something fishy its better you go to the depth of it rather than say for example, many times what happens is that we are covered by some kind of an insurance.

So for example, let us say you have an accident insurance policy it is true that many insurance policies say that you can have n number of accidents and still your insurance would be paid and you do not feel happy about it. For example, I have a car and I can have some n number of claims within a year it does not mean that I should bang everyone and then make the claim again and again and again.

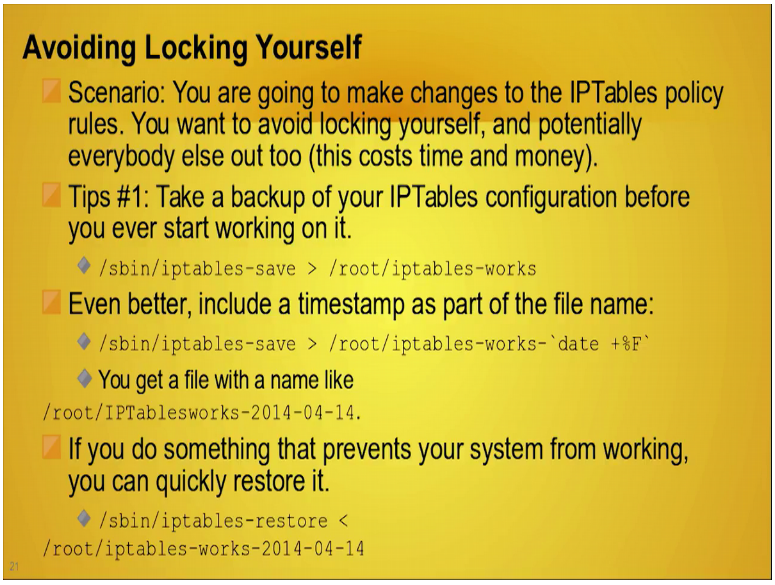
For example, if someone comes and hits my car more than once or a twice or a thrice then actually there is a suspicion that either you are not driving well or you have a bad luck in your life. So, you have to go in depth and find out whether there is a problem with your driving or I mean fate is that your car you are not lucky with your car ok.

So, that is known as so whenever there is a symptom just go to your root cause just do not just leave the symptom as it is and then cure the symptoms to say that I am very happy about it. Similarly in this kind of firewall configuration protection must be the key ok. So, that is why you have to go to defense in depth ok. So, once you are able to protect the network; you actually come out of lot of hassles if you are not going to protect your network you are going to be in deep trouble because once an incident is happened ok.

Then you have to spend lot of time identifying why the incident has happened; be you have to ensure that the incident does not repeat again. So, being proactive is the key here ok; so, by protection you are being proactive once I am breached definitely no one's PC is safe as I told at the beginning of this network security section everyone's PC is vulnerable, but the question is if you are attacked are you able to detect why you have been attacked.

And you should also detect who has attacked you ok. So, this is what you are supposed to do with the help of firewalls there are lot of features in firewalls other than what we have discussed. Because this is a sort of overall course on network security; we are just introduced this concept of firewall how to actually configure it is much more to the this ah. So, please go ahead and spend some time reading about firewalls intrusion detection and prevention system.

(Refer Slide Time: 15:33)



Avoiding Locking Yourself

- Scenario: You are going to make changes to the IPTables policy rules. You want to avoid locking yourself, and potentially everybody else out too (this costs time and money).
- Tips #1: Take a backup of your IPTables configuration before you ever start working on it.
  - `/sbin/iptables-save > /root/iptables-works`
- Even better, include a timestamp as part of the file name:
  - ``/sbin/iptables-save > /root/iptables-works-`date +%F` ``
  - You get a file with a name like

`/root/IPTablesworks-2014-04-14.`

- If you do something that prevents your system from working, you can quickly restore it.
  - `/sbin/iptables-restore <`

`/root/iptables-works-2014-04-14`

21

So, what are all the good rules that someone must follow? So, the first thing that you should do is avoid locking yourself ok. So, these are some of the good practices that you like to follow please be hands on try more rules as we discussed in the class, try more rules with your firewalls and see how the firewalls work.

Thank you very much.

Welcome to this section on network security and forensics. So, we were looking at how to install firewalls? How to work with firewall rules? What are the rules and how do you ensure that you use the firewalls in a nice manner to protect your organization as well as detect any issues that might come up.

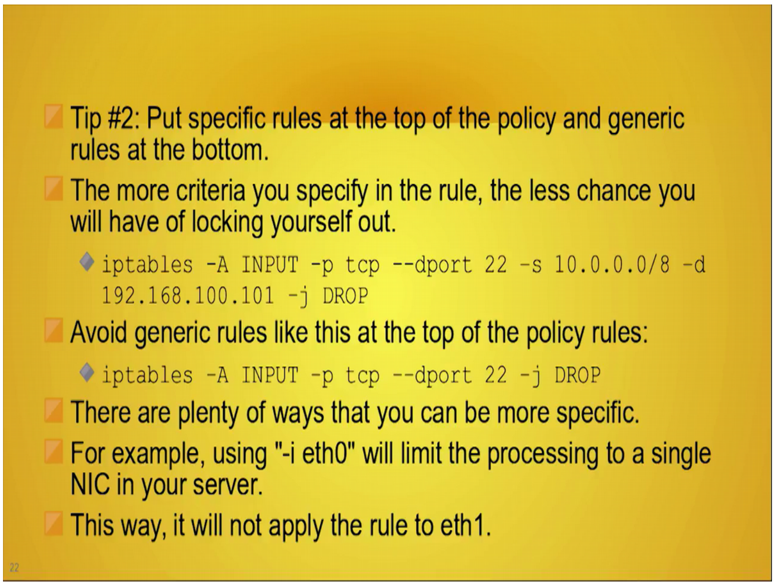
Now we will look at some of the good practices and we will also spend a few minutes on what all the different types of logs that one could get and how why we should write uniscripts, basescripts continuously to keep us updated; because the whole job of collecting the logs and doing the forensics as we had seen earlier is extremely difficult unless you automate it and you have bunch of tools you are going to find it difficult to solve any problem ok.

So, the most important thing that you should do is to avoid locking yourself when you are using this kind of tools like firewalls and intrusion detection systems etcetera. First thing we do is always take a back up of your IP tables configuration before you ever start working on it ah; I think we did that in our previous demo, but not during the IP tables demo ok.

So, we just wanted to caution you that the when the second time that we use we never took any backup which has (Refer Time: 17:20) and modify the tables just like that where as in smart demo actually we made a copy of it and then use the copy if you remember correctly ah. The other things that you should do is always save the IP tables or or your configuration with the timestamp because you should use the latest I mean your latest configuration file should be available if in case you face any problem ok.

And if you do something that burns your system from working when quickly restore it. So, you can restore it to this particular date etcetera and make a copy of this and store it separately; do not store it in the same machine because if your machine gets attacked you would lose this configuration its better you I have a backup of the configurations somewhere.

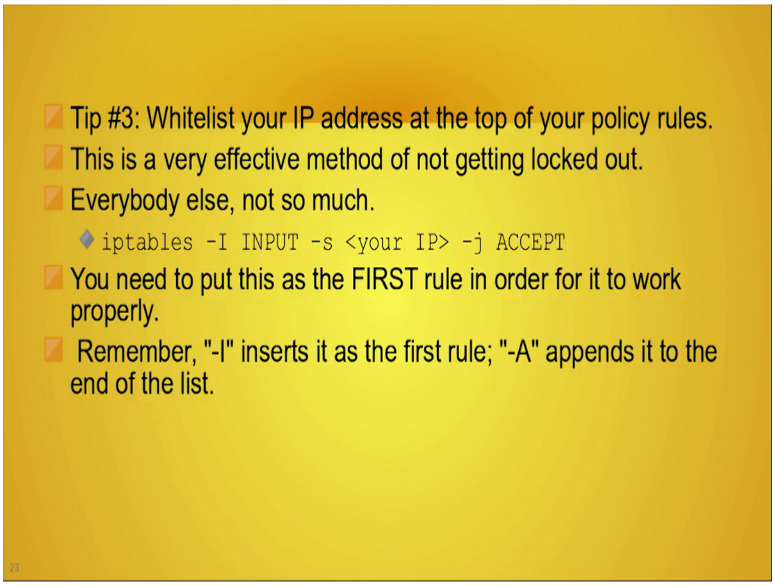
(Refer Slide Time: 18:02)



- Tip #2: Put specific rules at the top of the policy and generic rules at the bottom.
- The more criteria you specify in the rule, the less chance you will have of locking yourself out.
  - iptables -A INPUT -p tcp --dport 22 -s 10.0.0.0/8 -d 192.168.100.101 -j DROP
- Avoid generic rules like this at the top of the policy rules:
  - iptables -A INPUT -p tcp --dport 22 -j DROP
- There are plenty of ways that you can be more specific.
- For example, using "-i eth0" will limit the processing to a single NIC in your server.
- This way, it will not apply the rule to eth1.

Put specific rules at the top of the policy and generic rules at the bottom and I think we discussed this lot in the previous section ok. The more criteria you specify in the rule the less chance you will have a locking of yourself out ok. So, you need to be ah; so, because if you make very specific rules the chance that that specific rule will be applied is will be a very less ok. So, you could use some other for example, I am blocking a specific port then I could ask if I get blocked then I as well reconfigure to some other port and then enter the machine ok. So, that is what we need ok.

(Refer Slide Time: 18:44)



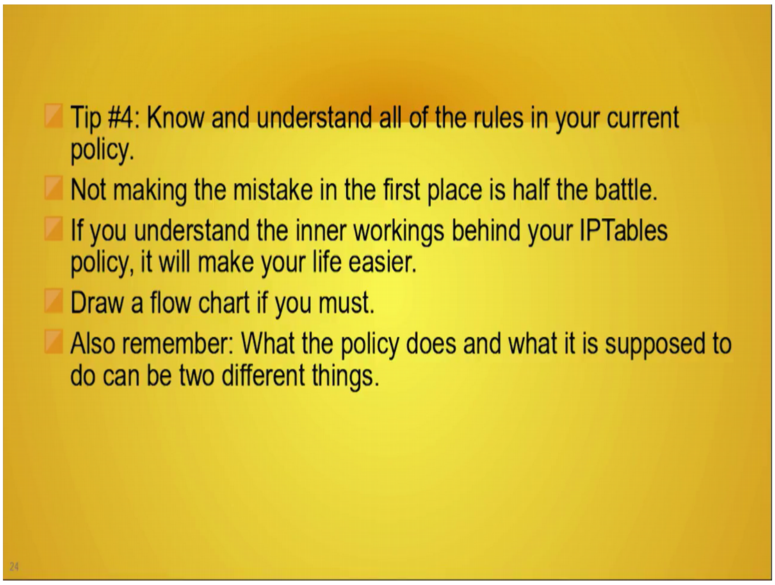
- Tip #3: Whitelist your IP address at the top of your policy rules.
- This is a very effective method of not getting locked out.
- Everybody else, not so much.
  - `iptables -I INPUT -s <your IP> -j ACCEPT`
- You need to put this as the FIRST rule in order for it to work properly.
- Remember, "-I" inserts it as the first rule; "-A" appends it to the end of the list.

So, the Whitelist your IP addresses are top of your policy rules; whitelist tells you that yes this is allowed. So, your IP address should be allowed for any activity for example, your machine your laptop must be allowed for any activity to configure in the firewall or some other place and all other IP address packing for administrative privileges should be blocked.

So, you can bring a rule says that ok. So, only if I login from my network you will get a administrative privileges if you or login from my laptop you will get a administrative privilege always have a back up laptop also for login in ok; you need to put this that accepting your IP address as a first rule in your file ok.

So, minus I inserts the rule if you remember we have put it and minus A appends the rule.

(Refer Slide Time: 19:34)



- Tip #4: Know and understand all of the rules in your current policy.
- Not making the mistake in the first place is half the battle.
- If you understand the inner workings behind your IPTables policy, it will make your life easier.
- Draw a flow chart if you must.
- Also remember: What the policy does and what it is supposed to do can be two different things.

24

One all these rules must be generated based on your organizational policy ok. So, this is true for snort this is true for firewalls ok; you should not introduce any rules which is not there in the policy. And if the policy does not sufficiently cover the security then escalate it and get it covered rather than introducing your own rules which does not stick your policies because there could be legal implications if you do that.

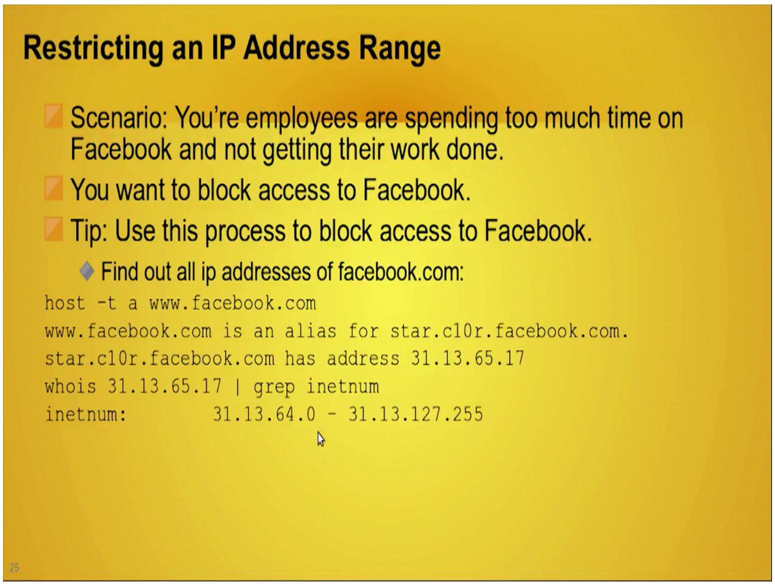
And getting the rules every time you configure the rules remember we gave you a command for checking the rules ok; please use that command, check that there is no syntax error in the rules and then apply the rule. Because the usually have this option of I think I i mentioned earlier also that if step two does not work we all goes to step three and then try to see whether step three works instead of step two working.

Now, that should be avoided when you configure this kind of firewalls and other thing is please understand what is the rule chain it is better have a flow chart a it is like a programming language. So, even if you take snort or if you take this IP tables it is what is specific as a rules is a sort of programming language.

And remember programming languages and programming you do it for others not for yourself ok. So, if you are not there will the other person will able to understand this whatever rules you are written that should be priority in mind rather than I am brilliant guy I have got a great rule and nobody else can understand what my rule is.

So, that that does not work in this kind of scenario especially in the area of security ok; the other thing is you have to match the policy with the rule ok. So, sometimes what happens is what the policy does and what is supposed to do can be two different things ok. So, this is exactly what I was telling you even if you have a rule see the intension behind the rule not the rule by itself ok.

(Refer Slide Time: 21:32)



Restricting an IP Address Range

- Scenario: You're employees are spending too much time on Facebook and not getting their work done.
- You want to block access to Facebook.
- Tip: Use this process to block access to Facebook.
  - Find out all ip addresses of facebook.com:

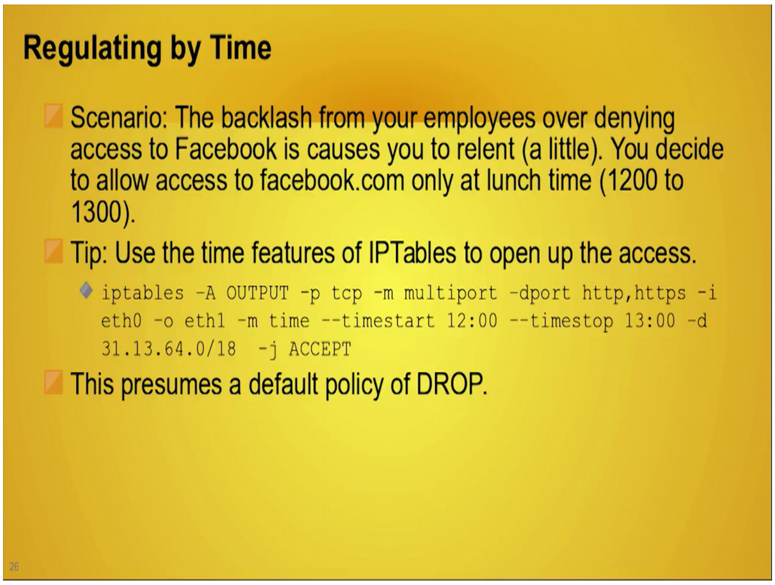
```
host -t a www.facebook.com
www.facebook.com is an alias for star.c10r.facebook.com.
star.c10r.facebook.com has address 31.13.65.17
whois 31.13.65.17 | grep inetnum
inetnum:        31.13.64.0 - 31.13.127.255
```

25

So, here is an example of. So, you are employees are you know that your employees are spending too much of time on Facebook and not getting their work done. So, you want to block access to Facebook ok. So, this is an example of how I can block access to Facebook ok. So, here it says host minus t minus a w w w Facebook dot com. So, it says that Facebook is an alias for star dot c 1 0 r then is an IP address of of 31 dot 13 dot 65 dot 17, whois so, grep I net num ok. So, it has bunch of numbers. So, what you can do is you can go ahead and block this whole set of stuffs and ensure that your Facebook is blocked for the organization ah.

Well many times people will login to some other public IP server and then login to Facebook ok. So, this always the challenge always a challenge for a network security specialist as an administrator, the more smart you try to become user become much more smarter than you. So, this kind of a attitudes that you have to live this is where it is very challenging. So, here is the other way of blocking; so, you can tell your organization that I am going to block it between this time and this time.

(Refer Slide Time: 22:50)



Regulating by Time

- Scenario: The backlash from your employees over denying access to Facebook is causes you to relent (a little). You decide to allow access to facebook.com only at lunch time (1200 to 1300).
- Tip: Use the time features of IPTables to open up the access.

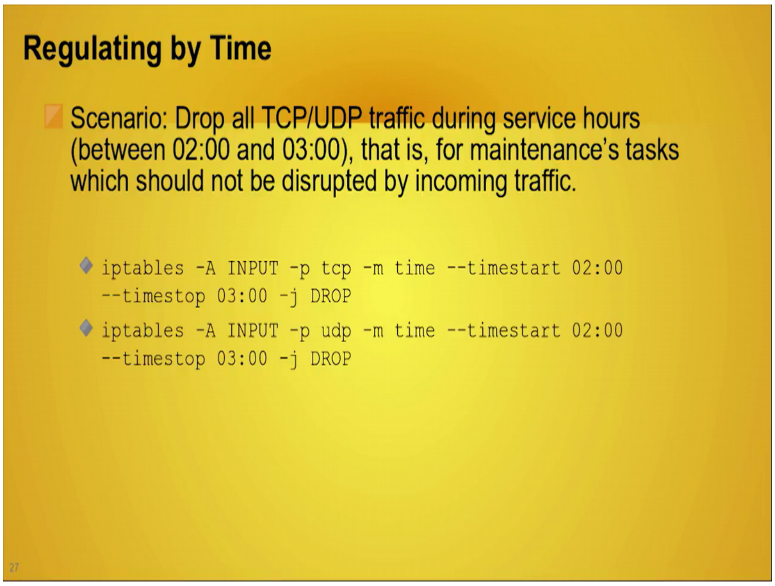
```
iptables -A OUTPUT -p tcp -m multiport -dport http,https -i
eth0 -o eth1 -m time --timestart 12:00 --timestop 13:00 -d
31.13.64.0/18  -j ACCEPT
```

- This presumes a default policy of DROP.

26

So, only between 12 and 1 during suppose it is a during lunch hour I can open up Facebook access and not for the rest of the time. So, here is small a example sometimes for example, some organizations will tell you that overall you can access only 10 minutes of a time you can go to Gmail and then login. So, those kinds of rules can be framed using firewalls.

(Refer Slide Time: 23:14)



Regulating by Time

- Scenario: Drop all TCP/UDP traffic during service hours (between 02:00 and 03:00), that is, for maintenance's tasks which should not be disrupted by incoming traffic.

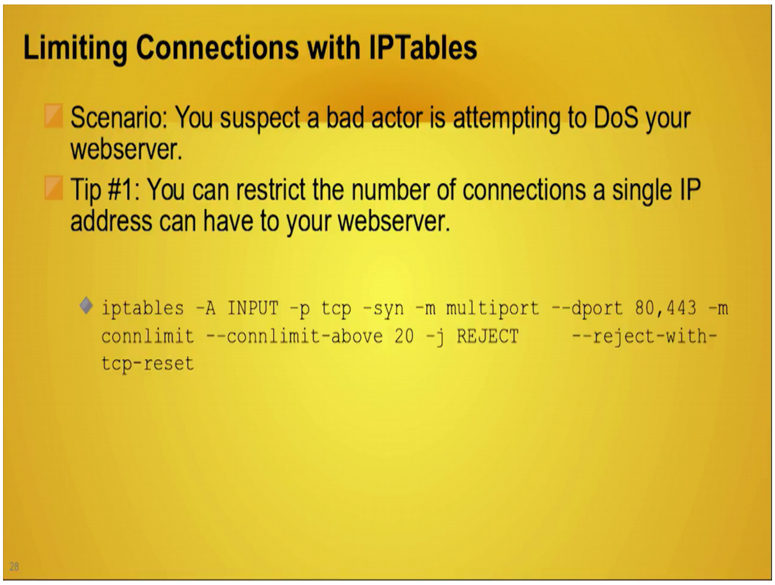
```
iptables -A INPUT -p tcp -m time --timestart 02:00
--timestop 03:00 -j DROP
iptables -A INPUT -p udp -m time --timestart 02:00
--timestop 03:00 -j DROP
```

27

So here is an example drop all TCP, UDP traffic during service hours between 2 and 3 that is for maintenance task which not be disrupted by incoming traffic. So, sometimes if you remember the net will be down that is what people say. Now how do you make the net down I mean you can either have wire and pull all the wires out or you can use the firewall which tells you that between this time and this time no network traffic should be allowed inside my network. So, that I drop every packet and you do the task whatever you want to do and then rest of that traffic.

So, this is another way of using the firewall. So, these are three different examples of using the firewall and the rules.

(Refer Slide Time: 23:51)



Limiting Connections with IPTables

- Scenario: You suspect a bad actor is attempting to DoS your webserver.
- Tip #1: You can restrict the number of connections a single IP address can have to your webserver.

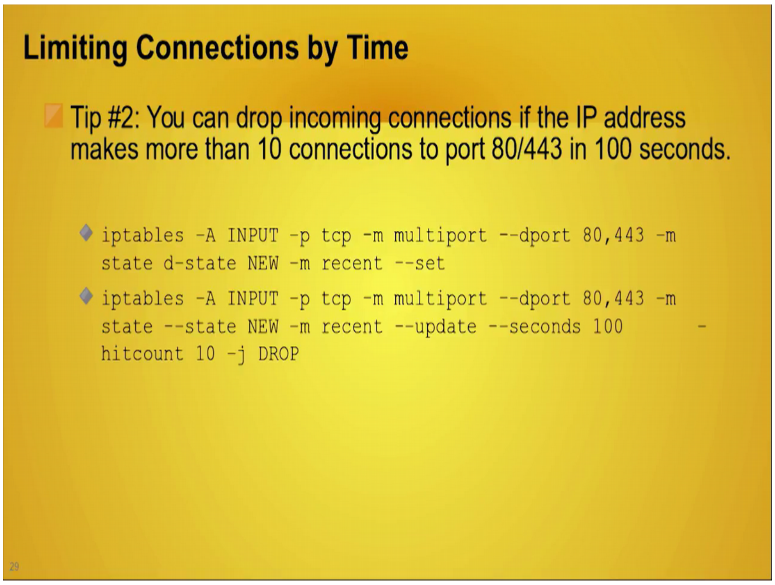
```
iptables -A INPUT -p tcp -syn -m multiport --dport 80,443 -m
connlimit --connlimit-above 20 -j REJECT     --reject-with-
tcp-reset
```

You can also have one more ok. So, you suspect you suspect there is a DoS attacks that is happening on your web server. So, how do I block it. So, here is a rule that can that can block the DoS attacks. So, here is a example of a rule I mean try to interpret this rule ok.

So, it says something like connection limit about 20 then you go ahead and reject it and then reject it with a tcp reset. So, so and what is the connection limit and then etcetera. So, so the idea is that; so, here you can use your firewall to block the DoS attack. So, remember we had a rate limiting of other way is you can you can do a rate limit here under many options available this is exactly what we are telling. So, what is the policy based on that you have to apply the rule either you rate limit or if it goes beyond you just reject it. So, these are all choices that are available to you.

So, how you configure what you configure depends on your organization policy.

(Refer Slide Time: 24:50)



Limiting Connections by Time

- Tip #2: You can drop incoming connections if the IP address makes more than 10 connections to port 80/443 in 100 seconds.

```
iptables -A INPUT -p tcp -m multiport --dport 80,443 -m
state d-state NEW -m recent --set
```

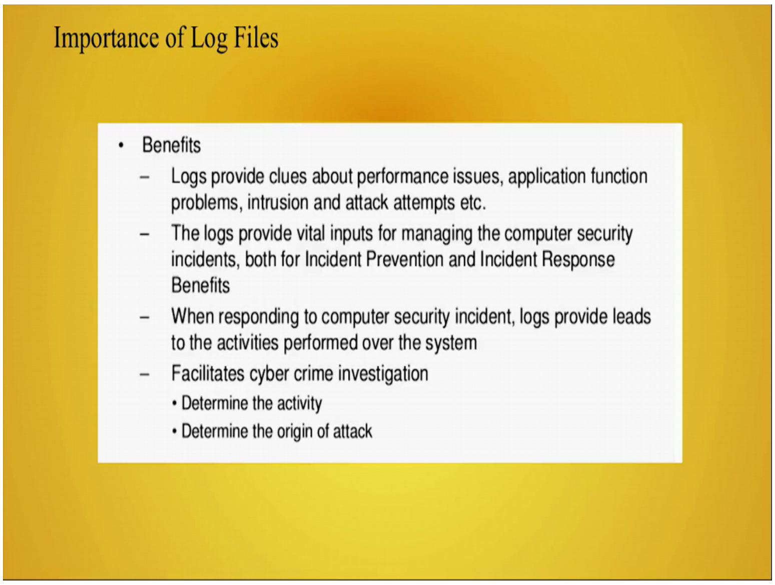
```
iptables -A INPUT -p tcp -m multiport --dport 80,443 -m
state --state NEW -m recent --update --seconds 100      -
hitcount 10 -j DROP
```

29

Here is the other example you can drop incoming packets with the IP address makes more than 10 connections to port 443 in 100 seconds. So, it is like there is heavy traffic how do I ensure that lot of people do not come in and then use my resources ok. So, here is an example of if you have more than10 connections within100 seconds; I can just drop the packets these are the ways in which you can use your firewall.

Before we conclude this session I would like to briefly explain to you about log management. Because all the time we have been looking at and relying on logs there are various logs that are available what is the importance of log ok.

(Refer Slide Time: 25:33)



Importance of Log Files

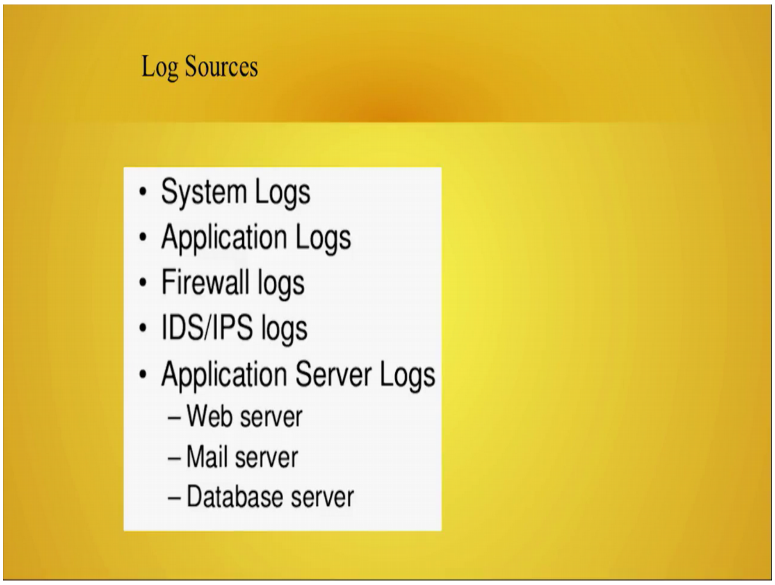
- Benefits
  - Logs provide clues about performance issues, application function problems, intrusion and attack attempts etc.
  - The logs provide vital inputs for managing the computer security incidents, both for Incident Prevention and Incident Response Benefits
  - When responding to computer security incident, logs provide leads to the activities performed over the system
  - Facilitates cyber crime investigation
    - Determine the activity
    - Determine the origin of attack

It provides performance issues, application function problems it identifies application function problems, intrusion detection prevent I mean attack atoms etcetera ok. And we are not going to get as you are seen we are not going to get one log I mean unless you use a master log server where everything gets locked to the particular server we are not proceeding that fashion. So, as a forensic investigator you have to get all the logs that are available and then combine them together and then to draw the event on the time lines ok.

So, essentially what is important is the time line. So, here the logs provide vital inputs for managing computer security incidents both for incident prevention and incident response benefits ok. And responding to computer security incident logs actually leads to the activities performed over the system we saw an example of it we also mention that you are supposed to use you can even buy commercial tools to look into this to make your life easier ok.

So, the logs actually facilitate cyber crime investigation it helps you to determine what activities happened and what are all the origins of attack etcetera.

(Refer Slide Time: 26:44)

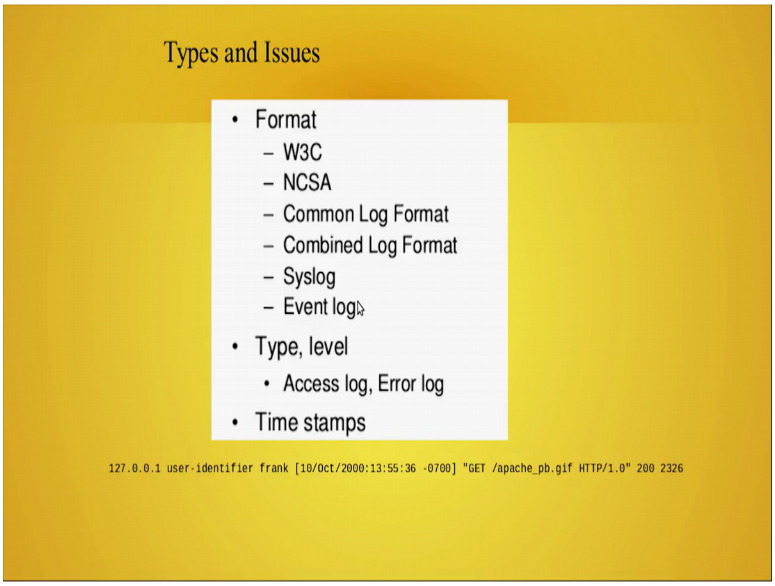


Log Sources

- System Logs
- Application Logs
- Firewall logs
- IDS/IPS logs
- Application Server Logs
  - Web server
  - Mail server
  - Database server

Here are the log sources that we had looked at we are looked at system logs I mean we will just briefly explain about system logs ah. Especially the syslog file of Linux or Unix then you can also have your application log we knew how to give logs for firewall then we saw some examples of firewall logs we saw some examples of Ids and IPs logs application log will include web server, mail server and database server.

(Refer Slide Time: 27:10)



Types and Issues

- Format
  - W3C
  - NCSA
  - Common Log Format
  - Combined Log Format
  - Syslog
  - Event logs
- Type, level
  - Access log, Error log
- Time stamps

```
127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

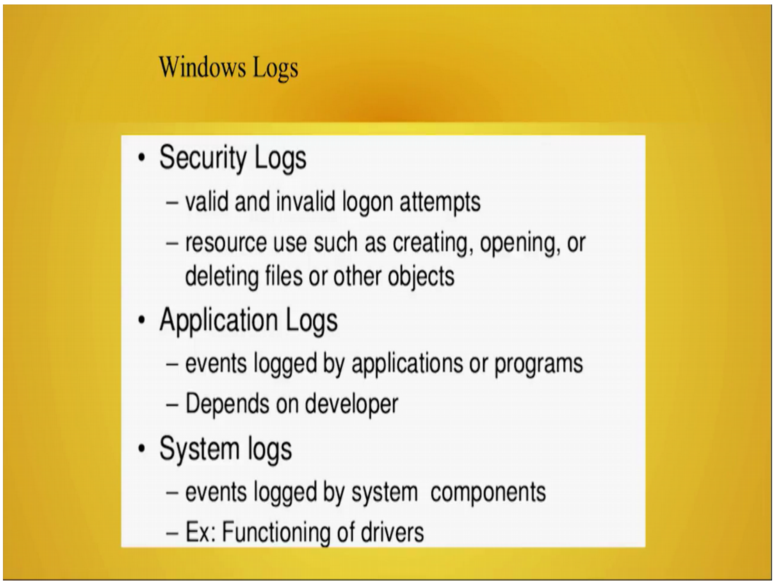
See there are various log formats usually the format will be like it will have a timestamp say for example, the following the given the one that we have shown here is an example of NCSA log which is provided by a web server kind of it is known as the common log format NCSA common log format.

It tells you the IP address and then the user identifier and who is the user and the then what time the user has try to do something, then it tells you the what is the request that you got what is the error message that was sent and what is the size of the packets that you received.

So and so, these kind of log will have structured format and many of the other things. So, that makes life easy for us to parse and for example, sed using commands like sed, and all those things if you remember we use that in your snort to comment out bunch of rules ok. So, , you could have these kind of the log formats could be in various formats.

So, you should make out use some kind of parser or which we have discussed I mean that is why we actually had a section on shell ok; you might have to use that kind of a parser to lock these, but most important thing is they will all have timestamps and they must be configured out timestamps.

(Refer Slide Time: 28:31)



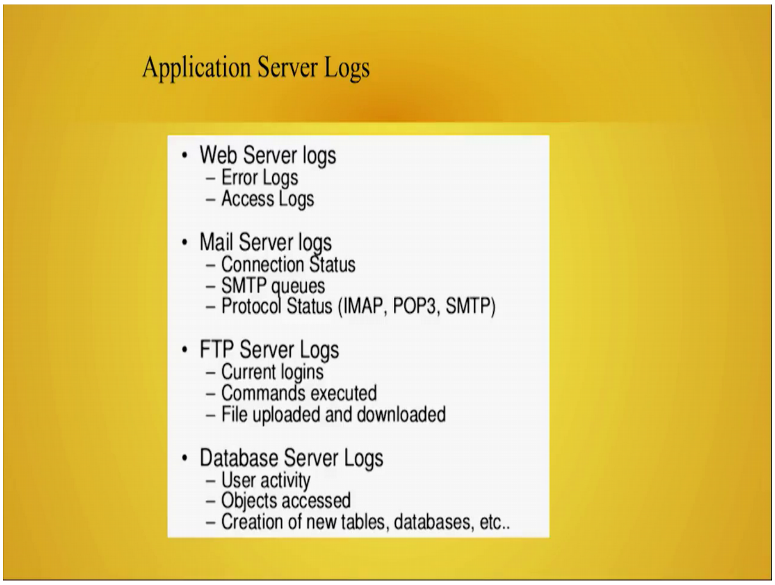
Windows Logs

- Security Logs
  - valid and invalid logon attempts
  - resource use such as creating, opening, or deleting files or other objects
- Application Logs
  - events logged by applications or programs
  - Depends on developer
- System logs
  - events logged by system components
  - Ex: Functioning of drivers

Windows OS might provide you security logs like valid and invalid login attempts ok; resource usage such as creating a file; opening a file; deleting a file and other objects. Then it could have a applications logs such as the events that are logged by applications ah.

But many of the application logs usually I mean they have some seven information levels and you can actually tune the application to dump what kind of information you want to have ok. Then there are this system logs whether the drivers are functioning whether your system has those drivers etcetera.

(Refer Slide Time: 29:09)

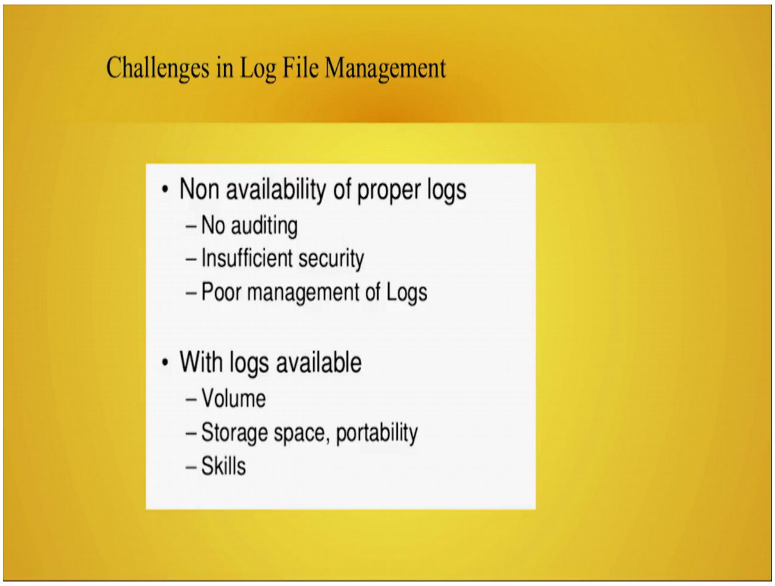


Application Server Logs

- Web Server logs
  - Error Logs
  - Access Logs
- Mail Server logs
  - Connection Status
  - SMTP queues
  - Protocol Status (IMAP, POP3, SMTP)
- FTP Server Logs
  - Current logins
  - Commands executed
  - File uploaded and downloaded
- Database Server Logs
  - User activity
  - Objects accessed
  - Creation of new tables, databases, etc..

With respect to application server logs you could have error logs and web server logs then mail server FTP server database server. So, all these logs have to be parse through. So, you should have some sort of a script which can pass through all the logs ok.

(Refer Slide Time: 29:38)



Challenges in Log File Management

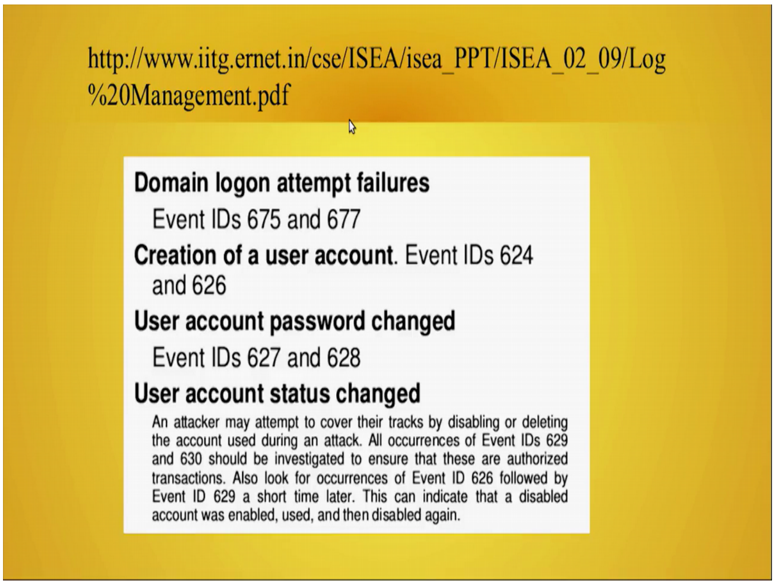
- Non availability of proper logs
  - No auditing
  - Insufficient security
  - Poor management of Logs
- With logs available
  - Volume
  - Storage space, portability
  - Skills

Use tools like grep, awk, sed and then get the required requested information that you need from these kind of logs ah. So, what are the challenges in this kind of log file management or network forensics? Sometimes you may not have proper logs available or the logs may not been audited or remember I mean if you have a read write access to all the logs; I mean then someone could have inserted the data. So, it may not be acceptable as a forensic evidence, if your log permissions is not ok.

So, that is something then there have been cases where you copied logs and while going to the court of law I mean the when you put it in front of the judge nothing works. So, poor this could be poor management law like you copy, but you do not test whether copy is or not. So, these are all simple thing which can costs something in terms of network forensics.

If, but in case the logs are available then you have other set of problems what is the volume of data you are supposed to carry ok. And how are you going to store it safely and I mean what if particular version of the OS is not available. For example, DoS file format take it there will be a control m at the end when you load it on Unix. So, there will be always be a control m that comes at the end of every lines that looks odd ok. So, for a technical person yes you can answer, but suppose let us say a person is not technical and this is a person who is making a judgment on whether the case are right or not.

When you sees the control m says this is something new; so, you have created it. So, this kind of stuff can happen.



http://www.iitg.ernet.in/cse/ISEA/isea_PPT/ISEA_02_09/Log%20Management.pdf

Domain logon attempt failures

Event IDs 675 and 677

Creation of a user account. Event IDs 624 and 626

User account password changed

Event IDs 627 and 628

User account status changed

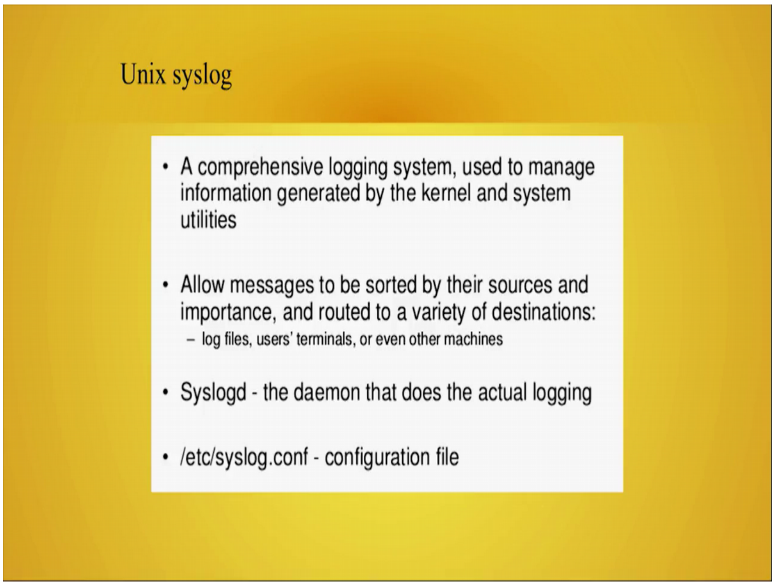
An attacker may attempt to cover their tracks by disabling or deleting the account used during an attack. All occurrences of Event IDs 629 and 630 should be investigated to ensure that these are authorized transactions. Also look for occurrences of Event ID 626 followed by Event ID 629 a short time later. This can indicate that a disabled account was enabled, used, and then disabled again.

Here are some examples of how event IDs could help to identify. So, here are things say let us say event ID 529, 530, 531, 32 so; that means, you are supposed to classify the logs and identify what has what is correct? What has gone wrong and things like it. So, it is better you prepare something like this ok.

So, these are all the local login attempt failures these are all misuse atoms these are all the logout attempts ok. And then you write a report on all these things I mean if you remember many of the security people they note down what vehicle is going on, what vehicle is coming back. So, this kind of log at the end of the day its better network security administrator keeps. So, that tomorrow in terms of any forensics this will help here is another example ok.

You can have a very detailed discussion of the slides that has given there it is one of the wonderful set of slides by sed dot in and they have given more on this log file management.

(Refer Slide Time: 32:09)



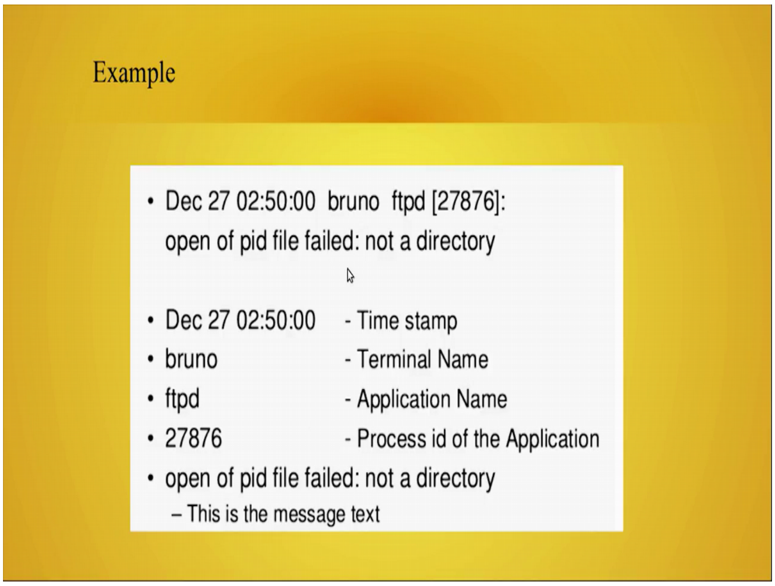
Unix syslog

- A comprehensive logging system, used to manage information generated by the kernel and system utilities
- Allow messages to be sorted by their sources and importance, and routed to a variety of destinations:
  - log files, users' terminals, or even other machines
- Syslogd - the daemon that does the actual logging
- /etc/syslog.conf - configuration file

Ah Most important thing is the Unix syslog a comprehensive logging system used to manage the information generated by the kernel and the system utilities ok. Even when I write an application I can I can take the syslog service and then I can merge myself into the syslog service it is a syslog is a daemons syslog d is daemon number that is running. I can attach my processor to a syslog daemon. So, whenever I want to give some messages the syslogs will take care of logging it in a proper format ok.

So, when you are developing application programming in Unix, try to use Unix syslog.

(Refer Slide Time: 32:43)

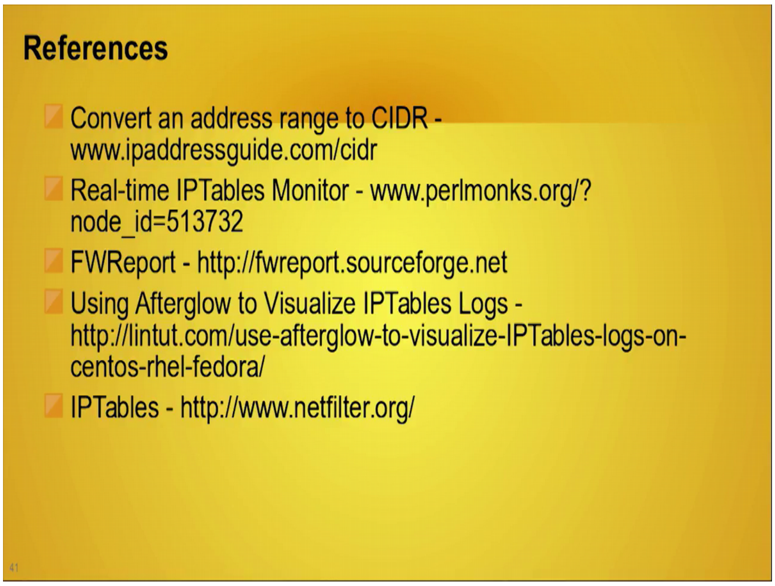


Example

- Dec 27 02:50:00 bruno ftpd [27876]: open of pid file failed: not a directory
- Dec 27 02:50:00 - Time stamp
- bruno - Terminal Name
- ftpd - Application Name
- 27876 - Process id of the Application
- open of pid file failed: not a directory
  - This is the message text

So, here is an example of a syslogs. So, it tells you that what timestamp at what terminal what is the application name that try to access and then why it failed etcetera it because it fail because it is not a directory.

(Refer Slide Time: 32:56)



References

- Convert an address range to CIDR - www.ipaddressguide.com/cidr
- Real-time IPTables Monitor - www.perlmonks.org/?node_id=513732
- FWReport - http://fwreport.sourceforge.net
- Using Afterglow to Visualize IPTables Logs - http://lintut.com/use-afterglow-to-visualize-IPTables-logs-on-centos-rhel-fedora/
- IPTables - http://www.netfilter.org/

41

So, here are some references for whatever sessions that you have done ah. If you look at this we are not endorsing everything, but these are something great to have ok. So, for IP tables for example, you can go to netfilter dot o r g to download the latest IP tables and have look at the manuals there ok. So, here is the real time IP table monitor, you can go to that particular website and then see what is there then source forge dot net has firewall report ah.

Essentially these things will make your life much more easier to work with I hope you enjoyed the this section on network security and forensics. So, as a concluding note ok; so, we will say there is lot to learn in this field not only should be the forensic person adapt in solving problem you should also understand how a network should be configured.

So, for example, why should as a forensic person learn about snort and IP tables ok. So, one yes when you go for forensics, you will know what data to collect and if if other person does not know you can teach them. Second you can when you submit the forensic audit report you can also say that an organization should have gone in for these kind of changes and that is very important.

So, unless you I mean that is a telling the organization how to prevent the attacks ok. So, and there unless you know the tools you will not be able to prepare such a report. So, if you want to prepare a comprehensive report on not only why the attack has happened, but also how to prevent it the knowledge of use of these kind of tools is very essential. And that is why we introduce the some of this tools during the course hope you enjoyed this section.

Thank you very much.