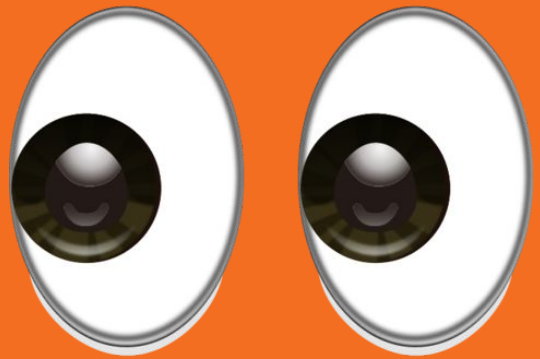
Welcome to RC3

RIT Competitive Cybersecurity Club

“Security Through Community”

Today’s meeting brought to you in part by…



Platinum

Gold

Educational Supporter

Why do we keep changing this up? We don’t know either

RC3 Sign-in Flag

Important dates & times

- The Incident Response Security Competition is **April 21st**
  - **White Team Signups:** https://tinyurl.com/irsec2018-whiteteam
  - Come volunteer and help us <3
- BSides Roc is **April 13-14th**
  - Buy tickets here: https://www.eventbrite.com/e/bsides-rochester-2018-tickets-43047674754
  - It's a great first conference.
    - 13th is Training day, 14th is the conference
  - If you cannot afford tickets to go, come talk to an RC3 E-board member
    - No one should be excluded from going to security events

Joining Eboard

Election nominations have now started: https://tinyurl.com/rc3-elections

Nominate someone you think would do a great job in the following positions:

Elected by current eboard

- President
- Vice President
- Competition Architect
- Tech Leads
- Web Admin
- Operations Lead

Elected by all attending members

- Treasurer
- Secretary

Disclaimer

The information contained in this presentation is for educational purposes **ONLY**! RC3 nor its members hold any responsibility for any misuse of the information provided in any slides, discussions, activities, or exercises.

…You have been warned.

Without further ado...

11. Intro to Blue Linux

#Cuccumber #RollYourOwn #NoBlueDistros #OpenBlueSD #fedora

Know your enemy

Think about the variety of persistence that we discussed last week

Backdoored Service Files	Web Shells	Backdoored Binaries
Malicious Cron Jobs	Bind Shells	Default Credentials
Aliased Commands	Reverse Shells	Rootkit?

Easiest Way to Defend

Think about the variety of persistence that we discussed last week

Backdoored Service Files Disable Unnecessary Services Harden Service Files	Web shells Audit Web Directory Harden PHP config?	Backdoored Binaries Reinstall Packages
Malicious Cron Jobs Stop and Disable Cron	Bind Shells Audit listening ports Firewalls (iptables)	Default Creds Change Passwords
Aliased Commands Unalias or prepend a \ Install and use a different shell	Reverse Shells Firewalls (iptables)	Rootkit? Disable unsigned modules Pray

Building Your 5 Minute Plan

1. Assess risks, with impact vs time to fix

i.e.

Default Creds → High impact, low time to fix

Reverse Shells → High impact, medium time to fix

Rootkit → High impact, high time to fix

Order your plan based on this criteria

Building Your 5 Minute Plan

2. Assess what defenses help you the most

i.e.

Killing a process stops one attack, but it doesn't fix the root issue

Setting up strict firewall rules stops Red Team implants from calling out

and stops Red Team from connecting to your system.

Example 5 minute plan overview

1. Change root password
2. Add a new admin user
3. Make a backup of critical services
4. Reinstall essential binaries
5. Backup database
6. Setup firewall rules
7. Audit your system
    a. processes, services, network connections, etc. Time to respond.

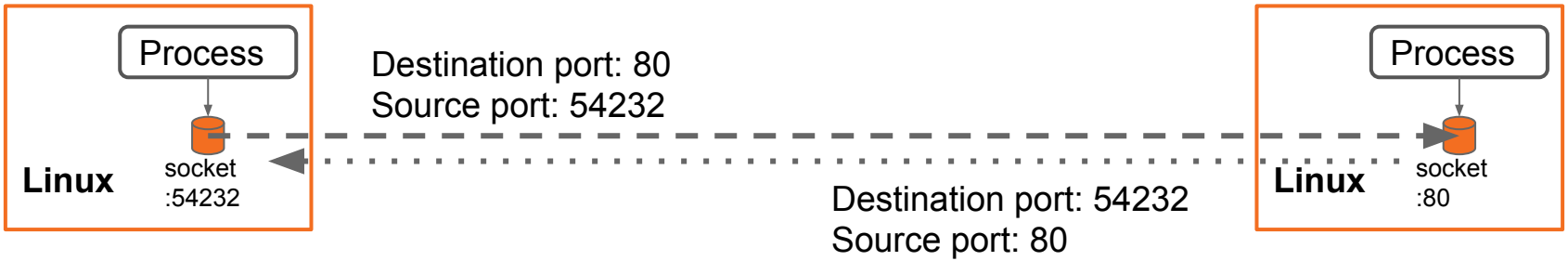
Brief Review

A socket is used to send or receive data on the network (or locally for IPC).

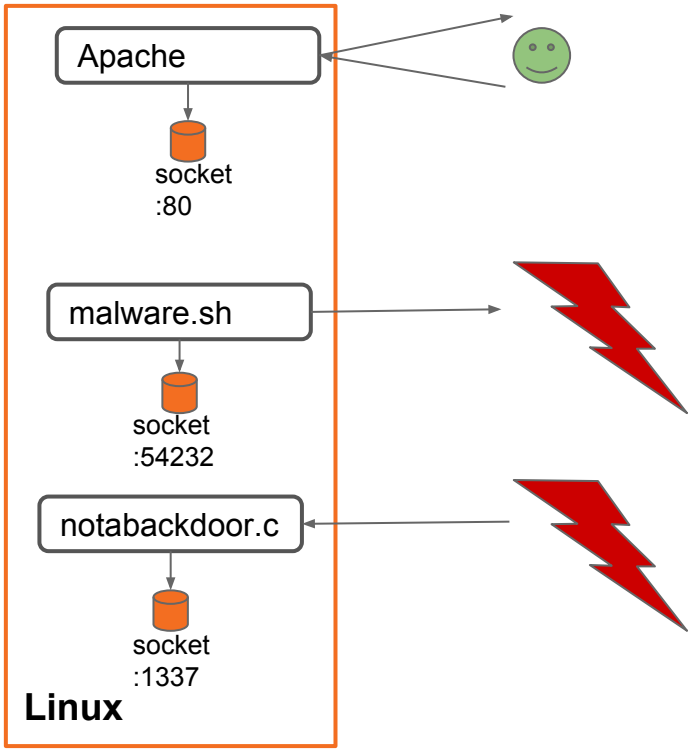
UDP and TCP operate based on port.

The Linux kernel restricts sockets, such that only one socket can be “bound” to a port at the one time.

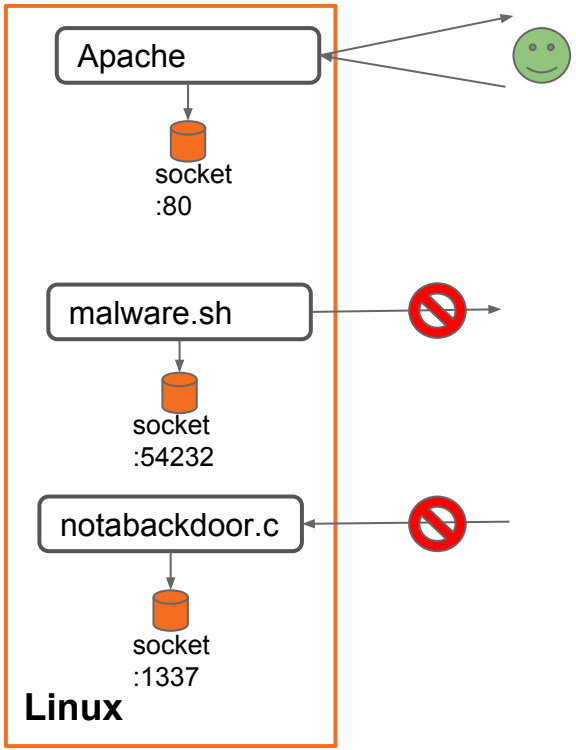
This means you can only have one process listen on port 80.



Competition Start



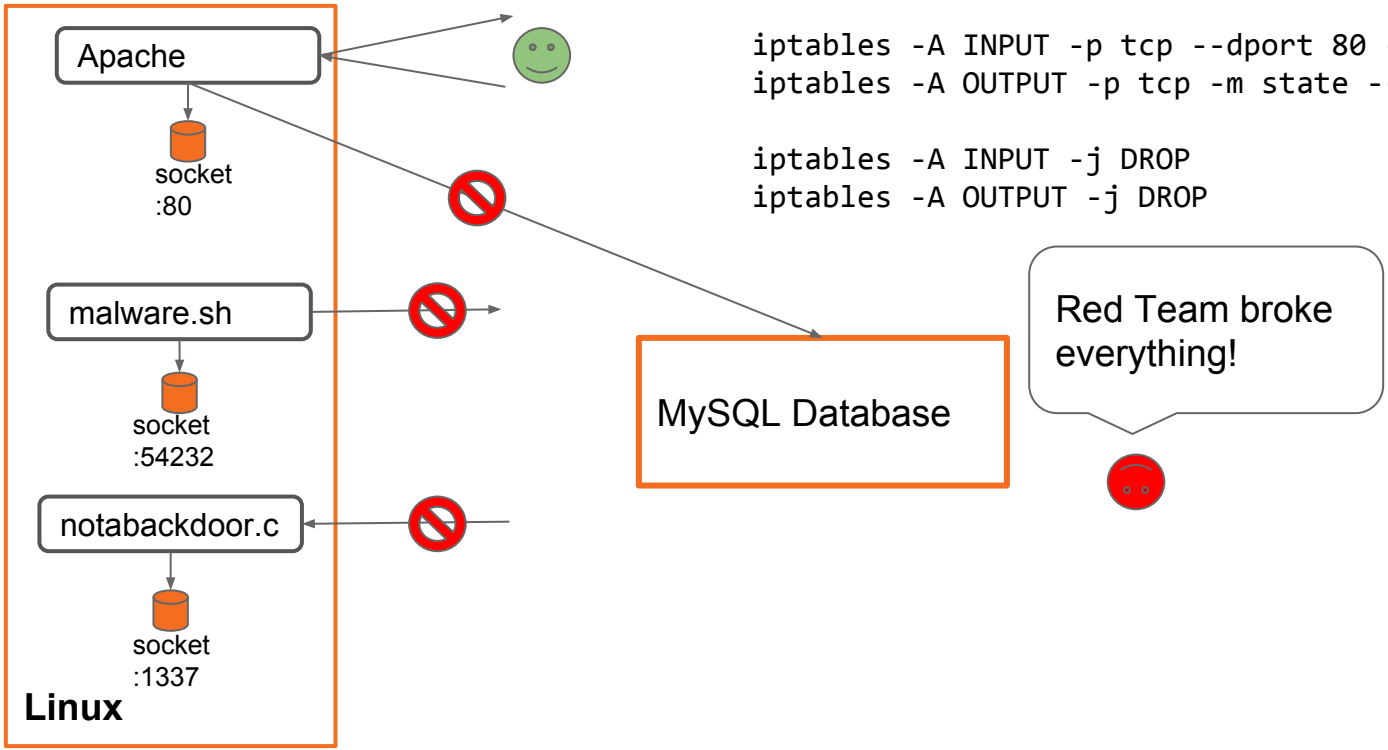
Limit Attack Surface




```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m state --state=ESTAB,REL -j ACCEPT

iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

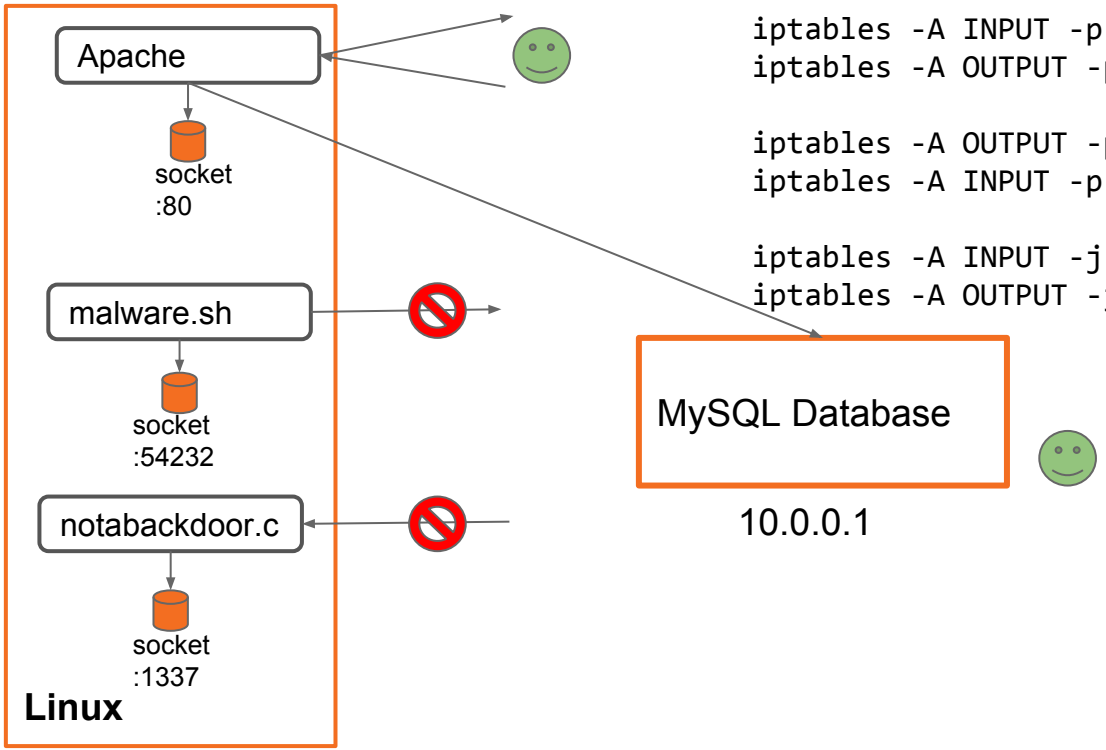
Don’t shoot yourself in the foot




```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m state --state=ESTAB,REL -j ACCEPT

iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

Don’t shoot yourself in the foot




```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m state --state=ESTAB,REL -j ACCEPT

iptables -A OUTPUT -p tcp --dport 3306 -d 10.0.0.1 -j ACCEPT
iptables -A INPUT -p tcp --sport 3306 -s 10.0.0.1 -j ACCEPT

iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

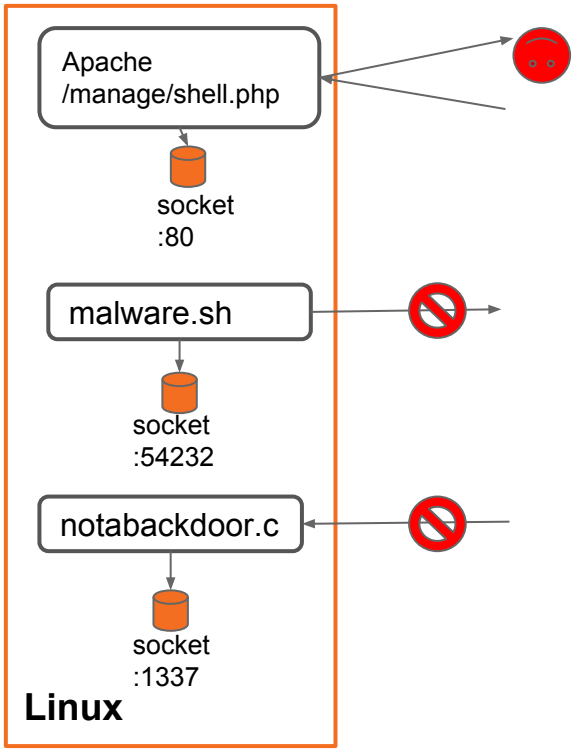
Not shooting yourself in the foot continued…

1. Change your password and forget it
   a. echo “root:$(head -c5 /dev/urandom)” | chpasswd
      (What was my password???)
2. Firewall yourself out of cloud boxes
   a. ./iptables.sh
      (system hanging)
3. Accidentally remove critical files
   a. rm -rf / bin/malware
      (goodbye system)
4. Kill critical processes
   a. killall -9 java

Not shooting yourself in the foot continued…

1. Change your password and forget it
   a. Come with a precomputed password sheet, write down which passwords are for what
2. Firewall yourself out of cloud boxes
   a. Add a “sleep 10 && iptables -F” to the end of your script, and test your connection
   b. Ensure that the default policy is to accept “iptables -P INPUT(/OUTPUT) ACCEPT”
3. Accidentally remove critical files
   a. Try to avoid **rm**, use **mv** instead
4. Kill critical processes
   a. Don’t kill anything unless you’re sure it shouldn’t be there, and you know what it does
   b. Do IR on malware before killing it, otherwise you’ll just lose points and we’ll be back!
5. Don’t rush. We’re already in. Take your time, think about what you’re doing.

Understand Your Risks



blueteam.com%2Fmanage%2Fshell.php%3Fcmd%3D%E2%80%99iptables%20-F%E2%80%99%0D%0A

curl blueteam.com/manage/shell.php?cmd='iptables -F'

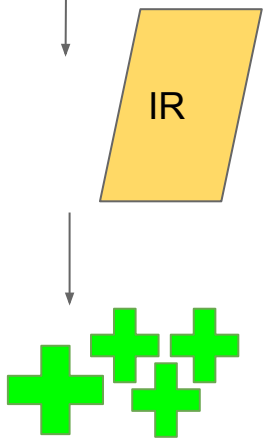
```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m state --state=ESTAB,REL -j ACCEPT

iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

Do Incident Response, Get Points Back

```
"GET /manage/shell.php?cmd=iptables -F HTTP/1.1"
```

/var/log/apache2/access.log



Fix the issue

```
# Save for Incident Response
mv /var/www/html/manage/shell.php /opt/incident_response/found_webshell
chmod 0000 /opt/incident_response/found_webshell

# Prevent it from easily coming back
touch /var/www/html/manage/shell.php && chattr +i /var/www/html/manage/shell.php

Disable shell_exec in php.conf
```

Setting up monitoring

- You can’t easily manage 4 boxes without automation
- Solution: Setup centralized monitoring and alerting
- Tools:
  - OSQuery
  - OSSEC
  - Splunk
  - Auditd
- Keep in mind, you won’t have much time. Set up what you can!

What to watch for

- Think of your attack surface
  - SSH logins?
  - IPTable logs?
  - File integrity?
  - Failed sudo attempts?
- Be careful about false positives
  - Being flooded with these will make your monitoring unuseable

Questions?

Demo info:

<info here>

Thank you

Feedback: https://rc3club.typeform.com/to/JdS2lV