# CyberCamp 2019

Securing Linux

Ricky Payne CISSP, AWS CSA, RHCE, RHCSA, Security+ , BS-IST, AS-CET

About Me

- Over 13.5 years of progressive DevSecOps experience from Intern to Security Analyst -> Architect -> CSO -> Sr. Eng
- Built and operationalized vuln mgmt process for 1000s of globally distributed machines
- Built "Gold Standard" federal security programs that produced 10+ federally certified systems.
- Expert generalist: from pre-sales proposal work, policy and reference architecture development, requirements decomposition into agile sprints, proof of concepts, implementation, operations, and technical training to incident response.

- Mentored/taught Windows and Linux security at CyberPatriot/CyberCamps since 2013. Accomplishments include 1st and 2nd in State and 1st in Regionals.

- As a Sr. SecEng for a global, Silicon Valley InsureTech firm, engaged in all SecOps activities for 1000s of heterogeneous machines across multiple cloud technologies
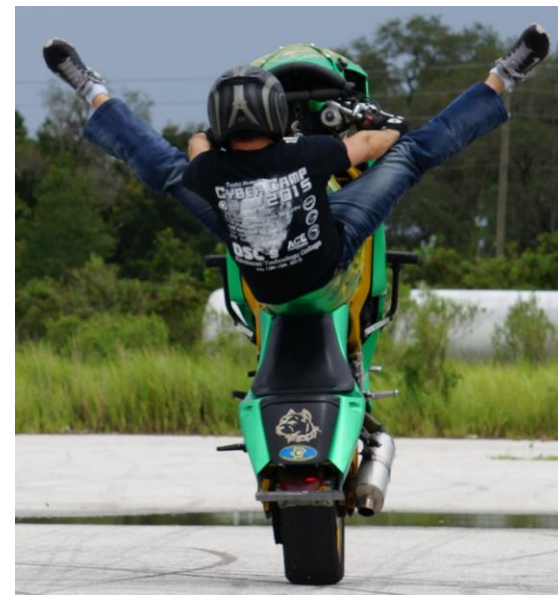
Ricky Payne
CISSP, AWS CSA, RHCE, RHCSA, Security+, BS-IST, AS-CET
grep.rickp@gmail.com
@RickPayne929

Agenda

- Linux 201 Overview
- Users, Groups, Passwords
- Package Mgmt, File Permissions
- Services / Daemons
- Port scans, Port monitoring
- Firewall
- Audit Logs: /var/log/messages,auth.log
- Security Guidance
- Your mission…

Linux 201

Linux 201

- This course is advanced and will be fast paced
- The course intent is to be practical with open discussions
- Please pay attention and keep up the best you can
- Let's begin!

Common Commands

Command	Description	Example
<cmd> --help	Command usage / syntax	**cat --help**
apropos <key word>	Query manual pages for <keyword>	**apropos password**
man <cmd>	Manual page for <cmd>	**man passwd**
sudo	Act as another user	**sudo cat /etc/passwd**
grep	search for a string in a file	**sudo cat /var/log/secure	grep failed**
vi	Launch vi	**vi /tmp/vitest**
find	Find a file in the FS	**sudo find / -type f -perm 0777**
cat	print a file to the screen	**cat /etc/passwd**
tail	Print the bottom of a file (-f to follow!)	**sudo tail –f /var/log/secure**

Users, Groups, Passwords

User, Groups, Passwords

- Setting the stage:
  - What users are on my system?
  - What users are in what groups? Admin? Sudo?
  - Is the root account locked?
  - Anything suspicious in the sudoers file?
  - Do all authorized users have a complex, strongly hashed, aging password?
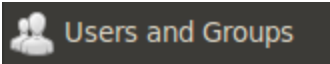
- Let's create a user, add him to a group, and check root account status and sudoers
- From the terminal(sudo as needed):
  - adduser yourname (use cybercamp for password)
  - adduser yourname sudo, usermod –a –G sudo yourname
  - addgroup testgroup
  - su yourname
- Verify from terminal with:
  - id yourname
  - groups yourname
- Root status, sudoers check:
  - Passwd –S root
  - less /etc/sudoers
- Create a badguy user and add him to the sudo group

- You can do the same via GUI

- From System -> Administration -> Users and Groups   Users and Groups

- Terminal: users-admin

Users, Groups, Passwords /etc/passwd /etc/shadow

- /etc/passwd entry

`ricknasty:x:1004:1005:rick,,,:/home/ricknasty:/bin/bash`

user password UID GID name home shell

- /etc/shadow entry

`ricknasty:$5$5I2W2GYo$tWmksAeTvoGyvrgQkSmTDZyHh8O3My9Jlpz6l7Smig9:16245:0:99999:7:::`

user   sha256 password hash   'Last pass change'   Min Max Warn

- chage –l yourname
- $1 = MD5, $6 = SHA512

- From the terminal(sudo as needed):
  - vi or gedit /etc/pam.d/common-password
    - Remove sha512, exit via :wq or save and close
  - passwd yourname
  - tail /etc/shadow
  - chage –l yourname
  - chage –M 60 –m 7 –W 7 yourname
  - tail /etc/shadow
  - vi or gedit /etc/pam.d/common-password
    - Add sha256, exit via :wq or save and close
  - passwd yourname
  - tail /etc/shadow

- From the terminal(sudo as needed):
  - sudo apt-get install libpam-cracklib
  - vi or gedit /etc/pam.d/common-password
    - password requisitie pam_cracklib.so line
      - dcredit=1 ucredit=1 lcredit=1 ocredit=1
    - password pam_unix.so line
      - remember=24

Package Mgmt, File Permissions

CyberCamp
2019

- Let's install a package and prepare to update From the terminal(sudo as needed):
  - apt-get install apt-file
  - apt-file update
  - apt-get update
  - apt-get upgrade (Press N! for now)
- Package Management via GUI:
  - System > Administration > Update Manager

Package Mgmt, File Permissions chmod, chown, chgrp

- Let's review our home folder's permissions, set cybercamp as the group for the Camp folder, and deny others access.

- From the terminal(sudo as needed):
  - ls -l /home/yourname
  - mkdir ~/Camp
  - chgrp cybercamp ~/Camp
  - chmod 770 ~/Camp

```
rick@cc-ubuntu1:~$ ls -l
total 40
drwxrwx--- 2 rick cybercamp 4096 2015-07-08 00:29 Camp
drwxr-xr-x 2 rick rick      4096 2015-07-08 00:16 Desktop
```

```
billy@cc-ubuntu1:/home/rick$ cd Camp/
bash: cd: Camp/: Permission denied
```

4 – Read
2 – Write
1 – Execute

Services / Daemons

CyberCamp
2019

Services / Daemons

- Let's disable/enable a service identified in our port probing
- From the terminal(sudo as needed):
  - Apt-get install ssh
  - service ssh status, stop, start, restart
  - apt-get install sysv-rc-conf chkconfig
  - sysv-rc-conf –list, or chkconfig --list
  - sysv-rc-conf ssh on, or chkconfig ssh on
  - sysv-rc-conf ssh –list, or chkconfig ssh –list
  - service ssh start
  - lsof –i :22
  - ps aux | grep ssh or PID

```
argus@cp-ub10-01:~$ sudo service ssh status
ssh start/running, process 3178
```

```
argus@cp-ub10-01:~$ chkconfig ssh --list
ssh              0:off  1:off  2:on   3:on   4:on   5:on   6:off
```
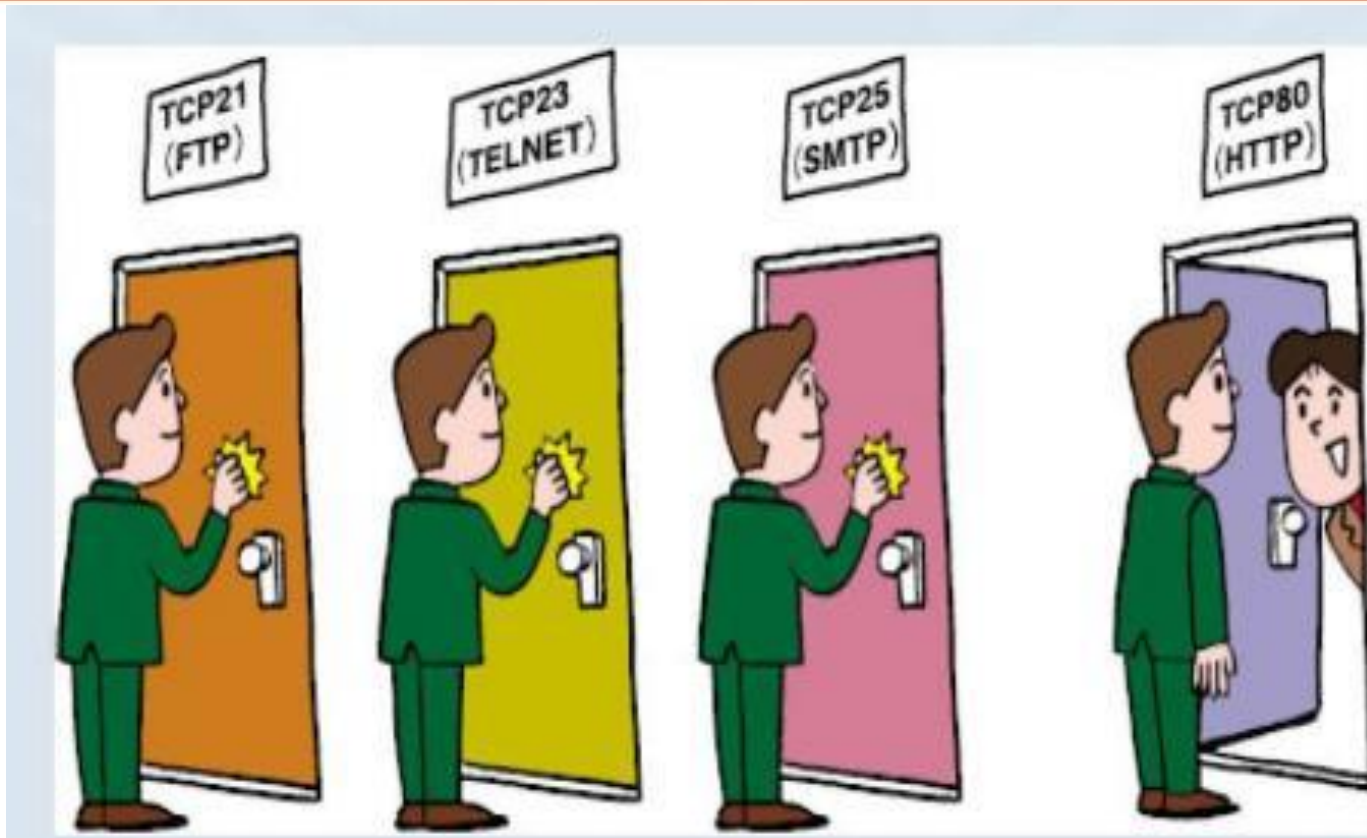
Port scan, Port monitoring

Port scan, Port monitoring

- Let's identify the system's open ports
- From the terminal(sudo as needed):
  - apt-file search /usr/bin/nmap
  - apt-get install nmap
  - Ifconfig
    - Note inet addr:
  - sudo nmap –p 1-1024 <inet addr noted above>
    - Note open ports
  - netstat –tuln
  - service ssh stop
  - Press up to rerun nmap and netstat again
    - What happened?
- Network tools GUI:
  - System > Administration > Network Tools
  - gnome-nettool

 Network Tools
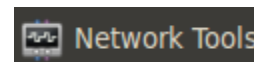
Firewall

Firewall

- Let's enable Ubuntu's uncomplicated firewall and add a network specific SSH exception
- From the terminal(sudo as needed):
  - apt-get install gufw
  - gufw
    - Click: Enabled
    - Add
    - Check: Show extended actions
    - Click: Advanced tab
    - 0, Allow, In, Log, TCP, From 192.168.128.0/24: 22, To blank: 22
    - Click: Add
  - ssh user@myIP
    - Success? Let's see what happened

Firewall

File Edit Help

Actual Status
☑ Enabled

Incoming: Deny ▼

Outgoing: Allow ▼

Rules

To	Action	From
22/tcp	ALLOW IN	192.168.128.0/24 22/tcp (log)

Audit Logs

Audit logs

- Let's investigate the logs to see what happened
- From the terminal(sudo as needed):
  - less /etc/rsyslog.conf
  - tail /var/log/auth.log

  ```
  Jun 24 14:57:37 cp-ub10-01 sshd[3659]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
  =0 tty=ssh ruser= rhost=cp-ub10-01.local  user=ricknasty
  Jun 24 14:57:39 cp-ub10-01 sshd[3659]: Failed password for ricknasty from 192.168.128.141 port 54112 ss
  h2
  ```

  - grep -i fail !$

  - tail /var/log/messages or tail /var/log/syslog
    - Any ideas?

  ```
  Jun 24 14:57:38 cp-ub10-01 kernel: [ 3051.185787] [UFW BLOCK] IN=eth1 OUT= MAC=00:0c:29:8e:8c:a8:00:0c:
  29:6f:2c:f3:08:00 SRC=192.168.128.134 DST=192.168.128.141 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=49756 DF
  PROTO=TCP SPT=58506 DPT=22 WINDOW=14600 RES=0x00 SYN URGP=0
  ```

  - gufw
    - Click add
    - Check: Show extended actions
    - Click: Advanced tab
    - 0, Allow, In, Log, TCP, From 192.168.128.0/24: **22**, To blank: 22
    - Click: Add
  - ssh user@myIP
    - Success?

Security Guidance

- DISA STIGs - http://iase.disa.mil/stigs/Pages/index.aspx
- CIS Benchmarks - https://benchmarks.cisecurity.org/

What we learned…

- Some common commands in the console
- Understanding users, groups and passwords
- Auditing and modifying file permissions
- Basic package management
- Starting and Stopping Daemons
- How to identify open network ports
- Understanding firewall configuration
- Using the audit logs
- Security Guidance

Your Mission…

Your mission....

- Delete the testgroup
- Remove badguy from the sudo group
- Lock the badguy account
- Install vsftpd
- Ensure the service is started
- Ensure the service persistently starts
- Identify which port was opened
- Add the port exception to the firewall
- Replicate the following perms → →
- Set the cybercamp's password to
  - expire in 60 days, 1 day minimum change and a 15 day warning
- Configure the system password hash to sha512
- Perform package upgrades

```
rick@cc-ubuntu1:~/Desktop$ ls -l
total 4
drw------- 2 rick cybercamp 4096 2015-07-08 01:08 Replicate
```

- Let's configure the file system ACL option, create mount.txt, set root as the owner and group, deny others access, but allow yourname to read via setacl permissions
- From the terminal(sudo as needed):
  - vi or gedit /etc/fstab
    - Add acl, option after ext4 and separate via ,comma,
    - reboot `UUID=3c9c9060-2e53-4979-bef9-2dd79310040b /          ext4     errors=remount-ro,acl 0          1`
  - mount > mount.txt
  - cat mount.txt | grep acl
  - ll mount.txt
  - chown root mount.txt
  - chgrp root mount.txt
  - chmod 600 mount.txt
  - getfacl mount.txt
  - setfacl –help
  - setfacl –m u:yourname:r mount.txt
  - getfacl mount.txt

```
sudo setfacl -m u:ricknasty:r mount.txt
argus@cp-ub10-01:~$ getfacl mount.txt
# file: mount.txt
# owner: root
# group: root
user::rw-
user:ricknasty:r--
group::---
mask::r--
other::---
```