How to win CCDC

A Red Team perspective

Intro

- Rob Fuller
  - Mid Atlantic CCDC Red Team since 2007
  - First year on Nationals Red Team
  - A Senior Red Teamer at my day job
  - Pentesting for a few years ;-)
  - Hak5
  - USMC
  - Father
  - <Incert acronym cert to make you trust me>

Tell 'em what you're gonna tell 'em

- Year(s) in review - what worked and didn't
- Practice and Preparation
- Know your team
- Know your role
- Know your space
- Know your network
- Know your defences
- Know your enemy
- Risk Prioritization
- Quick solutions to hard problems

Year(s) in review

What you do wrong...

- Get frustrated
- Don't ask enough questions
    - White cell is there to support you...
    - Injects are the only way you need to support them
- Focus too much on what is going wrong
- Patch everything
- Leave default passwords
    - Windows
    - SSH/Linux
    - Web Applications / Administration
    - Databases

Your complaints

Stolen from http://bit.ly/rmudge_derbycon

- How many -1 days did you use?
- If you have a head start that's unfair!
  - Real world attackers started attacking any Org that you get a job at before you got there.
  - You have the biggest advantage. You know we are coming. Don't expect to have this when you get to the 'real world'
- They used really advanced tools!
  - Nope, we found DEFAULT credentials

Practice and Preparation

The ugly red book that wont fit on a shelf

- Create a playbook
- Kill trees (have a copy for each member)
- Use Bit.ly instead of Googling for answers
- GITHUB... ;-) git clone all of your tools
- Password sheets _FOR EACH DAY_
- Cheat Sheets _FOR STUFF YOU NEED_
  - Looking through pages of references is just as bad as having to google it
- List of known and standard users per OS
- List of known and standard services per OS

Know your team

Roles & Chain of Command

- Team Captain
  - Gopher
    - Firewall Admin
    - Linux Admin
    - Windows Admin
    - Client Services
    - Incident Responder

Know your role

period

Team Captain Roles / Responsibilities

- Make sure everyone is where and when they need to be
- Coordinate responsibilities
- Constantly ask for feedback on tasks assigned
- Answer to the CEO and go to any and all meetings that are part of injects
- Focus team on objectives
- Stop any infighting
- Channel feedback from internal and external
- STAY OFF THE KEYBOARD

~~Secretary~~ Executive Assistant / Gopher

- Get/Download anything that is needed
- Get supplies / food stuffs
- Step in for Team Captain when not present
- Support all other roles as needed
- Deal with all paperwork based injects
- Inherits all physical security responsibilities
- Defend team against Nerf assaults

Firewall admin

- RAISE SHIELDS Mr Sulu!
- Monitor OUTBOUND connections
- Know your firewall and how to configure it
- Have or know exactly where to get any and all software you need to administer the firewall given to you.
- Egress and Ingress filtering
- IPv6 OFF
- deny any any is your friend
- Wireless gear is your baby, WPA2, WPS off (if possible), and long pass phrase
- Pass off Incident Reports to IR person
- CAPRICA (ACL generator) is _AWESOME_
    - http://code.google.com/p/capirca/

Linux Admin

- GRSEC _period_ because it's fun to watch Red Teamers attempt privilege escalation on older kernels.
    - Turn off the ability to change grsec settings via sysctl
    - Turn on EXEC logging
    - Watch the audit log for signs of escalation attempts
- If ($PHP) then shoot.self; (Fix php.ini)
- SETUID
- Watch those auth logs
- Create a process list file so IR can diff it
- Remove any unused users or services
- IPTSTATE is like TCPview for Linux, use it. love it. watch it.

Linux Admin (cont'd)

- File Integrity logging pays dividends:
  - Tripwire
  - OSSec (has pre-configurations for most *nix)
- Nothing new should enter here without you knowing:
  - /tmp/ (new files or binaries in here are bad news)
    - .hidden directory is a common place to put stuff
  - crontab for all users
  - ~/.ssh/ (and /root/ not just /home)
  - /etc/
  - /etc/passwd & /etc/shadow & /etc/sudoers
- Know all SetUID binaries and watch for new ones

Linux Commands

- Final all 'immutable' files
  - find . | xargs -I file lsattr -a file 2>/dev/null | grep '^....i'
  - 'chattr -i file' to change it back
  - Doing this on / takes a long time, point it where it counts: /etc/, ~/, /tmp/   etc.. etc..

Sorry Raph.. :-)

```
time find / | xargs -I file lsattr -a file 2>/dev/null | grep '^....i'
----i-------------- /etc/bob.txt
----i-------------- /etc/bob.txt

real    9m15.451s
user    0m51.505s
sys     6m38.862s
```

Just /etc =>   real   0m2.674s

Windows Admin

- Event Viewer is your friend
- Autoruns is your friend
- Process Explorer and TCP View are your friend
- OSSEC works for windows too
    - (agent only, must talk to a Linux server for reporting)
- Change passwords and fast!
- Remove unused users and services
- Turn your firewall on and REMOVE EXCEPTIONS
- Turn off Teredo

Mark Russinovich is your friend.

Windows Admin - Changing Passwords Fast

- Program one:
  - AutoIt (make a binary to do it faster)
- Download one:
  - http://bit.ly/bulkpasswordcontrol (AD only - not local)
  - Advantage: pseudo random passwords
- Built in one:
  - dsquery user ou=Users,dc=testlab,dc=net | dsmod user -pwd RedTeamSucks! -mustchpwd yes
  - GPO for local admin passwords

Windows Admin - GPO (Security)

Some specific Windows Group Policy to set

Security Options

- Network security: LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM
- Network security: Do not store LAN Manager hash value on next password change - Enabled
- Network access: Do not allow anonymous enumeration of SAM accounts and shares - Enabled
- Network access: Do not allow anonymous enumeration of SAM accounts - Enabled
- Network access: Allow anonymous SID/name translation - Enabled
- Accounts: Rename administrator account - Rename to something unique (but remember it)
- Interactive logon: Message text for users attempting to log on - sometimes an inject

Windows Admin - GPO (Audit)

Audit Policy

Learn to configure windows audit logs and understand the events.

- Audit process tracking - Successes
- Audit account management - Successes, Failures
- Audit logon events - Successes, Failures
- Audit account logon events - Successes, Failures

Windows Admin - GPO (Other)

User Rights Assignment

- Debug programs - Remove all groups/users
- Allow log on through Terminal Services - Leave blank to disallow login via TS even if it has been started.

Client Services

- Turn on text only email reading if email is in play
- Microsoft Security Essentials free for SMB and home users so White Cell should be ok with it and hands down the best AV (IMHO)
- They have firewalls too! (nudge nudge)
- On windows systems install PeerBlock, it's a very small software package that does IP blocking for windows and supports LARGE IP lists (like every IP but my subnet) and supports egress
- On Linux remove all remote access options. It's a client, it doesn't need SSHd

Incident Responder

- Windows
  - Autoruns and other Sysinternals from a known good source. Ask White Team for a USB if you aren't allowed to have one/bring one
  - List logged in users (qwinsta)
  - If notepad.exe is running you've been breached
- Linux/BSD/Nix
  - .bash_history
  - ~/.ssh/authorized_keys
  - lsof -nPi / netstat -ano
  - know where logs are
  - diff process list
  - fuser -k pts/2
- Get the incident response forms and learn how to fill them out. Big points! 5 dolla

Know your space

Physical space

- Go into blackout (everyone has a single role) every morning. Check everything from network cables to users, services, and passwords
- Baseline and inventory your gear every day
- Look for tape on mouses
- Schedule 20 minutes before the ending bell to police your space. Remove and secure all media (physical and digital)
- Tag (like in graphiti) all of your gear, think SPY movie (small piece of tape to know if someone opened the door)
- GSM bugs? Keyloggers? Wifi Access Points? Voice recorders? Stuff that Tom Cruise would use (minus the couch jumping)
- If the fire alarm goes off, ask the White Cell if it's real.

Verbal Space

- If you get injects via phone, call back just like you (sh/w)ould your bank. Start to recognize the voice, have the same person answer every time.
- Verify _any_ communication with alternative means. Challenge / Response

Know your network

Forget Snort/Splunk/Nagios/Cacti

- You do not have time to install and configure these, much less watch them. Don't.
- Event Viewer, /var/logs, .bash_history
- Create a network map a head of time. Know it, love it, feed it breakfast
- NetworkMiner makes it easy to watch for new IPs connecting to/from your system
- nmap has NSE scripts to check for vulnerabilities
- Nikto can catch easy web app stuff

Know your defences

What gets the most bang for the buck?

- A clear head
- Firewalls
- AV
- File Integrity Monitoring (FIM)
- Logs

||

||

||

V

- Patches (At least all of them we'll talk later)

Know your enemy

THE RED TEAM ARE NOT GODS

when someone asks you if you are a god, you say: YES!

Realm of Possible

- ARP spoofing only works on a broadcast range. Configure your router/firewall and you're fine, stop worrying about it.
- DNS poisoning is hard and takes time, the Red Team _probably_ won't do it. Don't waste your time on it
- They cannot launch missiles by whistling the 2600MHz tone into your VoIP Phone

ME Gorrilllla

- Red Team posturing is just that, ignore it
- Red Team isn't going to get in if you focus on the basics and keeping them out instead of getting them out

Know the Red Team tools

- Run Poison Ivy, know how to remove it
- Run Metasploit's attacks psexec, MS08_067, and MS09_050 and see what changes are made to the system
- Run Metasploit's persistence script, know how to get rid of it
- AUTORUNS is your friend

Risk prioritization

You patch too much...

- Patch what is exploitable. This will save on download time, install time, and maximizes impact. Assume certain vulnerabilities.
- If XP/2k3 then PATCH MS08_067
- If Vista/7/2k8 then PATCH MS09_050
- If Linux/BSD don't patch, secure the kernel

NO ONE IS GOING TO DROP 0DAY AT CCDC

NO ONE IS GOING TO DROP 0DAY AT CCDC

NO ONE IS GOING TO DROP 0DAY AT CCDC

NO ONE IS GOING TO DROP 0DAY AT CCDC

Quick solutions to the right problems is the way to win.

Learn from mistakes, don't sweat them

Questions?

Rob Fuller
- mubix@hak5.org
- @mubix on twitter
- http://www.room362.com/
- https://www.deepmagic.com/
- http://www.practicalexploitation.com/

Special thanks to Devon, Joseph, Marco, Aaron, Raymond, and Brian for the 1 AM jam session to get these slides together. Go social media.

Alex Herrick for GPOs and other suggestions

Craig Balding for the beautiful 'iptstate' command