Defending Beyond Defense

Dr. Catherine J. Ullman
Principal Technology Architect, Security
University at Buffalo
@Investigatorchi

Agenda

- Introduction
- Background/History
- Defender Assumptions
- Immersion in Offensive Security
- Summary

Introduction

@investigatorchi

Dr. Catherine J. Ullman

- Principle Technology Architect, Security - University at Buffalo
- Staff: BSidesROC, UB GenCyberCamp, PHV/DEFCON, BSidesLV
- Volunteer: CPTC, Skytalks, CCDC, BlueTeamCon
- Speaker: Wall of Sheep, BTV, GrrCON, Diana Initiative, BlueTeamCon, Cyphercon, BSides Buffalo
- Loves sloths (see photo of adopted sloth, Flash, above)

Background/History

How Did I Get Here?

BSIDESROC

Another World?

Defensive Security Professionals

Security professionals responsible for defending an organization’s information systems against security threats and risks in the operating environment

Offensive Security Professionals

Security professionals who are responsible for testing the defensive mechanisms put in place to protect an organization's information systems to determine whether they prevent attacks or at least detect them once they have occurred

Defense View

Consider an average web server build:

- Install OS
- Fully patch OS/firmware
- Install/configure web server
- Configure host-based firewall
- Vulnerability scanning
- Document all hardware/software

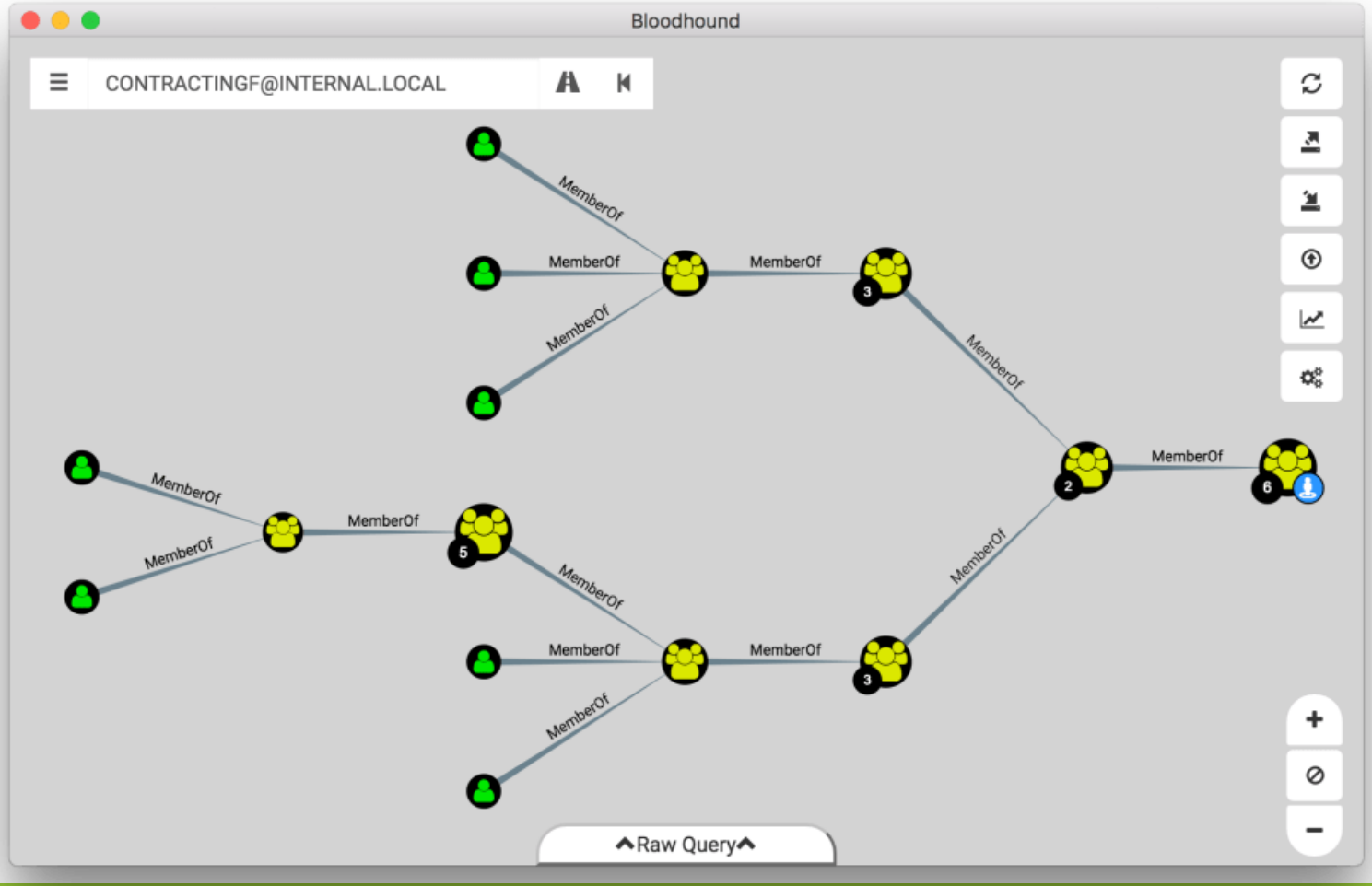
Offense View

- What can I do with port 80/443 open?
  - Are input fields sanitized?
  - Is the output properly encoded?
  - Are there forms with hidden fields?
  - Any interesting ways the site interacts with a server?
  - Is directory traversal possible?
- What is its relationship to other systems?

John Lambert - VP Security Research, Microsoft

"Defenders think in lists, Attackers think in graphs. As long as this is true, attackers win."

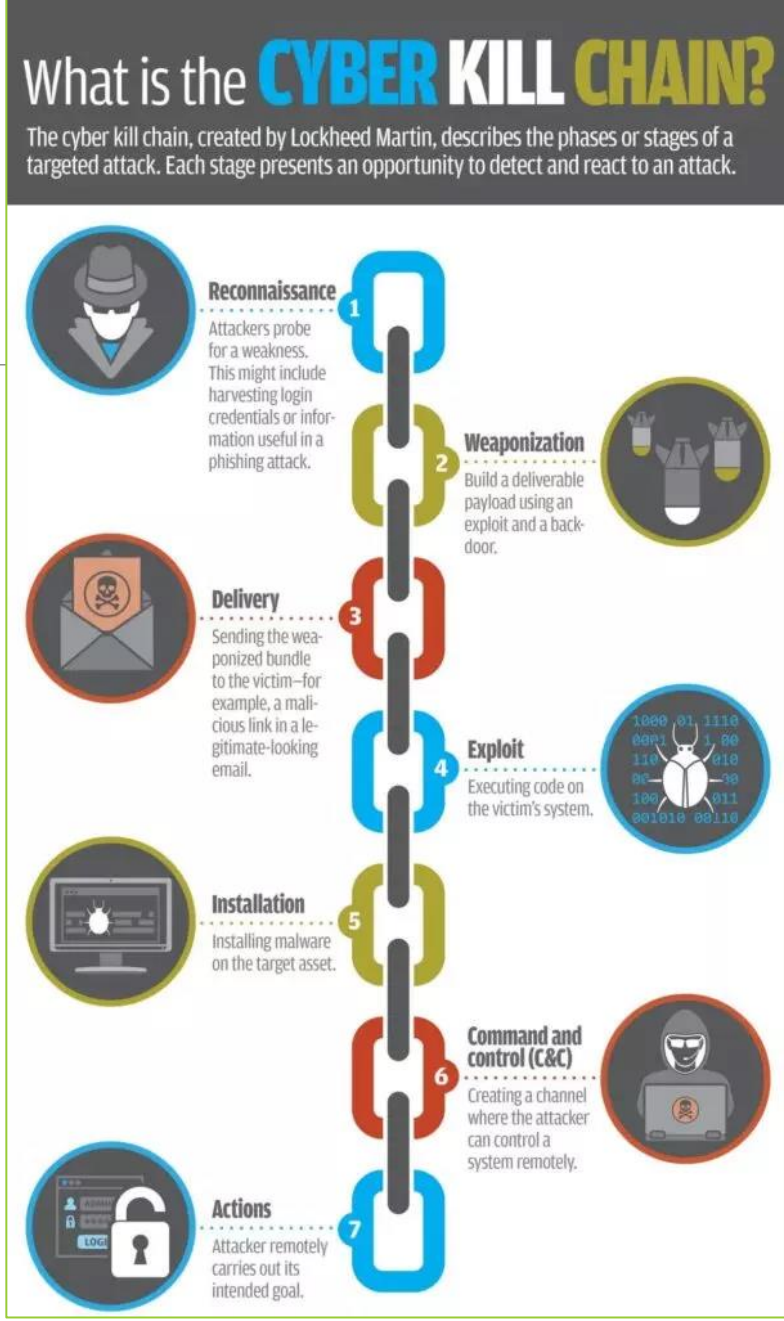
Relationships are Key



SpectreOps BloodHound: Andy Robbins (wald0)

Defender Assumptions

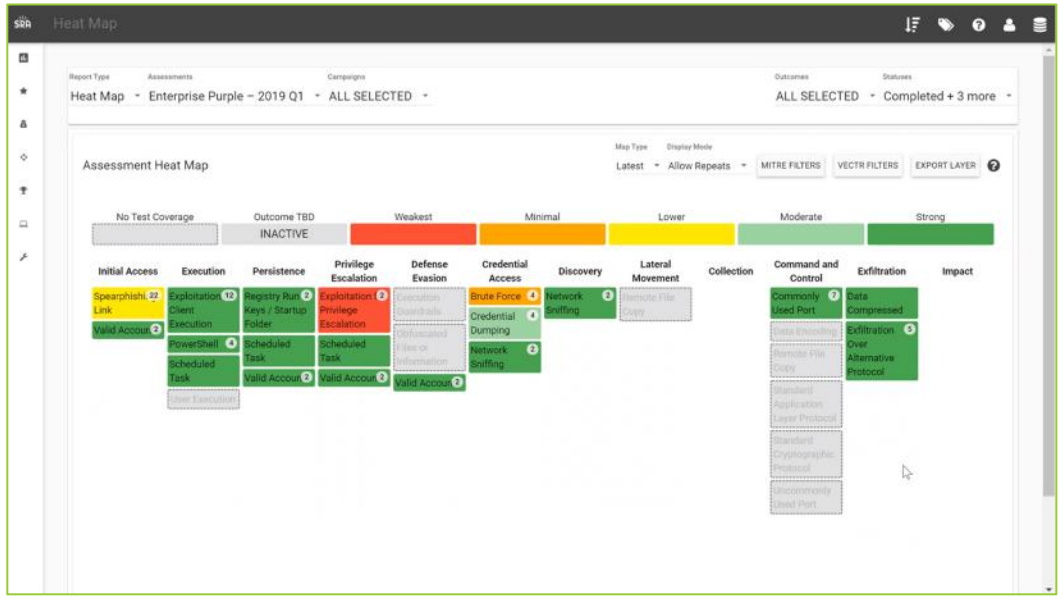
Just Break the Chain!



EDR/AV – We're Safe!

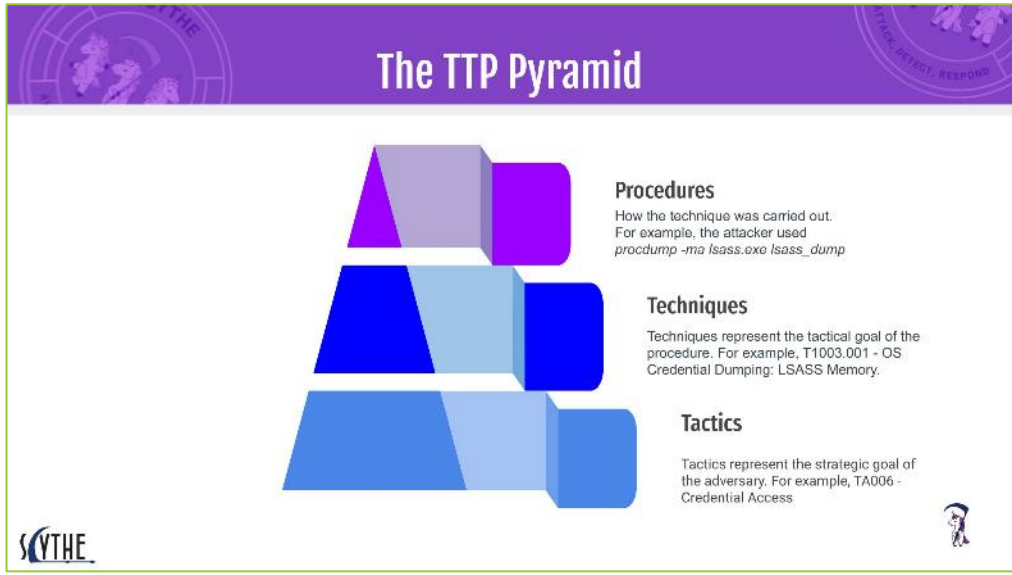
- All EDR/AV products can be bypassed/disabled
  - Tamper Protection/Heuristics irrelevant
  - Research exists against all products
- Many attacks escape EDR/AV entirely
  - C2 callbacks
  - Code execution
  - LOLbins
  - Active Directory abuse

No Worries - We Can Detect It!



What does green actually mean?

Detect Technique != Detect All Procedures



Our Tools Work As Designed!

- Microsoft Automatically Blocks Dangerous Drivers
  - Will Dormann's research (@wdormann)
  - Driver blocklist not enabled, despite HVCI-enabled devices (HVCI = Hypervisor-Protected Code Integrity)
  - ASR unable to block vulnerable drivers from disk (ASR = Attack Surface Reduction)

https://arstechnica.com/information-technology/2022/10/how-a-microsoft-blunder-opened-millions-of-pcs-to-potent-malware-attacks/

Our Tools Work As Designed! (cont.)

- Microsoft Defender for Endpoint
  - Olaf Hartong's research (@olafhartong)
  - Default unregistered events; events required for alerts/telemetry

Lifting the Veil, a Look at MDE Under the Hood - WWHF Presentation

https://www.youtube.com/watch?v=ovRdzyls-jU

MFA! Therefore, Not Phishable

- MFA fatigue
- Configuration issues
  - Legacy protocols still enabled
  - Unexpired passcodes
- Attacks
  - AITM (Evilginx, Muraena, Modlishka)
  - Pass-the-cookie
  - Social Engineering

A New Perspective Is Needed

Immersion in Offensive Security

Offensive Security Engagements

- Targeting – What do we attack?
- Initial Access – How do we get in?
- Persistence – How do we stay in?
- Expansion – How do we get to other things?
- Exfiltration – How do we take data out?
- Detection – How do they find us?

Finding OffSec Professionals

- Security BSides
- Other Security Conferences
- Local Security Meetups
- Makerspaces
- DEFCON Groups
- 2600 Meetings
- Online Security Communities
- Traditional Security Communities

Finding OffSec Training

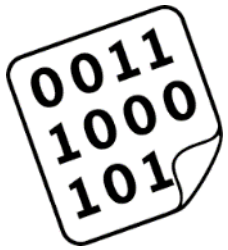
- Conference Trainings
  - Security BSides, DEFCON, GrrCON, Thotcon, WWHF, CircleCityCon, BlackHat
- Security Companies
  - Black Hills/Antisyphon, TrustedSec, Offensive Security, SANS
- Online Options
  - Hackthebox, Tryhackme, CTFs, YouTube
- Higher Education

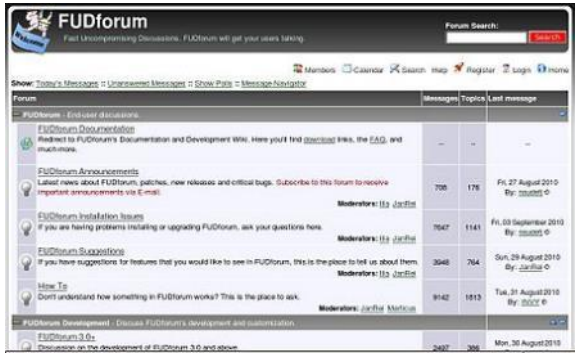
Places to Find Tradecraft Intel

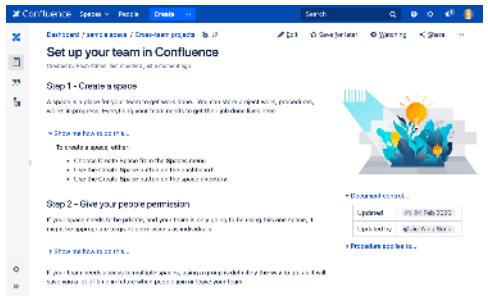
- Project Zero – Google's researchers
- Attackerkb – Rapid 7's researchers
- Discord/Slack
- Twitter
- Mastodon

Places to Find Organizational Intel

- LinkedIn
- Pastebin
- Github
- Message Boards
- Internal Wikis
- Haveibeenpwned





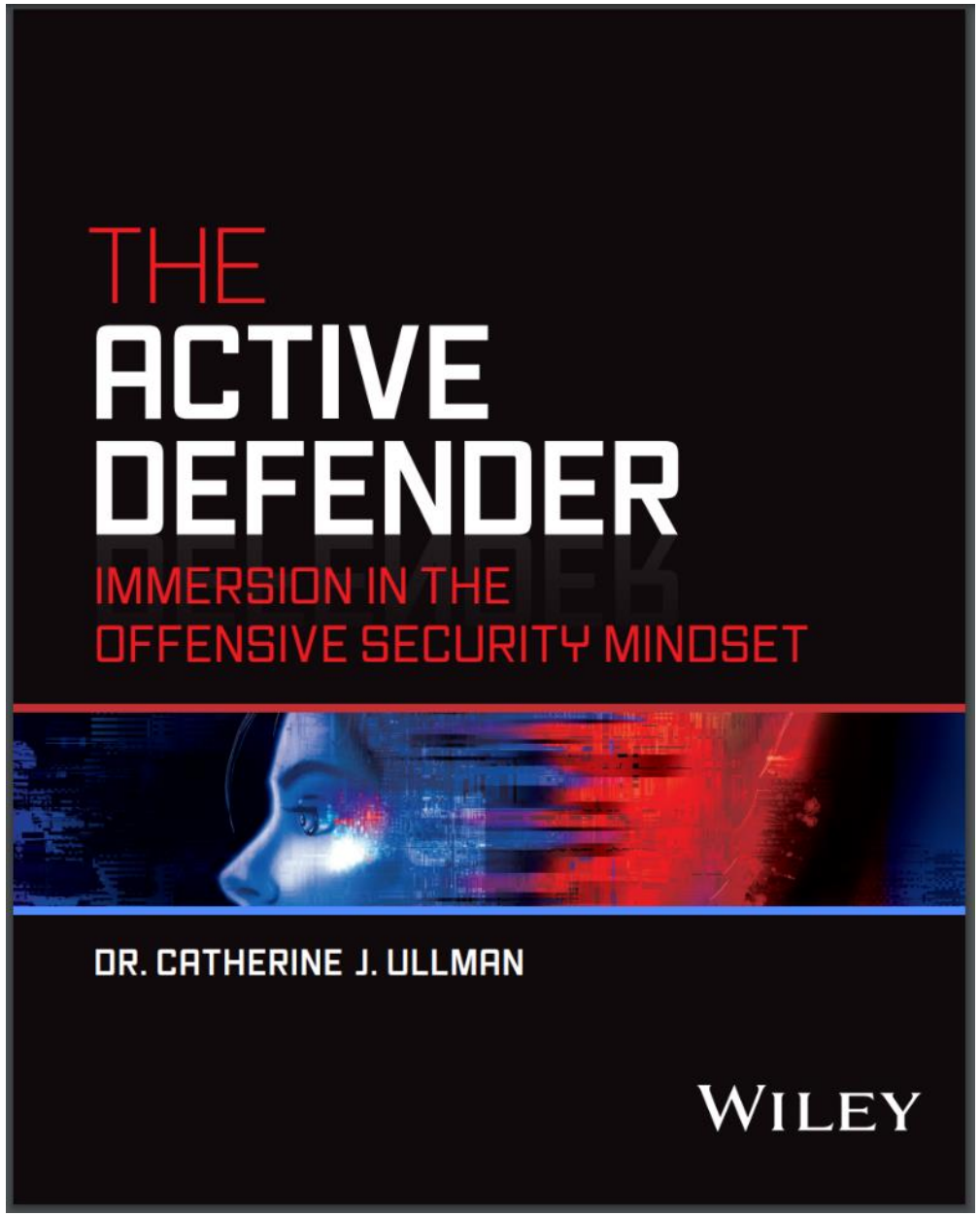


Tools Used by OffSec Pros

- Nmap/Zenmap
- Burp Suite/Zap
- Sqlmap
- Wireshark
- Metasploit Framework
- Shodan
- Social-Engineer Toolkit
- Mimikatz
- Responder
- Cobalt Strike
- Impacket
- Mitm6
- CrackMapExec
- Evil-winrm
- BloodHound/SharpHound/AzureHound

Summary

- Realize defense is only ½ the security story
- Beware of assumptions, especially about controls
- Jump into the other ½ of the security story (offense)
- Meet some OffSec folks
- Learn what they know (tradecraft/tools)
- Become a better defender



Shameless Self-Promotion

Available in both hardcopy and e-book from booksellers everywhere!

"I may not have gone where I intended to go, but I think that I have ended up where I needed to be." ~Douglas Adams