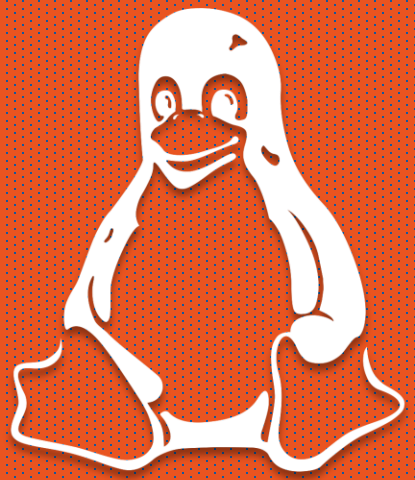
Basic Linux Security



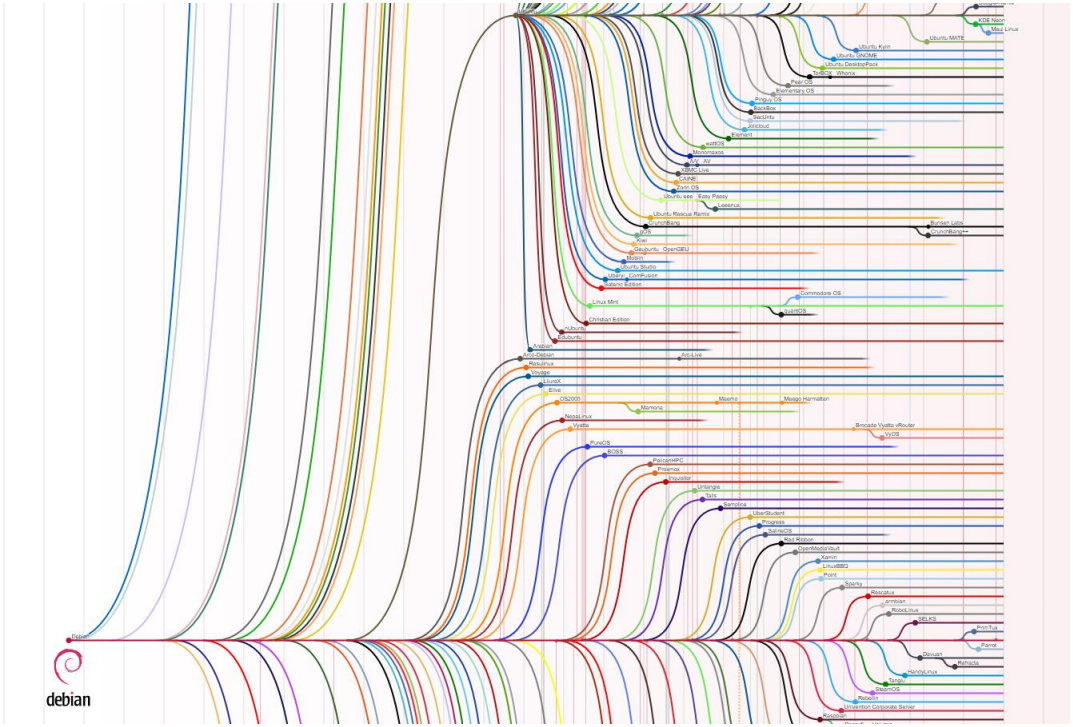
Roman Bohuk
University of Virginia

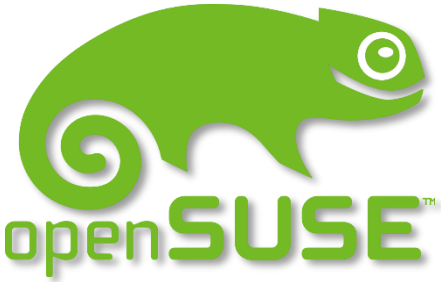
What is Linux?

- An open source operating system
- Project started by Linus Torvalds → kernel
  - Kernel: core program that controls everything else (controls processes, i/o between applications)
- Not to be confused with Unix – commercial OS
  - Unix-like / *nix – broad term encompassing both Unix and Linux

“Flavors”

- Timeline: https://tinyurl.com/LinuxDT





CentOS

debian

VM Setup

- Get the VM from a flashdrive or install your own version
- Login with `user:UV@cnsR0cks!`
- 2 ways to connect it to the internet and give SSH access. In the VM network settings, select
  - NAT
    - The machine “proxies” the traffic through your NIC
    - Add port 22 in the port forwarding settings, and SSH to localhost
  - Bridged Connection
    - The machine has its own IP on the LAN, and you can connect to it remotely
- If you want to set up a bridged connection, type `ifconfig` to find the MAC address, and add it at https://netreg.itc.virginia.edu/ (Register a device for network access)i

VM Setup

```
root@ubuntu-cns:~# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:05:3f:04
          inet addr:172.26.28.4  Bcast:172.26.31.255  Mask:255.255.248.0
          inet6 addr: fe80::a00:27ff:fe05:3f04/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1698 (1.6 KB)  TX bytes:2230 (2.2 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:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

root@ubuntu-cns:~#
```

What happens when Linux boots?

- BIOS looks for and executes a Master Boot Record (MBR)
- MBR loads GRUB, the Linux bootloader which loads and runs the kernel
- Kernel mounts the filesystem, executes the programs in /sbin/init
- The init file runs the Linux at a specific “runlevel”
- The runlevel-specific programs are executed from /etc/rc.d/rc*.d/
  - 0 – halt
  - 1 – single-user mode
  - 2 – multiuser mode (no networking)
  - 3 – full multiuser mode
  - 5 – GUI
  - 6 – reboot

Runlevels

- Practice:

```
who -r          # prints out the current runlevel
init *          # changes the runlevel to *
who -Ha         # lists the users who are logged in
```

Breaking Into Things

Why?

So you can defend it.

Cyber Kill Chain

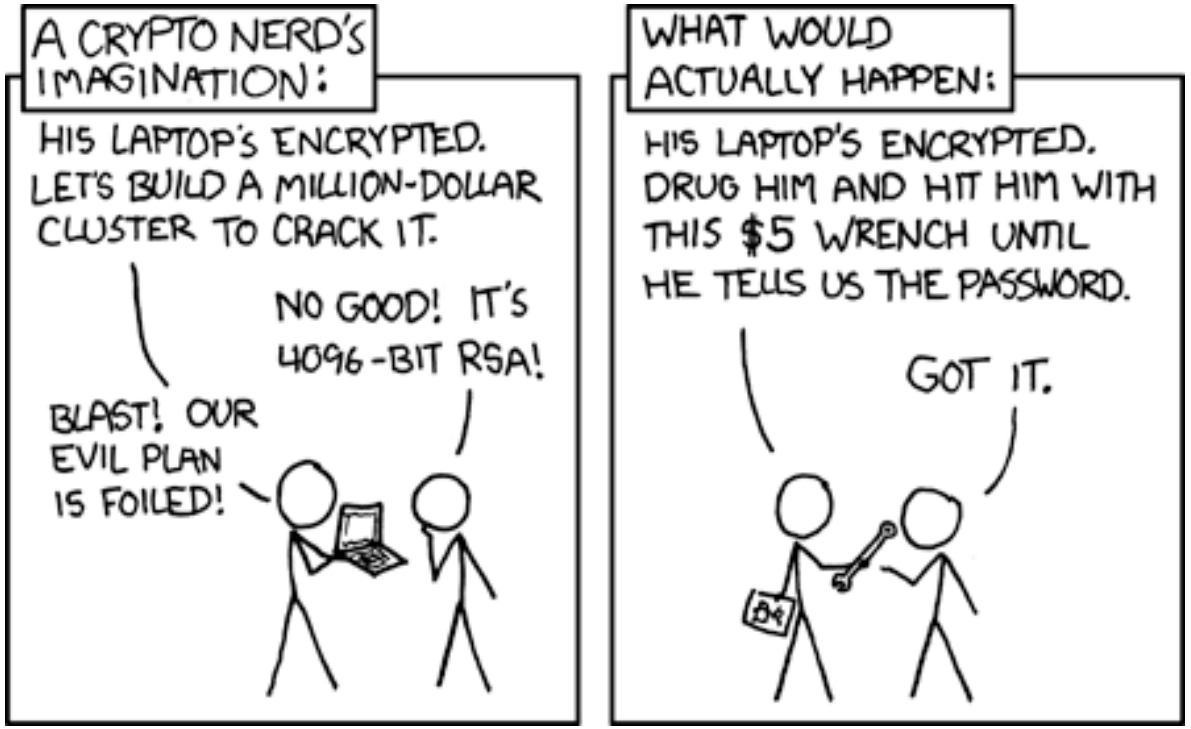
Locked up box

- No external services?
  - Comes down to whether or not there are any known vulnerabilities associated with the version of that system.
  - Read about the vulnerability and try to create a payload, or you can use a tool like metasploit to do the job for you.
  - Often works because it is hard to update something in a production environment (you can’t just pause the website until you update it)

External services?

- External services? (web server, ftp, ssh)
  - Same as the previous slide + extra attack surface
  - Look for vulnerabilities in each service
    - Identifying vulnerabilities comes down to experience and practice

Phishing?



XKCD #538

Linux Users

User information

- Can pull information from a remote database (LDAP)
- Usually, the user information is stored on the filesystem
  - General user info: /etc/passwd
  - Password hashes: /etc/shadow
  - Groups: /etc/group
- Every file and program has its own permissions and an owner

/etc/passwd

```
root@ubuntu-cns:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:,,,:/home/user:/bin/bash
```

/etc/shadow

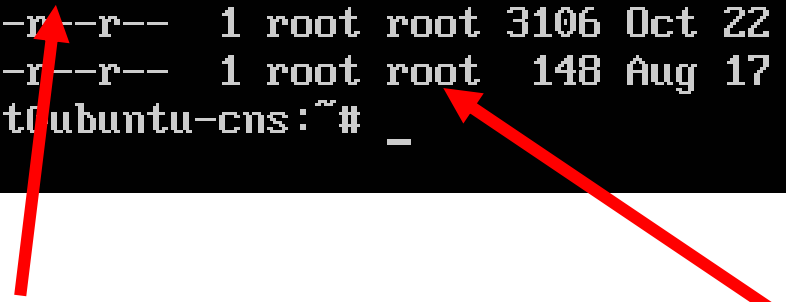
```
root@ubuntu-cns:~# cat /etc/shadow
root:$6$KA3Jq3z5$fw3B2oV/klrKKcSHdA/UoA/K9iEI44r5tRHTQ/4P.ZTk6JTTwtoqonAdNiTgNNaTVyUPNKhUTzp.TQL0wTM
nwl:17577:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
lxd:*:17577:0:99999:7:::
mysql:!:17577:0:99999:7:::
messagebus:*:17577:0:99999:7:::
uuidd:*:17577:0:99999:7:::
dnsmasq:*:17577:0:99999:7:::
sshd:*:17577:0:99999:7:::
user:$6$UisZQV.L$8Ems3qbxua6lN5YK1j2FDACJm/x.cwpvW4XaEm2NT6lbR84gaR4fQ536e4FBWLiGDW9d9YwlSkAcQzpozwM
wuu:17577:0:99999:7:::
root@ubuntu-cns:~#
```

/etc/group

```
root@ubuntu-cns:~# head /etc/group -n 30
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,user
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:user
floppy:x:25:
tape:x:26:
sudo:x:27:user
audio:x:29:
dip:x:30:user
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
```

Permissions

```
root@ubuntu-cns:~# ls -alt
total 28
-rw-------  1 root root   76 Feb 15 01:24 .bash_history
drwx------  4 root root 4096 Feb 15 01:24 .
drwx------  2 root root 4096 Feb 15 01:17 .cache
drwxr-xr-x  2 root root 4096 Feb 15 01:00 .nano
drwxr-xr-x 23 root root 4096 Feb 14 21:35 ..
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
root@ubuntu-cns:~# _
```



Permissions (read/write/exec)

user group world

Owner and Group

Permissions

- The goal of the attacker is to gain “sudo” permissions or become a “root.” This will allow him or her do anything on the system.
- Vulnerabilities can appear if permissions are not set properly
  - A program that has access to the shell runs as root
    - Ex: default settings for Jenkins server

Intermission

CTF Challenge

1. There is a site at http://10.164.31.92 that displays a random image of a cat or a dog upon request. Somewhere, there is also an image with a flag…

2. Also, can you get the hash of mark's password? (remember /etc/shadow)
   - The default directory for files on a web server is /var/www/html

3. Can you login as him?

Select Tricks

.bashrc

- .bashrc is a file that runs every time a user logs in
- Located in /home/user/.bashrc and /root/.bashrc
- Allows to execute a program as soon as the user logs in
- Fun:
  - Use the **alias** command as a joke

chattr +i

- Sets the immutable flag
- Even the root user can’t modify the file
- Remove lock using chattr –I

- Find all chattr’d files:
  - find /etc/ | xargs -I file lsattr -a file 2>/dev/null | grep '^....i'

cron

- Add a cron job to retain persistence
- Executed every few days, hours, or minutes
- Run a script to set configuration from a backup
- crontab –e to edit

SSH Keys

- A feature that allows users to be logged in without a password
- Stored in ~/.ssh/.authorized_keys
- Attackers can exploit it by adding extra keys
- SSH configuration can also be changed by adding a directive to the “AuthorizedKeysFile”

- Demo: creating a key and changing ssh settings

Systems users

- A lot of system users with no access to shell; check in /etc/passwd
- Attackers can give them sudo permissions and give access to shell
- If there is a global ssh key, no need to even set a password

- usermod -s /bin/bash username
- usermod -aG sudo username
- passwd username

Privilege escalation

- Once you have root access, no one can kick you out if you try hard enough
- Poor configuration can help gain privileges
- https://github.com/rebootuser/LinEnum

- There are special bits that let a program run as root even if it was called by a normal user
  - setuid and setgid permissions
- Attackers can exploit them if those programs leak access to shell

Changing time

- It can be especially easy to notice a suspicious file if

history

- Works both ways
- Attackers can see what the user did to secure the machine and try to kick them out
- Users can see what the attackers did and act accordingly

- nano and vim also store their own histories. Sometimes you can see exactly what was changed

- To clear, enter history –c and rm ~/.bash_history

Detection

Htop, tree

- Can see all processes
- The tree view allows to see what process is being run by what process

Lynis

- Can see all processes
- The tree view allows to see what process is being run by what process

Clamav

- Antivirus for Linux
- apt-get install clamav
- sudo freshclam

Backdoor your own system

- Add your own users and ssh keys
- Ls backdoor (devised by abiusx)
- https://tinyurl.com/lslog-ab

debsums -c

- Checks the filesystem to see if any configuration files have been modified

splunk

- More sophisticated event logger with analytics
- Combines logs from all services

Generic commands

- **who -Ha** lists authenticated users
- **nmap localhost** to check open ports
- **netstat -tulpnae** to check the network
- **ps aux** to check the running processes
- **last** shows the last login times for each user
- **cmatrix** because you can
- Try running privilege escalation tools against yourself