

INTRO TO ETHICAL HACKING

MIS 5211.701
Week 2
Site:
<https://community.mis.temple.edu/mis5211sec701fall2020/>

1

1

Tonight's Plan

- Continue Intro
- Network Components and their impact on penetration testing
- Google Hacking
- Linux fundamentals (Will not cover in class, review if you need it)

2

2

Infrastructure Firewalls

- Firewalls may block or minimize the capabilities of penetration testing.
- Pen testing activity, especially scanning, can cause performance issues in firewalls
- HTTP Proxies may alter encoding
- Next Generation firewalls (Like PaloAlto) may perform analysis and drop packets that are not well formed.

MIS 5211.001 3

3

Host Firewalls

- ❑ Avoid using firewalls on your test network and attack machines
 - May block activity before it ever leaves your systems
- ❑ Since this exposes test machines to attack, use a separate, off-network machine to take notes.
- ❑ Utilize USB drives to transfer information

MIS 5211.001

4

4

Harden Test Machines

- ❑ Machines in you testing network should be baselined and locked down as much as possible
- ❑ Keep patching up to date
- ❑ Turn off all unnecessary ports and services
- ❑ Increase security settings where possible

- ❑ Center for Internet Security provides some guidelines
 - <http://www.cisecurity.org/>
- ❑ MicroSoft Baseline Security Analyzer also helps
 - <https://www.microsoft.com/en-us/download/details.aspx?id=19892>

MIS 5211.001

5

5

Protecting Test Results

- ❑ Consider encrypting test findings as they accumulate
- ❑ Example
 - OpenPGP
 - <https://www.openpgp.org>
 - Symantec PGP
 - <https://www.symantec.com/products/encryption>
 - BitLocker
 - <https://support.microsoft.com/en-us/search?query=bitlocker>
- ❑ Encryption technologies are changing, stay up to date on what works, and what has been broken

MIS 5211.001

6

6

Clean Test Machines Between Tests

- When an engagement ends
 - Move test results off of systems
- Scrub systems thoroughly
 - Secure Deletion
 - Reimage
 - Revert to baseline

Note: Consider using Solid State Drive w/ Trim turned on, faster and deleted data auto zero's

MIS 5211.001

7

7

Penetration Testing Process

- Preparation
 - NDAs if applicable
 - Client concerns
 - Rules of Engagement
 - Scope
 - **Written Permission and Acknowledgement of Testing Risks**
- Testing
 - Perform Test
- Conclusion
 - Analyze results and retest as needed
 - Develop report and presentation if needed

MIS 5211.001

8

8

Permissions

- Vital that written permission be obtained
 - Without this you could be held criminally responsible
 - Good intentions are no defense
- Ensure individual granting permission has the authority to do so
 - Corporate Officer
 - Director
 - P&L Responsibility

MIS 5211.001

9

9

Insurance & Limitation of Liability

- Permission alone is not sufficient
- If you are not working "In-House"
 - Contract language needs Limitation of Liability language
 - Time to call in the lawyers
 - You, or the company you work for will also need liability insurance

MIS 5211.001

10

10

Rules of Engagement

- At a minimum
 - Contact Information
 - Periodic Debriefing (Daily?)
 - Dates and Times for Testing
 - When to start
 - When to stop
 - Hours when testing is acceptable
 - Announced or Unannounced

MIS 5211.001

11

11

Shunning

- What if Sys Admins detect testing and attempt to block.
 - Is this good, or bad?
 - Stop test, or remove blocks and keep testing?
- Verify if client IDS, IPS, or WAF may block attacks
 - This may be OK if test was focused on effectiveness of these systems
 - However:
 - Could cause Denial of Service
 - Resource consumption
 - May need to get you traffic excluded from protections to test systems behind these controls

MIS 5211.001

12

12

Black Box vs Crystal Box

- Black Box:
 - No data provided to tester other than target IP Address or URL
 - Mimics malicious attackers vantage point
 - Time and resource consuming
- Crystal Box:
 - Tester provided detailed data on systems and architecture
 - Allows tester to quickly move to value added work
 - May not uncover data leaked into public space that would have been found during reconnaissance phase

MIS 5211.001

13

13

Data on Compromised Systems

- How far should test team go?
 - Configuration Data
 - User Info
 - PII
- Should likely stop at configuration data
- Testers do have a responsibility to not go past agreed to boundaries
- Also applies to sniffer data
 - Will explain this in detail later in the course

MIS 5211.001

14

14

Observed Tests

- Is a client representative going to observe all testing
 - Ensure client data is protected
 - Inform testers that some area may be off limits
- Is client staff going to work with testing team
 - Client may want their staff to become familiar with tools and methodology

MIS 5211.001

15

15

Completing Planning

- ❑ Establish agreement on handling issues prior to starting
- ❑ Document the agreement and get sign-off from all parties

- ❑ Congratulations - You now have your Rules of Engagement

MIS-5211.001

16

16

Scope

- ❑ Identify Client Security Concerns
 - Disclosure?
 - Availability?
 - Reputation?
 - Financial Loss?
 - Other?

- ❑ Only the client can tell you what they are really worried about

MIS-5211.001

17

17

Additional Scope Questions

- ❑ Identify known issues
 - Do you need to verify them?
- ❑ Identify likely threats
 - State Actors
 - Disgruntled Employees
- ❑ Determine what to focus on

MIS-5211.001

18

18

What to Test

- Determine clear and explicit scope
- What to test
 - Which systems?
 - Which address space?
 - Individual hosts?
- What to stay away from
 - Known "brittle" systems
 - Critical systems

MIS 5211.001

19

19

Third Parties

- If third parties are to be tested, they need to provide written permission
- If out of scope, need to know who and what they are to avoid them
 - This is a particular concern in web application testing as sites routinely link or have content hosted form third parties

MIS 5211.001

20

20

Production vs Test

- Test environments offer lower risk of impact
 - May not match production
 - May respond slower, impacting test efficiency
 - May not be possible, as only a production system exists

MIS 5211.001

21

21

How to Test

- How hard are you going to try
 - Ping Sweeps
 - Port Scanning
 - Vulnerability Scanning
 - Penetration into Target
 - Application Level Attacks
 - Client Side Attacks
 - Business Logic
 - Physical
 - Social Engineering
 - Denial of Service

MIS 5211.001

22

22

Internal or Near Internal Testing

- What about insider threats
- Possibilities
 - Official site visit and granted access
 - Onsite and breaks in
 - WiFi
 - Dial-In
 - VPN
 - Citrix
 - Teams
 - Public Kiosk

MIS 5211.001

23

23

Client Side

- Old process focused on servers and infrastructure
- More and more focus on client side testing
- Can I pivot through a compromised client browser (Think Target)
- Can I target vulnerable staff? Or does the client organizing want to provide a willing target to accept the attack (and avoid embarrassing employees)

MIS 5211.001

24

24

Social Engineering

- ❑ Very powerful
- ❑ Manipulating employees may impact morale, but also may serve an awareness function
- ❑ Client needs to think through and consider pros and cons

MIS 5211.001

25

25

Conducting a Social Engineering Test

- ❑ **Explicit written permissions**
- ❑ Defined goal, what are you after?
- ❑ Develop several scripts and get them vetted by client
- ❑ Select the right tester
 - People person
 - Someone others want to help
 - Sympathetic

MIS 5211.001

26

26

Denial of Service

- ❑ Dangerous to test
- ❑ Often not done because it is already known that systems can be knocked down
- ❑ If in scope, ensure specifically documented as "in scope"
- ❑ Consider carving out a subsystem to test so as not to take down entire client

MIS 5211.001

27

27

Dangerous Exploits

- ❑ Some tests are known to be dangerous
- ❑ Nessus has separate category of vulnerabilities it can scan for that are known to knock targets of line
- ❑ Some Metasploit attacks will either succeed or crash the target system
- ❑ Access testing can lock out users inadvertently

MIS-5211.001

28

28

Reporting Results

- ❑ Always create a report
 - It may be the only evidence you have there
 - Will likely be around a long time
 - Therefore, make sure it is clean, correct, and reflects well on the effort you put in
 - Report may make the difference between repeat engagement or no more engagements
- ❑ Even if "In-House" create the report
 - Brands your team and their effort

MIS-5211.001

29

29

Scan Results Are Not A Report

- ❑ Scanning reports may be included in an appendix, but they should not constitute the body of the report
- ❑ Description of findings, with impact and recommended mitigation go in the body of a report
- ❑ Don't accept scanning result ratings at face value.
 - May need to adjust based on other information developed during test

MIS-5211.001

30

30

Suggested Format

- ▣ Executive Summary
- ▣ Introduction
- ▣ Methodology
 - How did you do the testing
- ▣ Findings
 - Ranked by severity
- ▣ Recommendations
- ▣ Conclusion
 - Clients often want to know how they stack up against their vertical
- ▣ Appendices (if needed)

MIS 5211.001

31

31

Executive Summary

- ▣ Most important part of test
 - Management representatives may never read beyond the summary
- ▣ Keep it short
 - 1 page, 1.5 at most
- ▣ Briefly acknowledge test team and client employees who participated
- ▣ Summarize overall risk posture

MIS 5211.001

32

32

Executive Summary

- ▣ Include bulleted list of most significant findings
 - Three to six at most
 - Framed in terms of business impact
 - ▣ Why does the line of business care about the risks identified
 - Describe mitigation paths
 - ▣ People
 - ▣ Processes
 - ▣ Technology

MIS 5211.001

33

33

Screenshots and Illustrations

- ❑ Screenshots or illustrations help capture audience attention and make findings more “real”
- ❑ Only include “useful” screenshots
- ❑ Focus on important area, zoom in
- ❑ Use mask to exclude sensitive information
 - Passwords
 - User Names
 - Employee or Customer Data

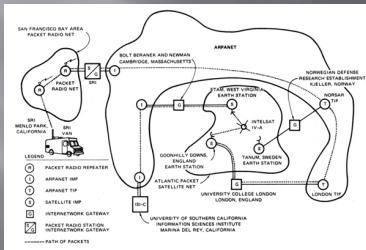
MIS 5211.001

34

34

Networking

- ❑ The very first internetworked connection:



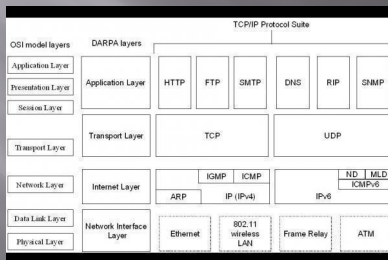
Source: http://en.wikipedia.org/wiki/Internet_protocol_suite

35

35

Internet Protocol Suite

- ❑ How Data fits together:



36

36

A word about Ports

- Ports – logical assignment to packets of data
- Used to distinguish between different services that run over transport protocols such as TCP and UDP
- IANA Registry:
<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1>

37

37

Protocols

- What we will cover
 - IP
 - ICMP
 - UDP
 - TCP
 - ARP

38

38

IP Protocol

- Internet Protocol
 - Primary protocol of the Internet Layer of the Internet protocol
 - Three main functions
 - For outgoing packets – Select the next hop host (Gateway)
 - For incoming packets – Capture the packet and pass up the protocol stack as appropriate
 - Error detection

39

39

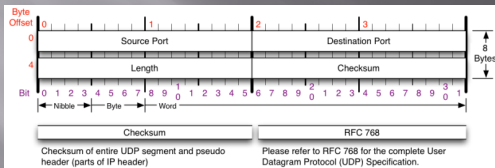
UDP Protocol

- User Datagram Protocol
 - Simple transmission model with limited mechanisms
 - No guarantee of delivery
 - No acknowledgement of receipt
 - Does include checksum and port numbers

43

43

UDP Protocol



Source: <http://nmap.org/book/tcpip-ref.html>

44

44

TCP Protocol

- Transmission Control Protocol
 - Sometimes called TCP/IP
 - Provides **reliable, ordered and error checked** delivery of a stream of data (or Octets) across local area networks, intranets, and public internet
- This is the protocol used for HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, Telnet, and others

45

45

Switches

- Used to connect devices together on a network
- Depending on functionality can operate at different layers of the OSI model
 - "Layer 1" - Hub - Traffic is not managed - Every packet repeated to every port
 - "Layer 2" - Data Link Layer - Some management - Switch knows MAC Address of locally connected devices and sends appropriate packets
 - "Layer 3" - Switch understands "routing" and knows what packets to pass out of the local segment

Microsoft Explanation of OSI Model :
<http://technet.microsoft.com/en-us/library/cc959881.aspx>

49

49

Routers

- Forwards packets between computer networks
- Works to keep localized traffic inside and only passes traffic intended for targets outside the local network
- Boundary between "Routable" and "Non-Routable" IP addressing

50

50

Non-Routable Addressing (Private)

- 10.0.0.0 to 10.255.255.255
 - Class A
 - 16,777,216 addresses
- 172.16.0.0 to 172.31.255.255
 - Class B
 - 1,048,576 addresses
- 192.168.0.0 to 192.168.255.255
 - Class C
 - 65,536 addresses

51

51

Firewalls (Standard)

- Standard Enterprise Firewalls are “2nd Generation”, implies stateful
- Filters traffic based on:
 - Address
 - Port
- Stateful: Retains enough data about previous packets to understand connection state

52

52

Firewalls (Next Generation)

- Extend operation into the Application layer
- Provides for Application layer filtering
 - Understands certain applications and protocols
 - Can determine if data inside a packet is consistent with the application or protocol

53

53

Firewalls (Web Application)

- Similar to Next Generation, but retains even more information around “normal” web site activity
- Builds a profile of how users interact with a website, and what the traffic should look like
- Generates alerts when patterns change
- Can generate false positives if web site undergoes high volumes of change

54

54

Network Address Translation (NAT)

- ▣ Modifies network addresses in the IP datagram
- ▣ Translation - Replaces the IP address in the packet with another address
 - Obscures addressing behind the NAT device, typically a firewall
 - Can convert non-routable addresses to routable addresses
 - Means the address you see is not necessarily the address of the target device

55

55

Load Balancers

- ▣ Distributes sessions across multiple server
 - User does not "Know" what server is in use
 - May terminate SSL connection for server, improving server performance
 - ▣ May apply additional SSL restrictions outside of certification rules
 - Internal tester can usually direct access to a particular machine or cell via alternate port

56

56

Google Hacking

- ▣ Search Bar Commands
 - -
 - Site:
 - Filetype:
 - Inurl:
 - Intitle:
 - Intext:
 - Allinurl:
 - Allintext:
 - Search Terms

MIS 5211.001

57

57

- Simple one that tells google to not include items that match what comes directly after "-"
- Example:
- Hacking -ethical - gives all results that include information about hacking as long as they do not include the term "ethical"

MIS 5211.001 58

58

Site:

- Site: restricts searches to a specific site
- Examples
 - Site:edu - Restricts searches to only sites ending in .edu
 - Site:temple.edu - Restricts searches to a specific top level site
 - Site:mis.temple.edu -Restricts searches to a sub-site

MIS 5211.001 59

59

Filetype:

- Restricts searches to a specific file type
- Examples
 - Filetype:pdf - Only responds with sites linked to Adobe documents with file extension of pdf
 - Filetype:xls - Only responds with sites linked to Microsoft spreadsheets documents with file extension of xls
 - Filetype:xlsx - Only responds with sites linked to Microsoft spreadsheets documents with file extension of xlsx - Excel's newer file format

MIS 5211.001 60

60

Inurl:

- Restricts searches to sites where specific word or phrase is in the url
- Examples
 - `inurl:"/root/etc/passwd"`
 - `inurl:admin`
 - `inurl:j2ee/examples/jsp`
 - `inurl:backup`

MIS-5211.001

61

61

Intitle:

- Restricts searches to sites where specific words are used in the title of a page
- Examples
 - `intitle:index.of`
 - `intitle:"Test Page for Apache"`
 - `intitle:"Apache Status"`
 - `intitle:"PHP Explorer"`

MIS-5211.001

62

62

Intext:

- Restricts results to documents containing term in the text
- Examples
 - `intext:"root:x:0:0:root:/root:/bin/bash"`
 - `intext:"SteamUserPassphrase="`
 - `intext:"SteamAppUser=" -"username" -"user"`
 - `intext:"Usage Statistics for"`

MIS-5211.001

63

63

Allinurl:

- Restricts results to those containing all the query terms you specify in the URL
- Examples
 - allinurl:/hide_my_wp=
 - allinurl:"/main/auth/profile.php"
 - allinurl:"owa/auth/logon.aspx"
 - allinurl:forcedownload.php?file=

MIS 5211.001

64

64

Allintext:

- Restricts results to those containing all the query terms you specify in the text of the page
- Examples:
 - allintext: /iissamples/default/
 - allintext: "Please login to continue..."
 - allintext:"Browse our directory of our members top sites or create your own for free!"
 - allintext:"fs-admin.php"

MIS 5211.001

65

65

Search Terms

- Key search terms
 - "index of /"
 - "Please re-enter your password it must match"

MIS 5211.001

66

66

Google Hacking References

- GoogleGuide
 - http://www.googleguide.com/advanced_operators_reference.html
- Exploit Database
 - <http://www.exploit-db.com/>
- Wikipedia
 - http://en.wikipedia.org/wiki/Google_hacking
- Google Hacking Volume 3
 - https://www.amazon.com/Google-Hacking-Penetration-Testers-Third/dp/0128029641/ref=dp_ob_title_bk

MIS 5211.001

67

67

Questions

- ?

68

68

Linux

- What is Linux
 - Open source operating system
 - Many similarities with UNIX
- Why do we care
 - Some tools only available in Linux
 - Some tools work better in Linux
 - Best open source attack suites are built on Linux
 - Kali
 - Samurai WTF (Web Testing Framework)
 - SIFT (SANS Investigative Forensic Toolkit)

69

69

Logging In

- ❑ For Kali the default password is **toor**
- ❑ For Samurai the default password is **samurai**

70

70

root

- ❑ "root" is the base admin account on a Linux system.
- ❑ Should not be used for routine operations

71

71

SUDO

- ❑ Used to execute commands that require root privilege
- ❑ Requires user to supply their password, not the root password

```

tester@ubuntu:~$ tree
The program 'tree' is currently not installed. You can install it by typing:
sudo apt-get install tree
tester@ubuntu:~$ sudo apt-get install tree
[sudo] password for tester:

```

72

72

Changing Passwords (passwd)

- "passwd" command is used to change passwords
- Any user can change their password by typing passwd at the command prompt.
- Will be prompted to enter new password twice
- "root" or sudo user can change others passwords with command:

```
passwd [login_name]
```

73

73

Changing Accounts

- "su" command allows you to jump to another user account (with appropriate password of course)
- "whoami" command tells you who you are logged in as

74

74

Linux File System

```

tester@ubuntu:/S tree -L 1
.
├── bin
├── boot
├── cdrom
├── dev
├── etc
├── home
├── initrd.img -> boot/initrd.img-3.13.0-24-generic
├── lib
├── lib64
├── lost+found
├── media
├── net
├── opt
├── proc
├── root
├── run
├── sbin
├── srv
├── sys
├── usr
├── var
└── vmlinuz -> boot/vmlinuz-3.13.0-24-generic
21 directories, 2 files
tester@ubuntu:/S █

```

75

75

Navigating File System

- ❑ Command cd [directory_name] changes directory
- ❑ Command cd.. Moves up one level
- ❑ Command pwd tells you were you are
- ❑ Command cd by itself takes you to your home directory

76

76

Viewing Directories

- ❑ Command ls lists directory content
- ❑ Flags
 - -l - details including permissions
 - -a - shows all files
- ❑ When in doubt use command "man ls", this gives you the manual or man page for the command

77

77

Output from ls -la

```

@ @ @ tester@ubuntu: /
tester@ubuntu:/ $ ls -la
total 304
drwxr-xr-x 23 root root 4096 Sep  2 18:50 .
drwxr-xr-x 23 root root 4096 Sep  2 18:50 ..
drwxr-xr-x 2 root root 4096 Sep  2 18:51 bin
drwxr-xr-x 3 root root 4096 Sep  2 18:53 boot
drwxr-xr-x 2 root root 4096 Sep  2 18:45 cdrom
drwxr-xr-x 15 root root 4200 Sep  2 18:52 dev
drwxr-xr-x 129 root root 12288 Sep  2 18:53 etc
drwxr-xr-x 3 root root 4096 Sep  2 18:46 home
lrwxrwxrwx 1 root root 33 Sep  2 18:50 initrd.img -> boot/initrd.img-3.13.0-24-generic
drwxr-xr-x 23 root root 4096 Sep  2 18:51 lib
drwxr-xr-x 2 root root 4096 Apr 16 18:21 lib64
drwxr-xr-x 2 root root 16384 Sep  2 18:40 lost+found
drwxr-xr-x 3 root root 4096 Apr 16 18:21 media
drwxr-xr-x 3 root root 4096 Sep  2 18:53 net
drwxr-xr-x 2 root root 4096 Sep  2 18:53 opt
dr-xr-xr-x 302 root root 0 Sep  2 18:52 proc
drwxr-xr-x 2 root root 4096 Apr 16 18:28 root
drwxr-xr-x 23 root root 820 Sep  2 19:01 run
drwxr-xr-x 2 root root 12288 Sep  2 18:53 sbin
drwxr-xr-x 2 root root 4096 Apr 16 18:21 srv
dr-xr-xr-x 13 root root 0 Sep  2 18:52 sys
drwxr-xr-x 10 root root 4096 Sep  2 19:02 tmp
drwxr-xr-x 10 root root 4096 Apr 16 18:21 usr
drwxr-xr-x 13 root root 4096 Apr 16 18:29 var
lrwxrwxrwx 1 root root 30 Sep  2 18:50 vmlinuz -> boot/vmlinuz-3.13.0-24-generic
tester@ubuntu:/$

```

78

78

Make and Remove Directories

- ❑ Command mkdir creates directory
- ❑ As before man mkdir gives you the manual
- ❑ Command rmdir removes directory

79

79

Make and Remove Directories

```

tester@ubuntu:~/tmp
tester@ubuntu:/$ pwd
/
tester@ubuntu:/$ cd /tmp
tester@ubuntu:~/tmp$ ls
ssh-GRAH9V72on  vmware-config0  vmware-root  vmware-tester
unity_support_test.0  vmware-root  vmware-root-3209747160
tester@ubuntu:~/tmp$ mkdir tester
tester@ubuntu:~/tmp$ ls
ssh-GRAH9V72on  unity_support_test.0  vmware-root-3209747160
tester          vmware-config0      vmware-root  vmware-tester
tester@ubuntu:~/tmp$ rmdir tester
tester@ubuntu:~/tmp$ ls
ssh-GRAH9V72on  vmware-config0  vmware-root  vmware-tester
unity_support_test.0  vmware-root-3209747160
tester@ubuntu:~/tmp$

```

80

80

Locate and Find

- ❑ Command locate checks an index on system to look for common items
- ❑ Command find searches file system
- ❑ On my test implementation, find required sudo privileges

81

81

Locate and Find

```

tester@ubuntu:/$ locate firefox | more
/etc/firefox
/etc/apparmor-d/usr.bin.firefox
/etc/apparmor-d/abstractions/ubuntu-browsers.d/firefox
/etc/apparmor-d/disable/usr.bin.firefox
/etc/apparmor-d/local/usr.bin.firefox
/etc/apparmor-d/blacklist.d/firefox
/etc/apparmor-native-origins.d/firefox
/etc/firefox/pref
/etc/firefox/pref.js
/etc/firefox/pref/apurl.js
/usr/bin/firefox
/usr/lib/firefox
/usr/lib/firefox-addons
/usr/lib/firefox/ffrunner-small_gif
/usr/lib/firefox/application.ini
/usr/lib/firefox/browser
/usr/lib/firefox/chrome.manifest
/usr/lib/firefox/components
/usr/lib/firefox/crashreporter
/usr/lib/firefox/crashreporter.ini
/usr/lib/firefox/defaults
/usr/lib/firefox/dependentLibs.list
/usr/lib/firefox/dictionaries
/usr/lib/firefox/distribution
/usr/lib/firefox/firefox
/usr/lib/firefox/firefox.sh
/usr/lib/firefox/hyphenation
/usr/lib/firefox/libfreebl3.chk
/usr/lib/firefox/libfreebl3.so
..More

```

```

tester@ubuntu:/$ sudo find / -name firefox
/etc/apparmor-native-origins.d/firefox
/etc/apparmor/blacklist.d/firefox
/etc/apparmor-d/abstractions/ubuntu-browsers.d/firefox
/etc/firefox
/usr/lib/firefox
/usr/lib/firefox/firefox
/usr/bin/firefox
/usr/share/doc/firefox
/usr/share/lintian/overrides/firefox
tester@ubuntu:/$

```

82

Editing Files

- ❑ Lots of choices, lets keep it simple
- ❑ Command gedit opens a text editor
- ❑ Command gedit test opens an existing file named test. If no such file exists, the file is created
- ❑ Edit as wish, save when done

83

Editing Files

```

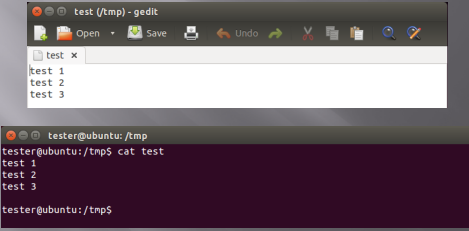
tester@ubuntu:/$ ls
tester@ubuntu:/tmp$ ls
ssh-GRAh9V72on vmware-config0 vmware-root vmware-tester
unity_support_test.0 vmware-root-3209747160
tester@ubuntu:/tmp$ gedit test
Testing
tester@ubuntu:/tmp$ cat test
Testing
tester@ubuntu:/tmp$ rm test
tester@ubuntu:/tmp$ ls
ssh-GRAh9V72on vmware-config0 vmware-root vmware-tester
unity_support_test.0 vmware-root-3209747160
tester@ubuntu:/tmp$

```

84

Viewing Files

- Command cat shows content of a file



85

85

Looking at Output

- Output often larger than screen
- Commands less and more
- Work similarly
 - less requires you hit q when done to return to command prompt
 - more dumps to command prompt when last screen is completed

86

86

Miscellaneous Commands

- Command ps shows running processes
 - Lots of switches to refine results
- Command CTRL-z interrupts running com
- Command bg restores interrupted command to run in background
- Command & tells job to run in background from the beginning
- Command jobs shows jobs running
- Command fg moves job to foreground

87

87

Network

- Command ifconfig shows network configuration. Similar to ipconfig in windows

```

tester@ubuntu:/$ ifconfig
tester@ubuntu:/$ ifconfig
eth0
Link encap:Ethernet  HWaddr 00:0c:29:28:06:5b
inet addr:192.168.233.133  Bcast:192.168.233.255  Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe28:65b/64  Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:2850 errors:0 dropped:0 overruns:0 frame:0
TX packets:1244 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3877660 (3.0 MB)  TX bytes:125222 (125.2 KB)

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:138 errors:0 dropped:0 overruns:0 frame:0
TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:12724 (12.7 KB)  TX bytes:12724 (12.7 KB)

tester@ubuntu:/$

```

88

Netstat

- Netstat prints information about the Linux networking subsystem. The type of information printed is controlled by the first argument, as follows:
 - (none) - By default, netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families will be printed.
 - --route, -r - Display the kernel routing tables. See the description in route(8) for details. netstat -r and route -e produce the same output.
 - --groups, -g - Display multicast group membership information for IPv4 and IPv6.
 - --interfaces, -I - Display a table of all network interfaces.
 - --masquerade, -M - Display a list of masqueraded connections.
 - --statistics, -s - Display summary statistics for each protocol.

89

Netstat

```

tester@ubuntu:/$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default 192.168.233.2 0.0.0.0 UG 0 0 0 eth0
192.168.233.0 * 255.255.255.0 U 0 0 0 eth0

tester@ubuntu:/$ netstat -g
IPv6/IPv4 Group Memberships
Interface RefCnt Group
-----
lo 1 all-systems.mcast.net
eth0 1 224.0.0.251
eth0 1 all-systems.mcast.net
lo 1 ip6-allnodes
lo 1 ff01::1
eth0 1 ff02::fb
eth0 1 ff02::1:ff28:65b
eth0 1 ip6-allnodes
eth0 1 ff01::1

tester@ubuntu:/$ netstat -I
Kernel interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1500 0 2884 0 0 0 1270 0 0 0 0 B
HWU
lo 65536 0 176 0 0 0 176 0 0 0 0 L
RU
tester@ubuntu:/$

```

90

grep

- grep searches the named input FILES for lines containing a match to the given PATTERN. By default, grep prints the matching

91

91

Grep w/ netstat and ps

- Try grep with netstat to see what is using http
netstat -nap | grep http
- Try grep with ps to see if cron is running
ps aux | grep cron

92

92

Grep w/ netstat and ps

```

tester@ubuntu: /
tester@ubuntu:/$ netstat -nap | grep http
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        28      0 192.168.233.133:49261  91.189.92.23:443    CLOSE_WAIT
9289/gvFsd-htp
tcp        28      0 192.168.233.133:58838  91.189.92.11:443   CLOSE_WAIT
9289/gvFsd-htp
9289/gvFsd-htp
nlc        28      0 192.168.233.133:58820  91.189.92.11:443   CLOSE_WAIT
9289/gvFsd-htp
tcp        28      0 192.168.233.133:49272  91.189.92.23:443   CLOSE_WAIT
9289/gvFsd-htp
tcp        28      0 192.168.233.133:34738  91.189.92.10:443   CLOSE_WAIT

tester@ubuntu: /
tester@ubuntu:/$ ps aux | grep cron
root      1016  0.0  0.0 23656  488 ?        Ss   18:52  0:00 cron
tester   11326  0.0  0.0 15944  924 pts/2    S+   21:31  0:00 grep --color=au
to cron
tester@ubuntu:/$

```

93

93

Going Further

- Get VMWare and a Linux ISO
 - Kali
 - <http://www.kali.org/downloads/>
 - Ubuntu
 - <http://www.ubuntu.com/download/desktop>
 - Samurai
 - <http://www.samurai-wtf.org>
- Give it a try
- All examples here where created in a clean, plain vanilla Ubuntu install

94
