

MIS 5170

Operating System Security

Week 13

Unix/Linux Firewalls

Tonight's Plan

2

- ❑ Questions from Last Week
- ❑ Review on-line posts
- ❑ In The News
- ❑ Firewalls
- ❑ Sniffers
- ❑ Assignment 4 Review
- ❑ Next Week
- ❑ Quiz

Questions From Last Week

3

- ❑ Any Questions from last week?
- ❑ Review of quiz questions
 - ▣ How do you create a Unix/Linux script?
 - Remember you need to create it and use chmod to set the execution bit
 - ▣ SHA 1 has been cracked
 - Why is sha256
 - CRC is used for communication verification not mathematical summations
 - ▣ How do you get the members of a group
 - Right: getent group <Group Name>
 - Wrong: cat /etc/group

Questions From Last Week (cont)

4

- Any additional questions?

Review on-line posts

5

- Summary of the ITACS Panel Discussion:
 - ▣ Insurance: Wanted to talk a bit about this.
 - Help possible payment for DDOS Scrubbers or clean-up.
 - Info Sec groups.
- Digital Norms
 - ▣ I agree with Andres
 - We need to general add more than a single law
 - Star Trek comes to mind; federation of planets

Review on-line posts (Cont)

6

- Questions?

In the News

7

- ❑ Why I Always Tug on the ATM
 - ❑ Securing your Operating System and how this applies?
 - <https://krebsonsecurity.com/2017/03/why-i-always-tug-on-the-atm/>
- ❑ Critical Security Updates from Adobe, Microsoft
 - ❑ Remember Patch Tuesday
 - <https://krebsonsecurity.com/2017/04/critical-security-updates-from-adobe-microsoft/>
- ❑ Google Chrome to Distrust Symantec SSLs for Mis-issuing 30,000 EV Certificates
 - ❑ EV Cert Trust Wars (“my words”)
 - <http://thehackernews.com/2017/03/google-invalidate-symantec-certs.html>

In the News (Cont)

8

reddit PWNED hot new rising controversial top gilded wiki promoted

Interested in gaining a new perspective on things? Check out the r/askreddit subreddit! (reddit.com)
promoted by redditads
promoted

1 20 Ohio prison system hacked by inmates ... from inside their prison (theregister.co.uk)
submitted 5 hours ago by grrrreg
1 comment share

2 17 DTMF replay phreaked out the Dallas tornado sirens, say researchers (theregister.co.uk)
submitted 11 hours ago by wickedplayer494
1 comment share

3 13 Nintendo Will Reward You \$20,000 to Hack Their New Console (theissue.com)
submitted 11 hours ago by jimmyradola
5 comments share

4 20 Anti-LGTB spanish organization HazteOir pwned: interview with ACABgang (eldesarmador.org)
submitted 20 hours ago by kalikaneko
comment share

5 1 Is this thing possible in windows 10? Windows Session Hijacking (youtu.be)
submitted 10 hours ago by greenterminal
comment share

6 30 Healthcare data breaches are 'significantly underreported' as information sharing challenges persist (fiercehealthcare.com)
submitted 1 day ago by Pabla_bla
comment share

7 5 A ransomware attack at San Antonio-based ABCD Children's Pediatrics may have breached the data of 55,447 patients. (healthcareitne)
submitted 1 day ago by Taavi_avi
1 comment share

8 33 Identity thieves may have hacked files of up to 100,000 financial aid applicants - IRS tool used for FAFSA applications manipulated (washingtonpost.com)
submitted 4 days ago by misconfig_exe
1 comment share

9 69 Computer hack sets off 156 emergency sirens across Dallas (reuters.com)
submitted 4 days ago by ruskeeblue
9 comments share

10 20 Ransomware Attack on Texas Pediatric Provider Exposes Data of 55,000 Patients (medicalbuyer.co.in)
submitted 5 days ago by doni_coni
7 comments share

11 45 Gamestop.com Investigating Possible Breach (krebsonsecurity.com)
submitted 5 days ago by shaunc
comment share

In the News (Cont)

9

- Questions?

Firewalls

10

- ❑ What is a firewall?
- ❑ How do we configure it on Windows?

Firewalls (cont)

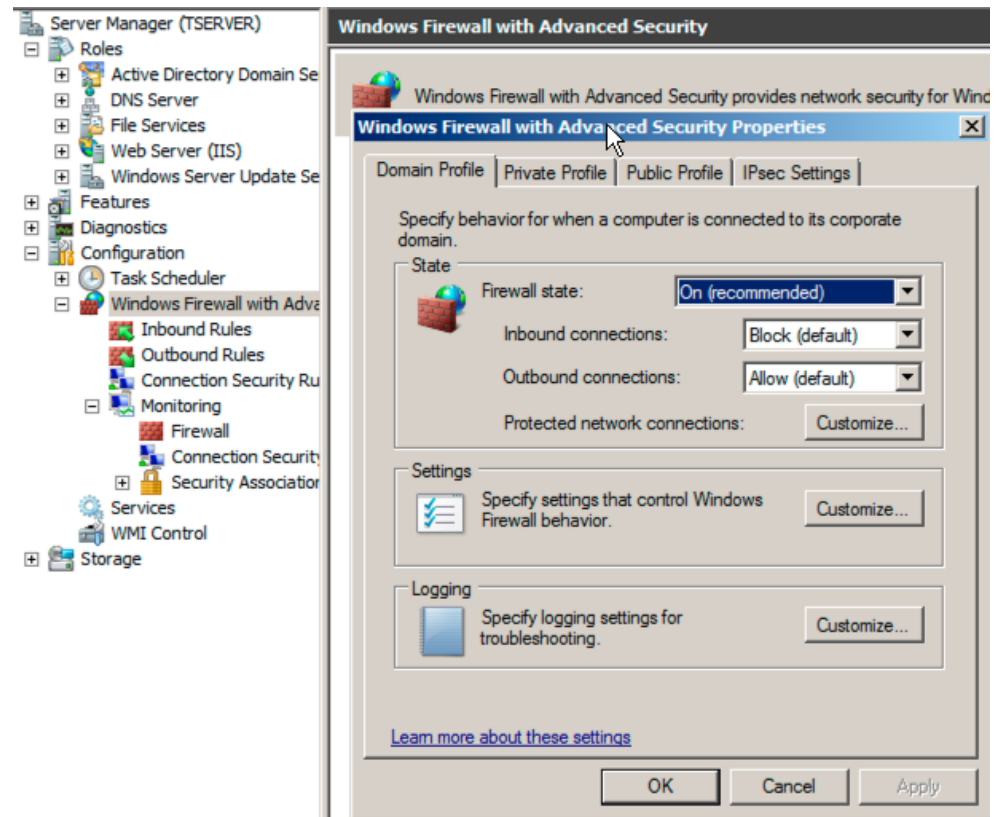
11

- ❑ What is a firewall?
 - ❑ A firewall network security system that monitors and controls the incoming and outgoing network traffic.

Firewalls (cont)

12

- How we configured logging on Windows
 - ▣ Turn on Logging:



Firewalls (cont)

13

- ❑ How do we configure it on Unix/Linux?
 - ❑ Turn on Logging:
 - iptables -N LOGGING
 - iptables -A INPUT -j LOGGING
 - iptables -A OUTPUT -j LOGGING
 - iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables-Dropped: " --log-level 4
 - iptables -A LOGGING -j DROP

Firewalls (cont)

14

- How do we configure it on Unix/Linux?

```
root@kali: /mnt/hgfs/Kali_Linked
File Edit View Search Terminal Help

Chain LOGGING (2 references)
num  pkts bytes target    prot opt in     out     source destination
1      0    0 LOG          all  --  *     *     0.0.0.0/0 0.0.0.0/0
burst 5 LOG flags 0 level 4 prefix "IPTables-Dropped: " limit: avg 2/min
root@kali:/mnt/hgfs/Kali_Linked# iptables -A LOGGING -j DROP
root@kali:/mnt/hgfs/Kali_Linked# iptables -L -n -v --line-number
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
1      3   585 LOGGING   all  --  *     *     0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
1      0    0 LOGGING   all  --  *     *     0.0.0.0/0 0.0.0.0/0

Chain LOGGING (2 references)
num  pkts bytes target    prot opt in     out     source destination
1      1   195 LOG          all  --  *     *     0.0.0.0/0 0.0.0.0/0
burst 5 LOG flags 0 level 4 prefix "IPTables-Dropped: " limit: avg 2/min
2      0    0 DROP      all  --  *     *     0.0.0.0/0 0.0.0.0/0
root@kali:/mnt/hgfs/Kali_Linked#
```

Firewalls (cont)

15

- ❑ You should now seeing anything that does not have an allow

```
root@kali: /var/log
File Edit View Search Terminal Help
Apr 13 15:12:09 kali kernel: [ 3473.011601] IPTables-Dropped: IN=eth0 OUT= MAC=f
f:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=172.16.69.1 DST=172.16.69.255 LEN=1
95 TOS=0x00 PREC=0x00 TTL=64 ID=37605 PROTO=UDP SPT=17500 DPT=17500 LEN=175
Apr 13 15:12:39 kali kernel: [ 3503.065226] IPTables-Dropped: IN=eth0 OUT= MAC=f
f:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=172.16.69.1 DST=172.16.69.255 LEN=1
95 TOS=0x00 PREC=0x00 TTL=64 ID=16303 PROTO=UDP SPT=17500 DPT=17500 LEN=175
Apr 13 15:13:04 kali kernel: [ 3527.967061] IPTables-Dropped: IN= OUT=lo SRC=127
.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=39163 DF PROTO=TCP SPT=
45350 DPT=631 WINDOW=43690 RES=0x00 SYN URGP=0
Apr 13 15:13:05 kali kernel: [ 3528.966584] IPTables-Dropped: IN= OUT=lo SRC=127
.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=39164 DF PROTO=TCP SPT=
45350 DPT=631 WINDOW=43690 RES=0x00 SYN URGP=0
Apr 13 15:13:07 kali kernel: [ 3530.970870] IPTables-Dropped: IN= OUT=lo SRC=127
.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=39165 DF PROTO=TCP SPT=
45350 DPT=631 WINDOW=43690 RES=0x00 SYN URGP=0
Apr 13 15:13:09 kali kernel: [ 3533.105114] IPTables-Dropped: IN=eth0 OUT= MAC=f
f:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=172.16.69.1 DST=172.16.69.255 LEN=1
95 TOS=0x00 PREC=0x00 TTL=64 ID=40006 PROTO=UDP SPT=17500 DPT=17500 LEN=175
Apr 13 15:13:11 kali kernel: [ 3534.975540] IPTables-Dropped: IN= OUT=lo SRC=127
.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=39166 DF PROTO=TCP SPT=
45350 DPT=631 WINDOW=43690 RES=0x00 SYN URGP=0
Apr 13 15:14:43 kali evolution-sourc[1050]: secret_service_search_sync: must spe
cify at least one attribute to match
```

Firewalls (cont)

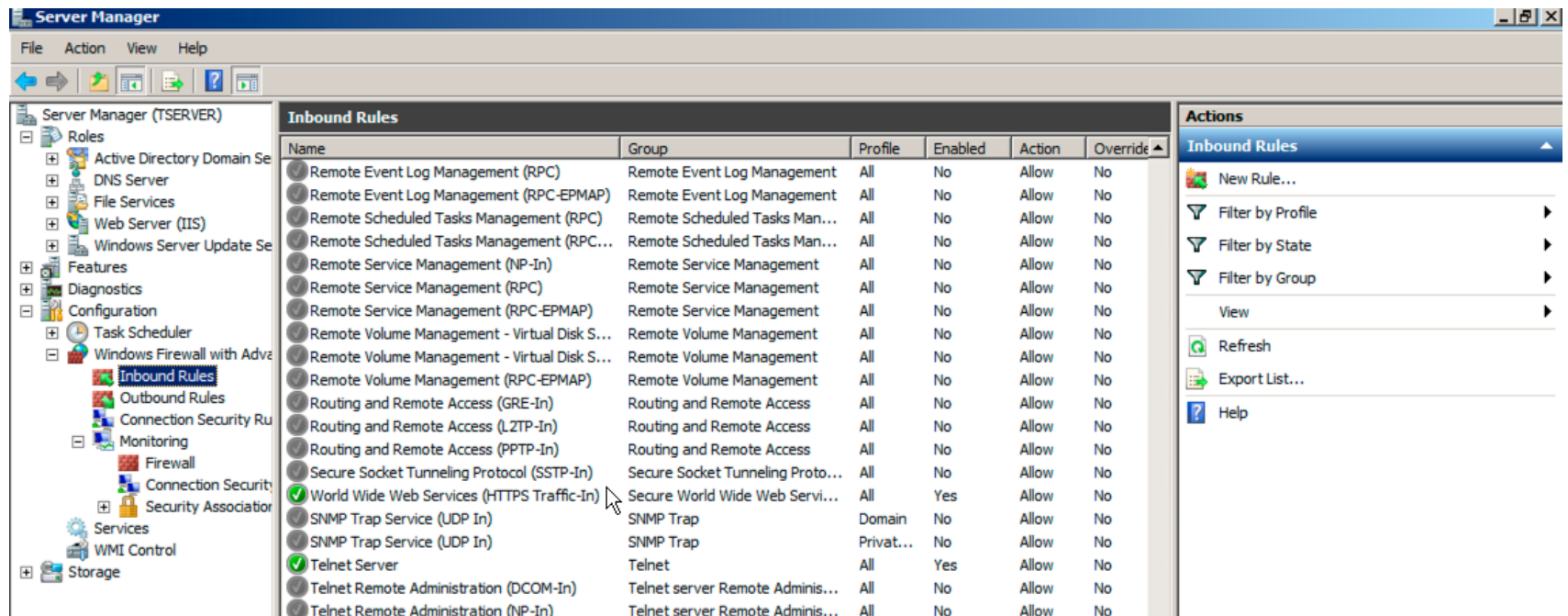
16

- Demo

Firewalls (cont)

17

- How we installed Telnet on Windows
 - ▣ Add the Telnet Client and Server under Features
- How we created a rule to allow Telnet on Windows



The screenshot shows the Windows Server Manager interface. The left-hand navigation pane is expanded to 'Firewall', and the 'Inbound Rules' folder is selected. The main pane displays a table of inbound rules. The 'Telnet Server' rule is highlighted with a green checkmark in the 'Enabled' column, indicating it is active. Other rules include Remote Event Log Management, Remote Service Management, and various Routing and Remote Access rules.

Name	Group	Profile	Enabled	Action	Override
Remote Event Log Management (RPC)	Remote Event Log Management	All	No	Allow	No
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Management	All	No	Allow	No
Remote Scheduled Tasks Management (RPC)	Remote Scheduled Tasks Man...	All	No	Allow	No
Remote Scheduled Tasks Management (RPC-EPMA...)	Remote Scheduled Tasks Man...	All	No	Allow	No
Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	No
Remote Service Management (RPC)	Remote Service Management	All	No	Allow	No
Remote Service Management (RPC-EPMAP)	Remote Service Management	All	No	Allow	No
Remote Volume Management - Virtual Disk S...	Remote Volume Management	All	No	Allow	No
Remote Volume Management - Virtual Disk S...	Remote Volume Management	All	No	Allow	No
Remote Volume Management (RPC-EPMAP)	Remote Volume Management	All	No	Allow	No
Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow	No
Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No
Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No
Secure Socket Tunneling Protocol (SSTP-In)	Secure Socket Tunneling Proto...	All	No	Allow	No
World Wide Web Services (HTTPS Traffic-In)	Secure World Wide Web Servi...	All	Yes	Allow	No
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow	No
SNMP Trap Service (UDP In)	SNMP Trap	Privat...	No	Allow	No
Telnet Server	Telnet	All	Yes	Allow	No
Telnet Remote Administration (DCOM-In)	Telnet server Remote Adminis...	All	No	Allow	No
Telnet Remote Administration (NP-In)	Telnet server Remote Adminis...	All	No	Allow	No

Firewalls (cont)

18

- ❑ Install Telnet on Kali
 - ❑ apt-get install telnetd

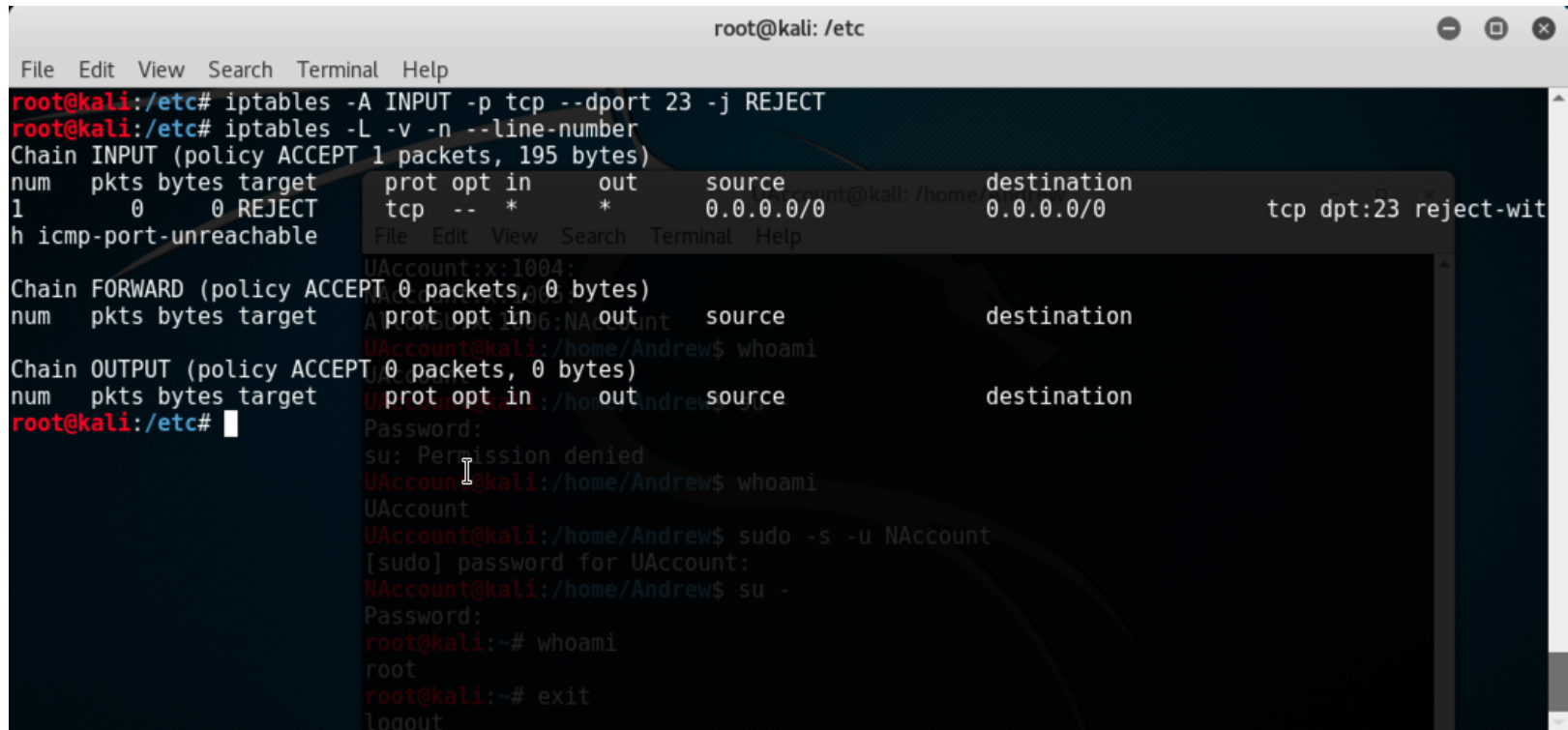
```
root@kali: /etc/pam.d
File Edit View Search Terminal Help
Use 'apt' or 'aptitude' for user-friendly package management.
root@kali:/etc/pam.d# dpkg -s telnet
dpkg-query: package 'telnet' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
root@kali:/etc/pam.d# apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  telnetd
0 upgraded, 1 newly installed, 0 to remove and 1907 not upgraded.
Need to get 44.6 kB of archives.
After this operation, 105 kB of additional disk space will be used.
Get:1 http://archive-8.kali.org/kali kali-rolling/main amd64 telnetd amd64 0.17-41 [44.6 kB]
Fetched 44.6 kB in 1s (38.8 kB/s)
Selecting previously unselected package telnetd.
(Reading database ... 303568 files and directories currently installed.)
Preparing to unpack .../telnetd_0.17-41_amd64.deb ...
Unpacking telnetd (0.17-41) ...
Setting up telnetd (0.17-41) ...
Adding user telnetd to group utmp
Processing triggers for man-db (2.7.5-1)
root@kali:/etc/pam.d#
```

Firewalls (cont)

19

- How to block Telnet on Kali

▣ **iptables -A INPUT -p tcp --dport 23 -j REJECT**



```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# iptables -A INPUT -p tcp --dport 23 -j REJECT
root@kali:/etc# iptables -L -v -n --line-number
Chain INPUT (policy ACCEPT 1 packets, 195 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1      0      0 REJECT    tcp  --  *      *      0.0.0.0/0            0.0.0.0/0            tcp dpt:23 reject-wit
h icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
root@kali:/etc#
```

UAccount:x:1004:
Account@kali:~\$ su -s -u NAccount
[sudo] password for UAccount:
NAccount@kali:~\$ su -
Password:
root@kali:~# whoami
root
root@kali:~# exit
logout

Firewalls (cont)

20

- ❑ Let's test our rule for telnet
 - ❑ **telnet 127.0.0.1 and see what happens?**

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# telnet 127.0.0.1
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
root@kali:/etc#
```

```
UAccount@kali: /
File Edit View Search Terminal Help
UAccount:x:1004:
NAccount:x:1005:
```

Firewalls (cont)

21

- How to block Telnet on Kali
 - ▣ **iptables -A INPUT -p tcp -dport 23 -j DROP**

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# iptables -A INPUT -p tcp --dport 23 -j REJECT
root@kali:/etc# iptables -L -v -n --line-number
Chain INPUT (policy ACCEPT 1 packets, 195 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1      0      0 REJECT    tcp  --  *      *      0.0.0.0/0            0.0.0.0/0            tcp dpt:23 reject-wit
h icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
root@kali:/etc#
```

```
UAccount:x:1004:
Account:1006:NAccount
UAccount@kali:/home/Andrew$ whoami
UAccount@kali:/home/Andrew$
Password:
su: Permission denied
UAccount@kali:/home/Andrew$ whoami
UAccount
UAccount@kali:/home/Andrew$ sudo -s -u NAccount
[sudo] password for UAccount:
NAccount@kali:/home/Andrew$ su -
Password:
root@kali:~# whoami
root
root@kali:~# exit
logout
```


Firewalls (cont)

22

- ❑ How do I remove a rule?
- ❑ `iptables -D INPUT 1`

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# iptables -L -v -n --line-number
Chain INPUT (policy ACCEPT 9 packets, 1541 bytes)
num  pkts bytes target    prot opt in     out     source            destination
1    2    120 REJECT    tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         tcp dpt:23 reject-wit
h icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 4 packets, 296 bytes)
num  pkts bytes target    prot opt in     out     source            destination
root@kali:/etc# iptables -D INPUT 1
root@kali:/etc# iptables -L -v -n --line-number
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination
root@kali:/etc#
```

Firewalls (cont)

23

- ❑ Install VMWare tools
 - ❑ <http://docs.kali.org/general-use/install-vmware-tools-kali-guest>
 - apt update
 - apt -y install open-vm-tools-desktop fuse
 - reboot
 - ❑ Link Folder to host
 - mkdir /mnt/hgfs
 - mkdir /mnt/hgfs/Kali_Linked
 - vmhgfs-fuse -o allow_other -o auto_unmount .host:/Kali_Linked /mnt/hgfs/Kali_Linked

Firewalls (cont)

24

- Demo

Firewalls (cont)

25

- ❑ Questions?

Sniffers

26

- Demo

Sniffers (cont)

27

- ❑ Questions?

Assignment 4 Review

28

- ❑ Shared VM's with the Wade's class
- ❑ Will get the results
- ❑ Will post the grades; may have a field trip or Saturday class to talk about the findings and/or corrections

Next Week

29

- ❑ Quiz will be based on this weeks Patching review and tonight's slides on Firewalls and Sniffers.
- ❑ Network controls
- ❑ Review for Test 2; All questions you want to ask
 - ❑ General Unix/Linux questions about what happened or what went wrong.

Quiz

30

- We can start the Quiz