

Active Defense, Offensive Countermeasures, and Cyber Deception

John Strand | Bryce Galbraith | Paul Asadoorian

• Course Virtual Machines

- Definitions and Disclaimers
- Mourning Our Destiny, Leaving Youth and Childhood Behind
- **Lab: Bad Guy Defenses**
- Basics and Fundamentals (or, Don't Get Owned Doing This) ****
- Kansa
- **Lab: Kansa**
- Segmentation
- Self-Assessment
- **Playing with Advanced Backdoors**
- Software Restriction Policies
- **Lab: AppLocker**
- Legal Issues
- Venom and Poison
- **Annoyance**
- Attribution
- Attack!



Course Virtual Machines

- The course VMs were exported into OVF format to facilitate importation
 - Open Virtual Machine Format (OVF)
- VMware's Player/Workstation/Fusion are officially supported
 - Other VMEs should work as well (e.g., VirtualBox)
- To begin, File -> Import (or Open) the .ovf file for each VM
 - You should allocate 2 GB+ of RAM to each VM
 - Configure the virtual networking to Bridged (wired adapter)
 - Acquire a DHCP address from the classroom's DHCP server (wired network)
- Open the usage_docs.html file on the desktop
 - The browser should open to a convenient web-based menu system
 - Most lab instructions are within these neatly organized web pages
- Screen resolution can be adjusted using the menu
 - Blue icon in upper-left corner -> Settings -> Display (adjust to your liking)



Instructions on VM

L
A
B



Instructions on VM

L
A
B

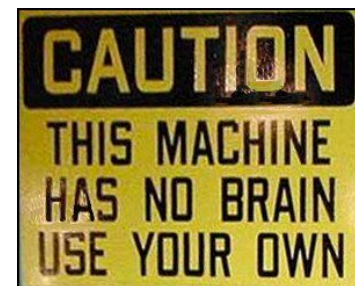
This Course Is Different

- 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! ;-)



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?

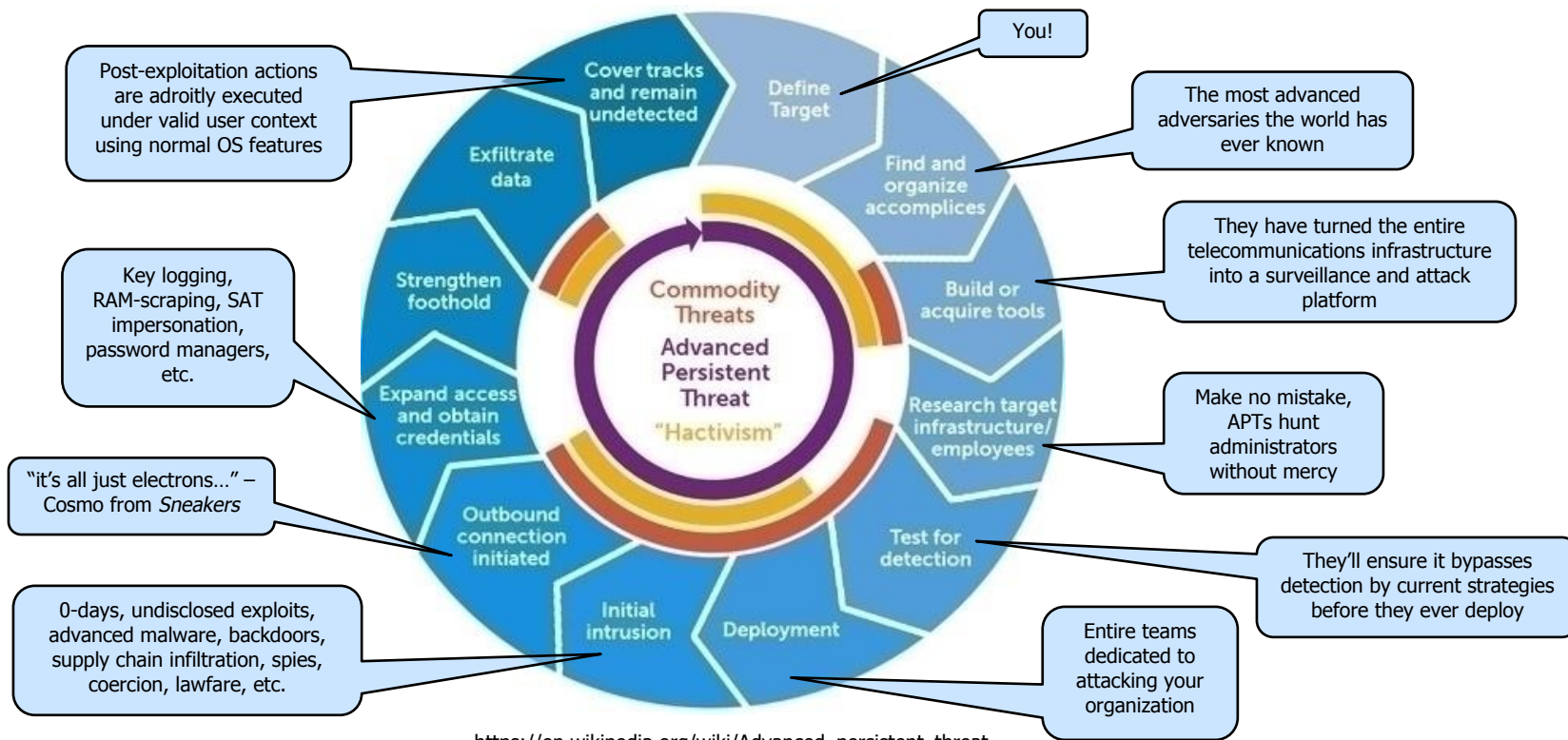
- Offensive countermeasures employ offensive techniques as aggressors attack ... *but with a defensive posture*
 - Aikido provides an excellent analogy
 - Aikido focuses on redirecting and blocking opponents' attacks while taking considerable care not to harm them in the process
 - Aikido practitioners *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?

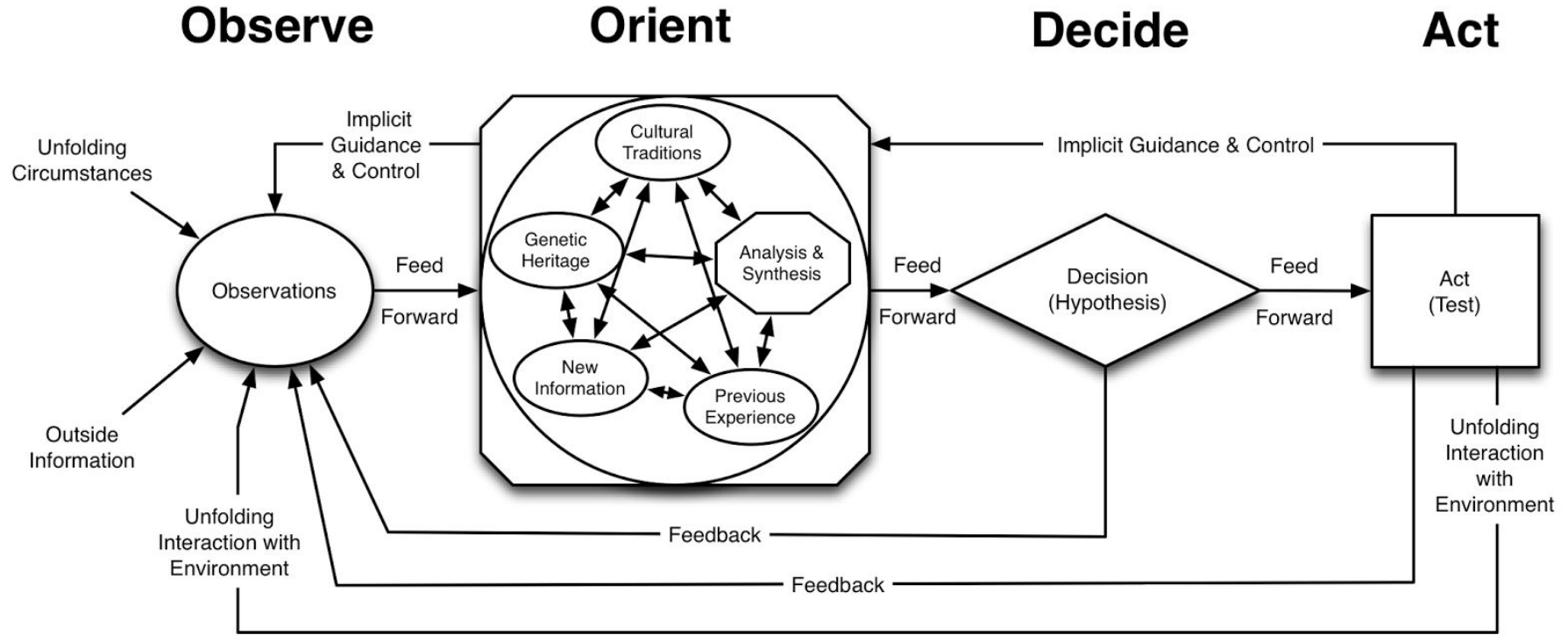
- Cyber deception is the deliberate and calculated process of deceiving attackers in an effort to wage a better defense
 - Slow them down, confuse them, deceive them ... make them work harder
 - Serves to significantly increase your chances of detection
 - Designed to make $\mathbf{Detection}_t + \mathbf{Reaction}_t < \mathbf{Attack}_t$ ($\mathbf{D}_t + \mathbf{R}_t < \mathbf{A}_t$)
- 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

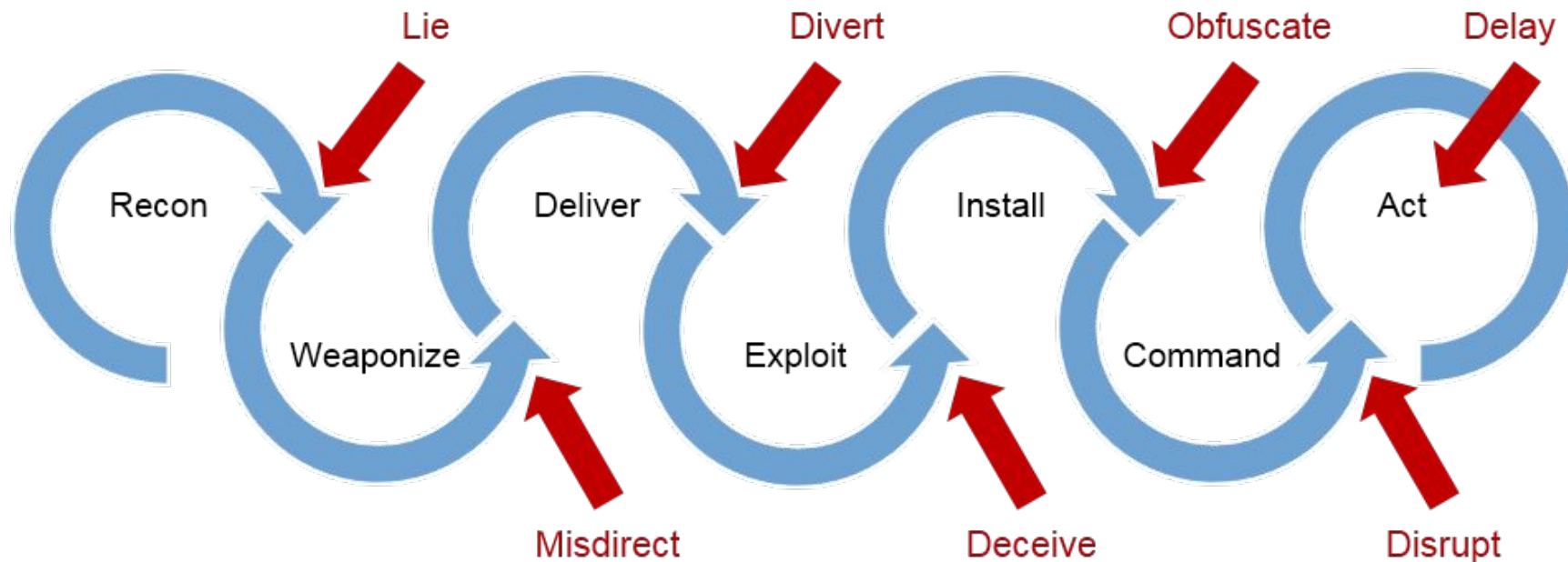


https://en.wikipedia.org/wiki/Advanced_persistent_threat

The OODA Loop



Disrupting the OODA Loop



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

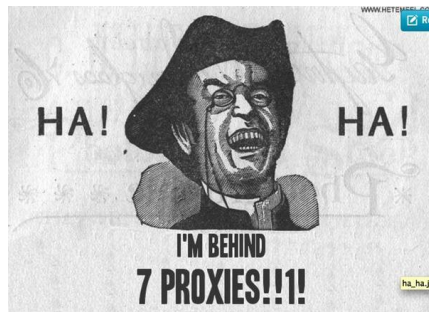


More Fun Check: @funny.com

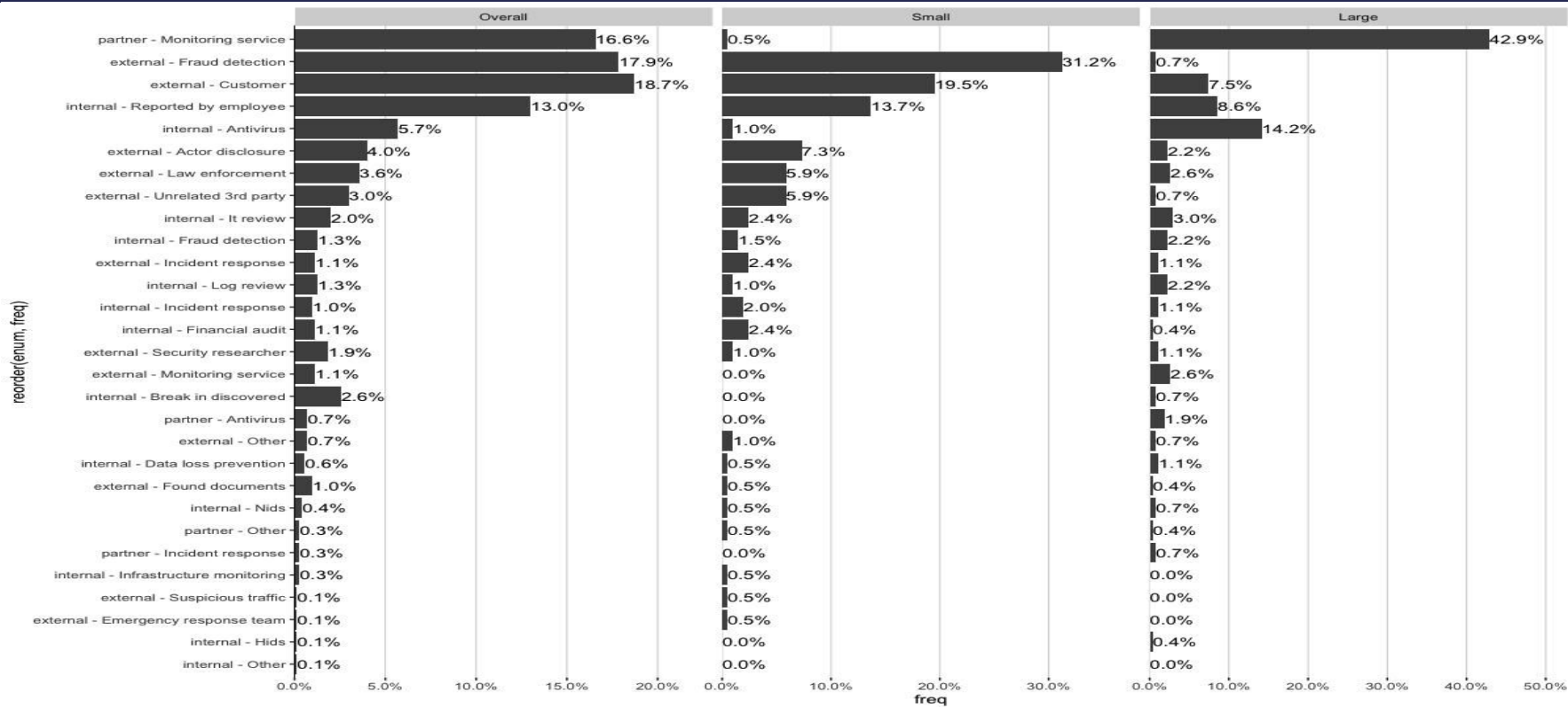


Why These Skills Are Critical

- 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



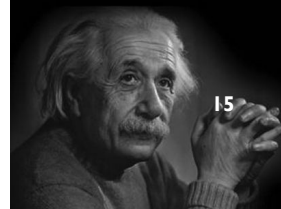
These Are Just The Ones We Know About...



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?

**Insanity: doing the
same thing over and
over again and
expecting different
results.**



Albert Einstein
German Theoretical-Physicist
(1879-1955)

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?



Behold, the Next-Gen Gate! (Accepting Orders Now)



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



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.

Introductions and Standards

- Course Virtual Machines
- Definitions and Disclaimers
- Mourning Our Destiny, Leaving Youth and Childhood Behind
- ***Lab: Bad Guy Defenses***
- Basics and Fundamentals (or, Don't Get Owned Doing This) ****
- Kansa
- ***Lab: Kansa***
- Segmentation
- Self-Assessment
- ***Playing with Advanced Backdoors***
- Software Restriction Policies
- ***Lab: Software Restriction Policies***
- **Legal Issues**
- Venom and Poison
- **Annoyance**
- Attribution
- Attack!



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

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 everyday

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



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



Annoyance

29

Commercial Cyber Deception

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



Why are we doing this?

- Because free will prime the pump
- Get the ideas flowing
- We need a fundamental change in security
- What we are doing is not working
- This can be done quickly and cheaply

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

Go on.. Be obvious!

The screenshot displays the Windows Active Directory Users and Groups console. On the left, a list of users is shown, with 'Admin ADM. Administrator' selected. On the right, the 'Admin ADM. Administrator Properties' dialog box is open, showing the 'General' tab. The user's first name is 'Admin' and the last name is 'Administrator', resulting in a display name of 'AdminADM.Administrator'.

Name	Type	Description
Abraham.Mccoy	User	
Admin ADM. Administrator	User	
Alberta.Armstrong	User	
Alberto.Patterson	User	
Alfredo.Perkins	User	
Allan.Reid	User	
Amos.Edwards	User	
Angela.Garner	User	
Angela.Hampton	User	
Angela.Knight	User	
Angelo.Richards	User	
Anthony.Caldwell	User	
Antoinette.Morrison	User	
Antonio.Garza	User	
Arlene.Poole	User	
Arturo.Abbott	User	
Becky.Wise	User	
ben.arnold	User	
Bernadette.Crawford	User	
Bernice.Lawson	User	
Bertha.Schultz	User	

Admin ADM. Administrator Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	

General | Address | Account | Profile | Telephones | Organization

Admin ADM. Administrator

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

Disable Logon Hours

User logon name:

@Win.Lab

User logon name (pre-Windows 2000):

☐ Unlock account

Logon Hours for Admin ADM. Administrator

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

All	12	2	4	6	8	10	12	2	4	6	8	10	12
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

☐ Logon Permitted
☒ Logon Denied

OK Cancel

Sunday through Saturday from 12:00 AM to 12:00 AM

Set up Snare



SNARE for Windows Open Source

Latest Events

Network Configuration

Remote Control Configuration

Objectives Configuration

HeartBeat and Agent Log

View Audit Service Status

Apply the Latest Audit Configuration

Local Users
Domain Users
Local Group Members
Domain Group Members
Registry Dump

SNARE Network Configuration

The Snare Agents are issued as both a free Open Source download (this agent) as well as an Enterprise Agent. Wondering how to determine the type of agent your organisation should use? Ask yourself the following questions to aid in selecting the right agent for your organization.

1. **Support** - If you need a supported security platform, then you need to use the Enterprise Agent. The Enterprise Agents include maintenance, upgrades, and bug fixes to ensure the agent is provided to the open source community free of charge for your organization.
2. **Complete and Factual** - If your organization needs to know that absolutely everything is being reported, then you need to use the Enterprise Agent. The Open Source Agent does not support TCP, caching, custom event logs, UTC or real time reporting. With integrity then you need to use the Enterprise Agent.
3. **Sensitivity and Confidentiality** - Should your organization work with sensitive data, then you need to use the Enterprise Agents which includes the ability to support secure communication practices and encryption protocols.

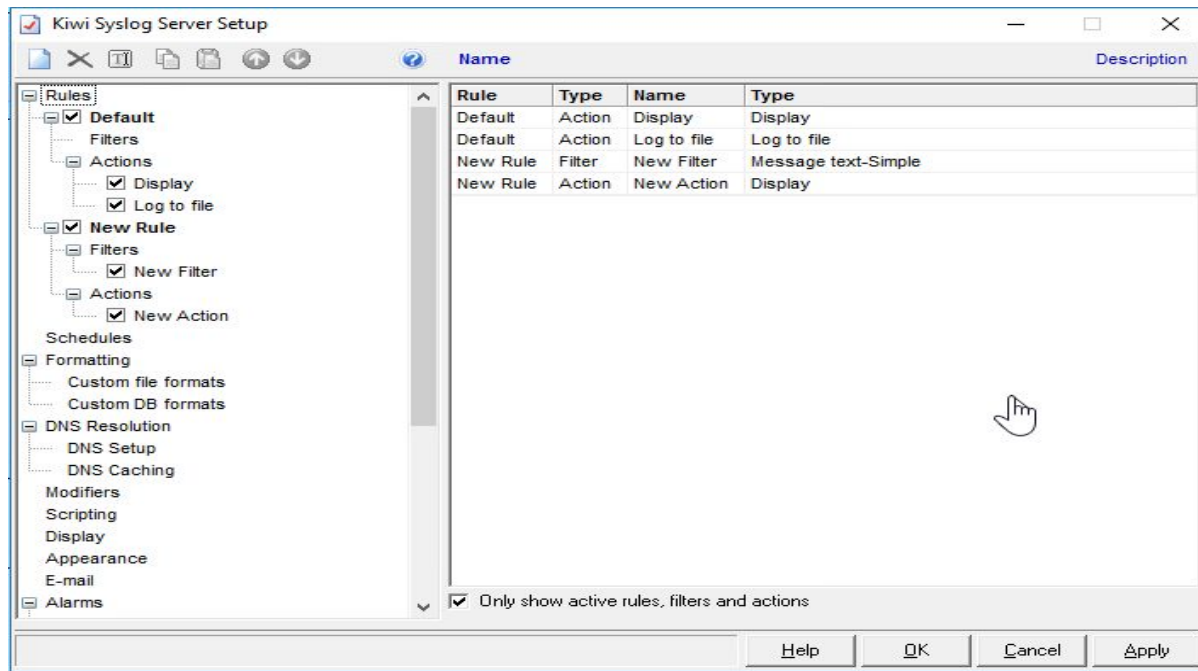


Click [Here](#) for more information on the Snare Enterprise Agent

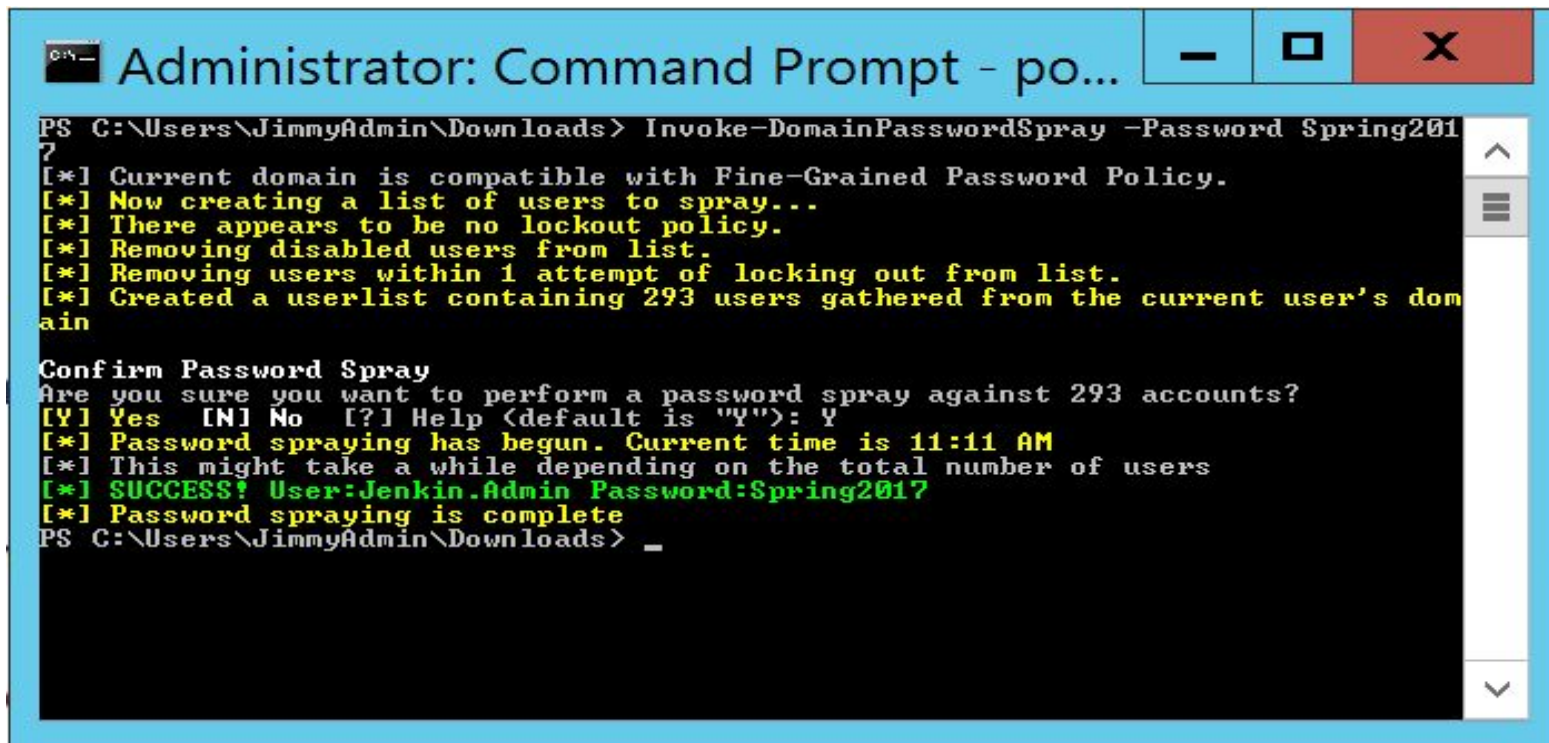
The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address (Multiple destinations available in the enterprise version)	10.233.233.245
Destination Port	514
Allow SNARE to automatically set event log max size (Enterprise version only)	<input type="checkbox"/>

Set up Kiwi



Password Spray



```
Administrator: Command Prompt - po...
PS C:\Users\JimmyAdmin\Downloads> Invoke-DomainPasswordSpray -Password Spring2017
[*] 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 domain

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

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>



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 o-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

- **Definitions and Standards**
- **Annoyance**
- OSfuscate, DNS, and Other Oddities
- ***Lab: OSfuscate***
- Fuzzing Attackers
- ***Lab: DOM-Hanoi***
- Evil Web Servers
- ***Lab: SpiderTrap***
- Not Getting Shot Is Important (or How to Set This Up at Work)
- ***Lab: Thug***
- Recon on Bad Servers and Bad People
- Remux.py
- ***Lab: Evil***
- Honeypots
- ***Lab: Dionaëa***
- Honeyports
- ***Lab: Honeyports***
- ***Portspoof***
- ***Lab: Portspoof***
- Kippo
- ***Lab: Kippo***
- Artillery
- ***Artillery***
- More Evil Web Servers
- ***Lab: Weblabyrinth***
- Cryptolocked
- ***Lab: Cryptolocked***
- Application-Specific Honeypots
- ***Lab: Conpot***

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

Portspooft 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      Control 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)
```

45

Annoyance

- **Definitions and Standards**
- **Annoyance**
- OSfuscate, DNS, and Other Oddities
- ***Lab: OSfuscate***
- Fuzzing Attackers
- ***Lab: DOM-Hanoi***
- Evil Web Servers
- ***Lab: SpiderTrap***
- Not Getting Shot Is Important (or How to Set This Up at Work)
- ***Lab: Thug***
- Recon on Bad Servers and Bad People
- Remux.py
- ***Lab: Evil***
- Honeyports
- ***Lab: Dionaea***
- Honeyports
- ***Lab: Honeyports***
- Portspooft
- ***Lab:*
*Portspooft***
- Kippo
- ***Lab: Kippo***
- Artillery
- ***Artillery***
- More Evil Web Servers
- ***Lab: Weblabyrinth***
- Cryptolocked
- ***Lab: Cryptolocked***
- Application-Specific Honeyports
- ***Lab: Conpot***

Lab: Portspooft

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



Instructions on VM

Attribution

- Dealing with TOR
- **Honeytokens**
 - **Lab: Canarytokens**
 - Word Web Bugs (or Honeydocs)
 - **Lab: Word Web Bugs**
 - Nova
 - **Lab: Nova**
 - Infinitely Recursive Windows Directories
 - **Attack**
 - **Capstone Exercise!**

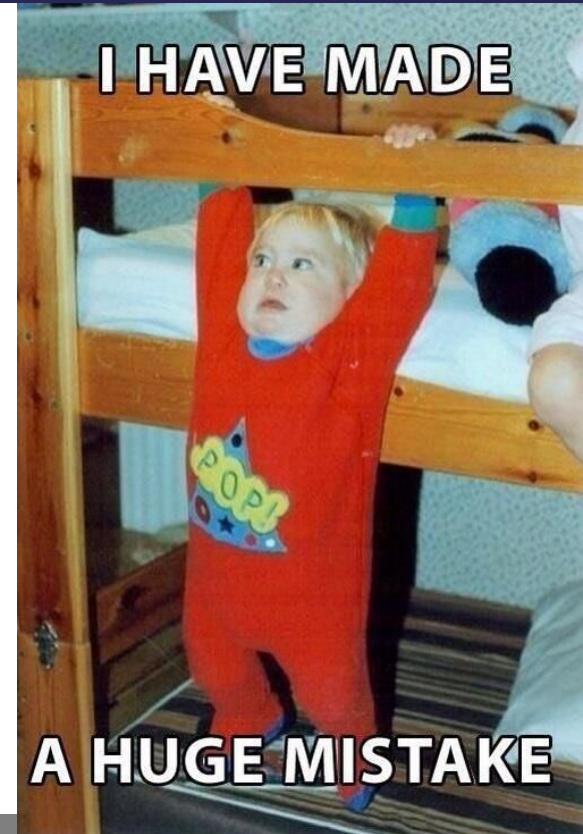


Implementing the Canarytoken Engine

- 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

Scenario: Recon

- Let's go through the attack phases and cover how we can disrupt an attacker attempting recon on an environment
- All attack methodologies are based on information gathered during this phase
- It is possible to trick an attacker at this phase



AWS Keys

Your AWS key token is active!

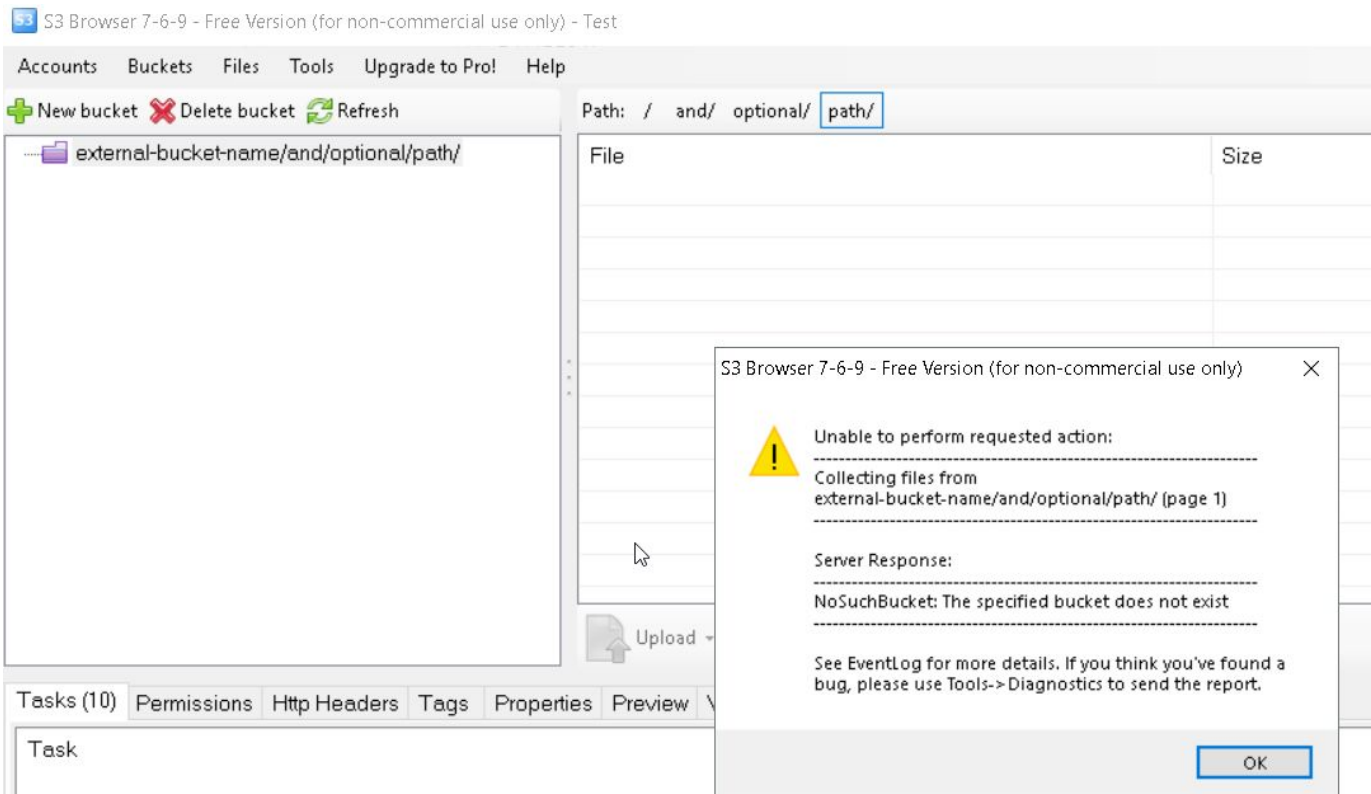
Copy this credential pair to your clipboard to use as desired:

```
[default]
aws_access_key_id = AKIAJRN2YPG2JK7EC7YA
aws_secret_access_key = F6W3nzTodbFf1o66OV31UjQhn2Rz/4+XI+Qckcz
output = json
region = us-east-2
```



Download your AWS Creds

Trigger



Alert

Canarytoken triggered

ALERT

An AWS API Key Token Canarytoken has been triggered by the Source IP 107.77.195.231.

Basic Details:

Channel	AWS API Key Token
Time	2019-09-05 18:17:08
Canarytoken	fi4tamoi5h2muzdh0ix4uv5n
Token Reminder	sdsdsd
Token Type	aws_keys
Source IP	107.77.195.231
User Agent	S3 Browser 8-4-1 https://s3browser.com

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Context

- Attackers love looking into Github for exposed AWS keys
- So do security researchers



.exe

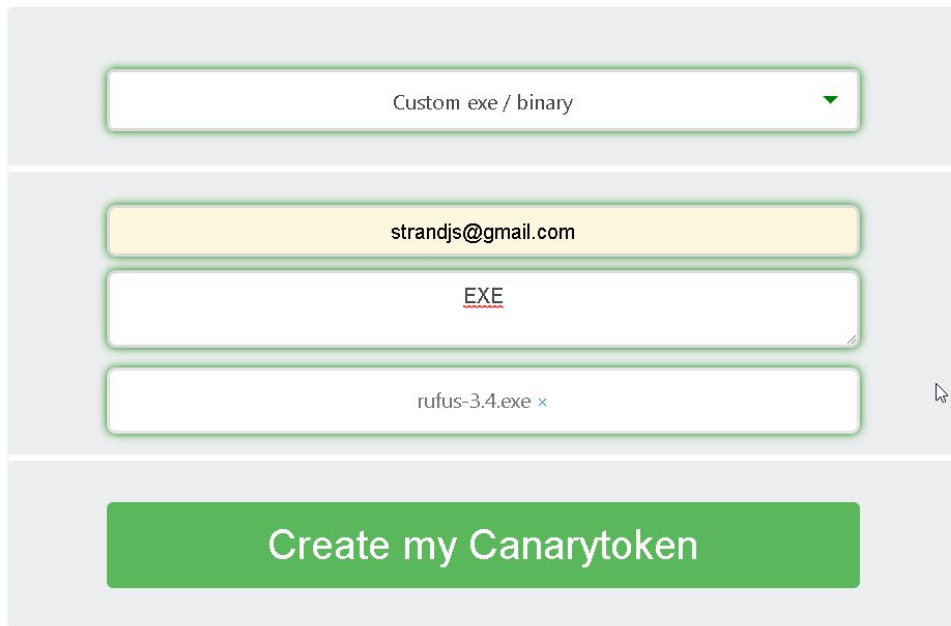
- How would we ever get an attacker to run a .exe?
- Easy
- vpnconfig.exe
- Sysprep.exe
- Oh.. So many ways



Setup

Canarytokens by Thinkst

What is this and why should I care?



A screenshot of the Canarytokens setup form. The form is divided into four horizontal sections. The first section contains a dropdown menu with the text "Custom exe / binary" and a downward arrow. The second section contains a text input field with the email address "strandjs@gmail.com". The third section contains a text input field with the file extension "EXE". The fourth section contains a text input field with the filename "rufus-3.4.exe" followed by a small 'x' icon. Below these sections is a large green button with the text "Create my Canarytoken".

Custom exe / binary ▼

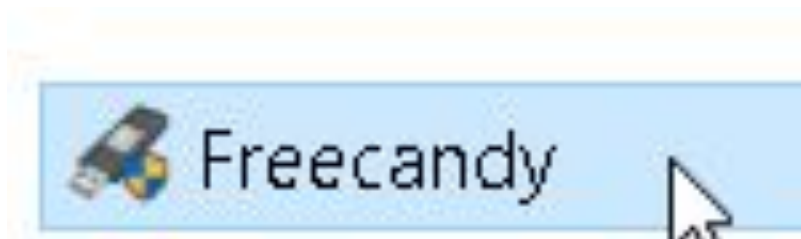
strandjs@gmail.com

EXE

rufus-3.4.exe x

Create my Canarytoken

Trigger



Basic Details:

Channel	DNS
Time	2019-02-27 21:41:15
Canarytoken	jznohj8hg1xrnu17wgxqstld
Token Reminder	EXE
Token Type	signed_exe
Source IP	24.214.199.44

Canarytoken Management Details:

Why not make it real?



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
```

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
```

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="+  
        encodeURIComponent(l) + "&r=" + encodeURIComponent(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.

Trigger

ALERT

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

Basic Details:

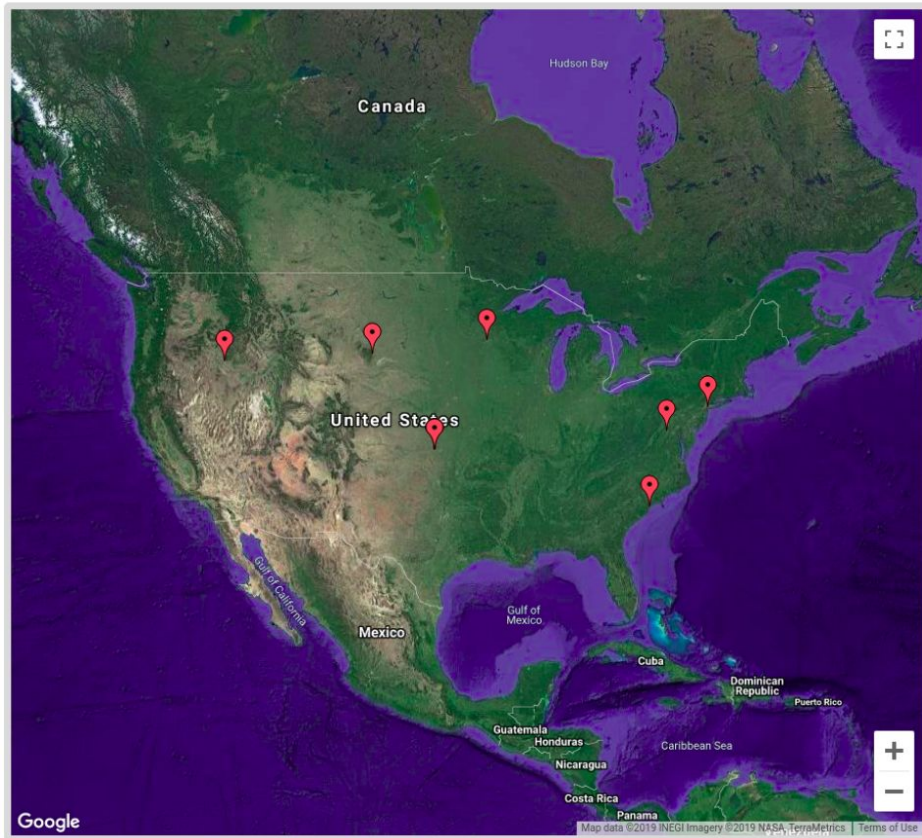
Channel	HTTP
Time	2019-08-13 13:16:13
Canarytoken	y7[REDACTED]22no
Token Reminder	Cloned website token for: [REDACTED].blackhillsinfosec.com
Token Type	clonedsite
Source IP	[REDACTED]
User Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 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

History

Incident Map



Incident List

Export

Date: 2019 Sep 06 14:30:36 IP: [REDACTED] Channel: HTTP

Date: 2019 Jul 25 09:06:48 IP: [REDACTED] Channel: HTTP

Date: 2019 Jul 25 04:10:21 IP: [REDACTED] Channel: HTTP

Date: 2019 Jul 24 23:51:42 IP: [REDACTED] Channel: HTTP

Date: 2019 Jul 24 23:49:15 IP: [REDACTED] Channel: HTTP

Date: 2019 Jul 24 23:49:13 IP: [REDACTED] Channel: HTTP

Date: 2019 Jul 24 23:49:05 IP: [REDACTED] Channel: HTTP

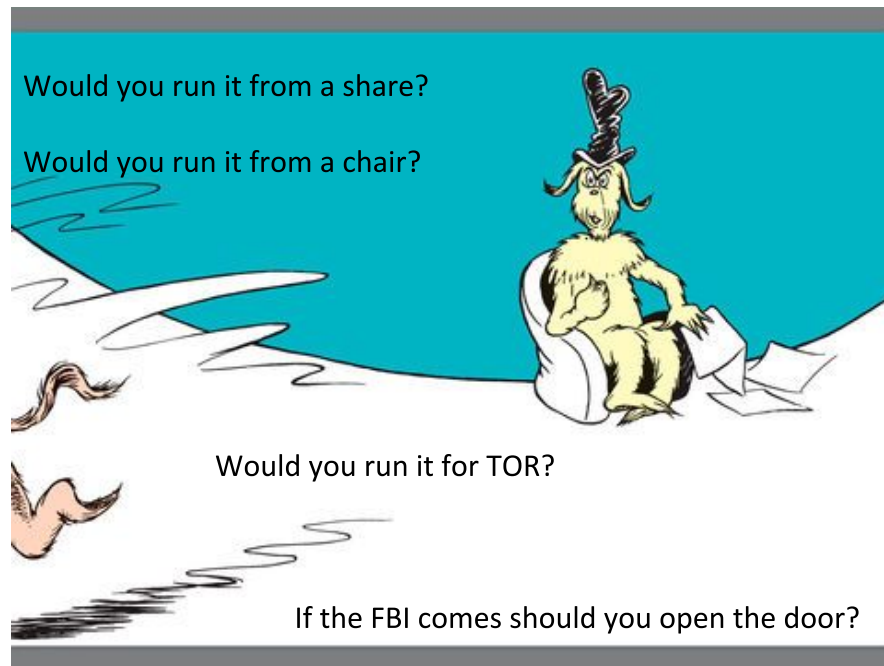
Date: 2019 Aug 18 07:27:35 IP: [REDACTED] Channel: HTTP

Date: 2019 Aug 13 17:44:54 IP: [REDACTED] Channel: HTTP

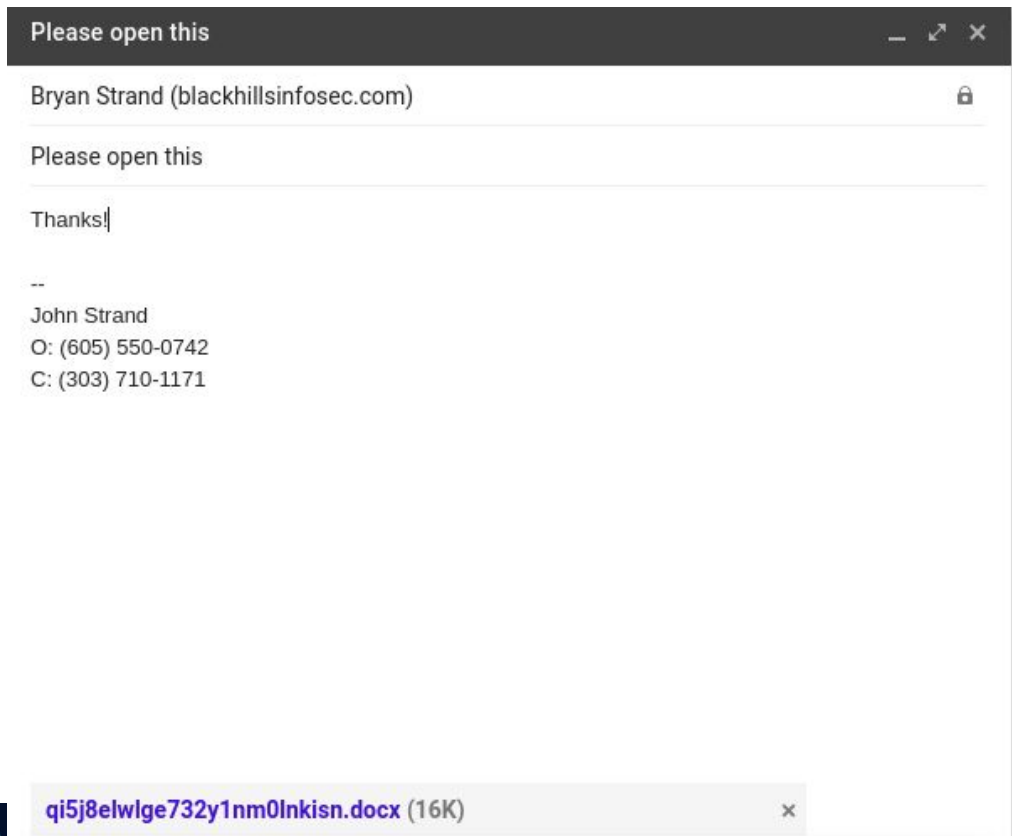
Date: 2019 Aug 13 13:16:12 IP: [REDACTED] Channel: HTTP

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...



Yes! CanaryTokens!

Canarytoken triggered

ALERT

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

Basic Details:

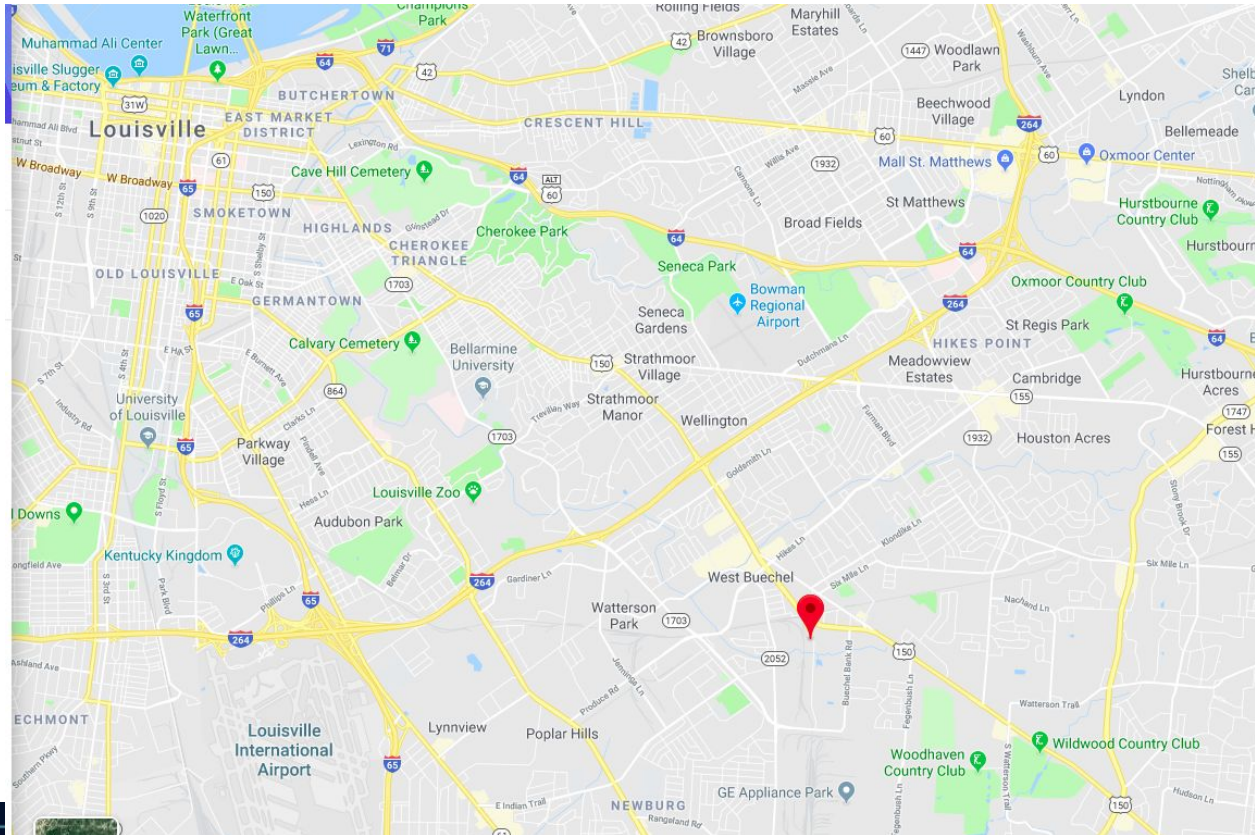
Channel	HTTP
Time	2019-09-06 10:51:36
Canarytoken	qi5j8elwlge732ylnm0lnkisin
Token Reminder	He opened it.
Token Type	ms_word
Source IP	74.143.15.100
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

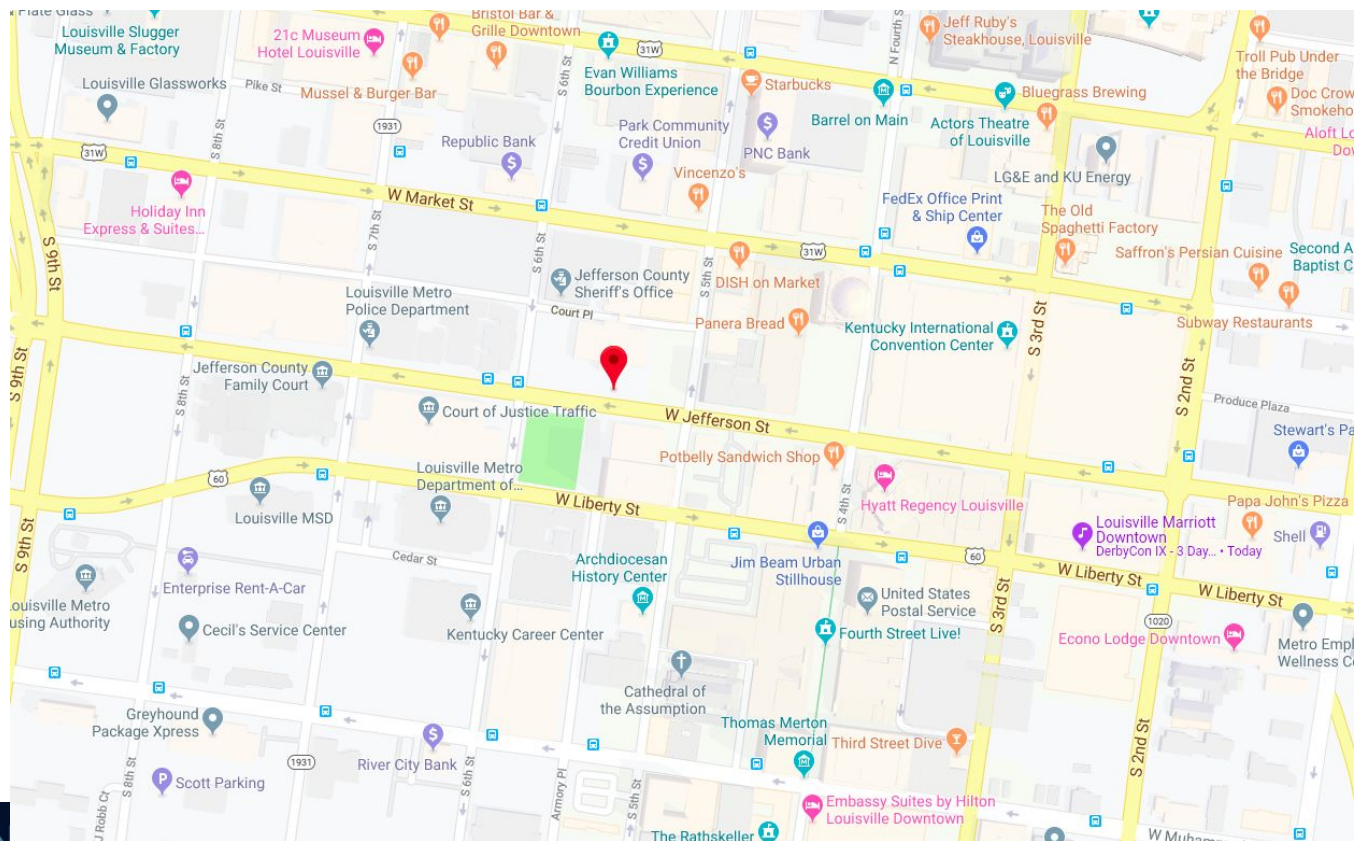
Not bad..



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
```

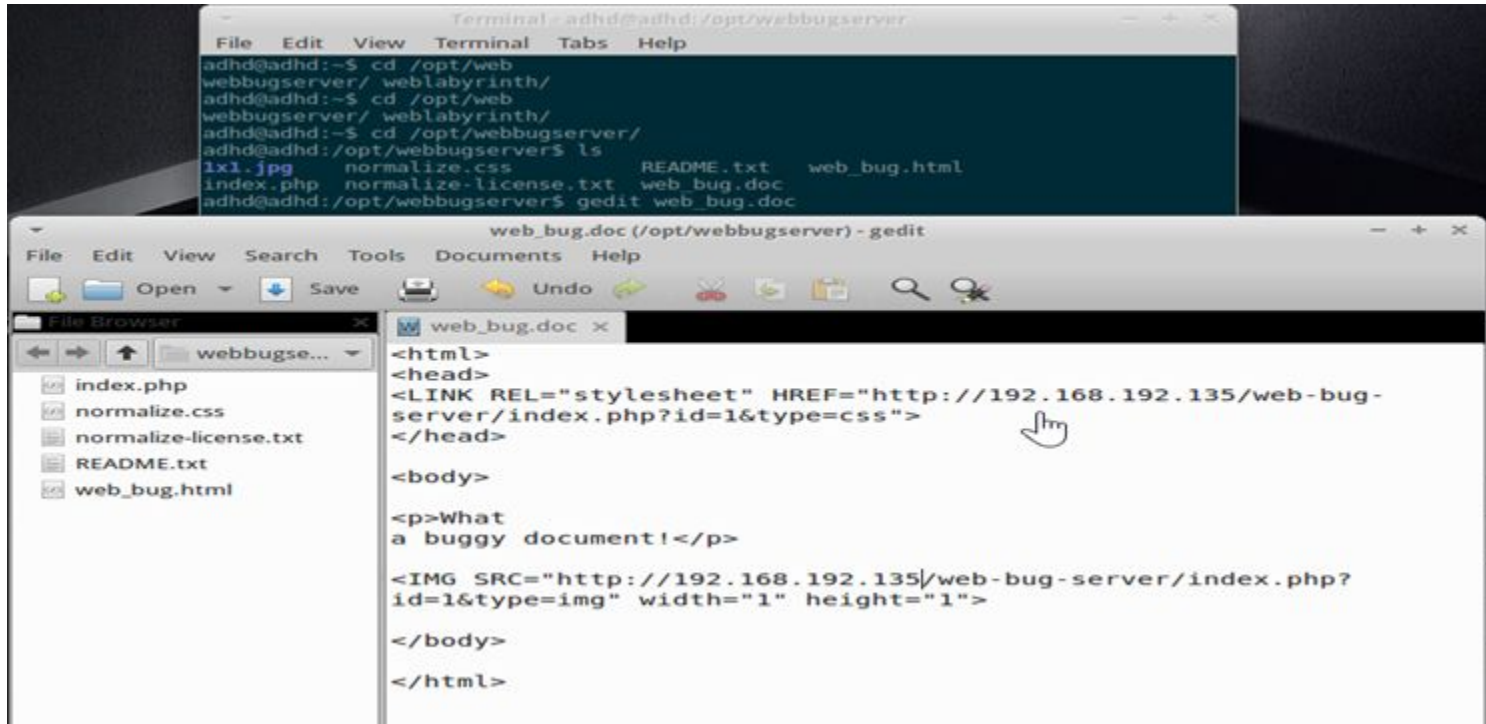

Enhance



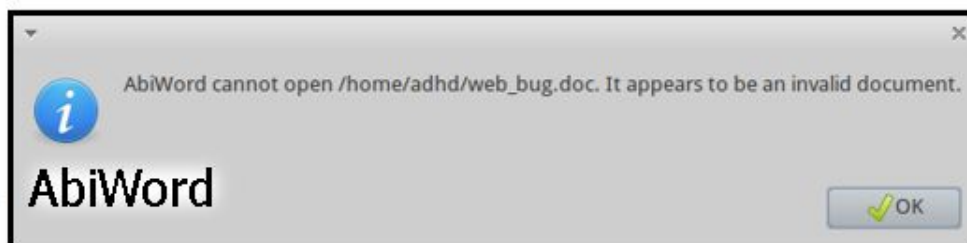
But!

- 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

Word Web Bugs



Tracking!



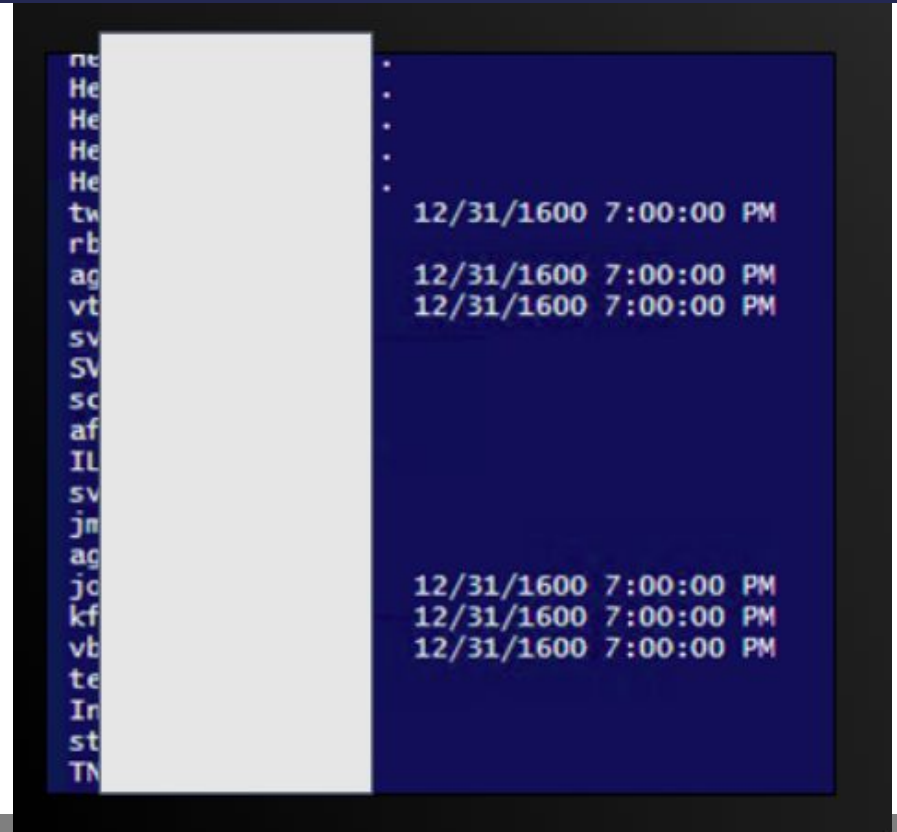
<u>type</u>	<u>ip_address</u>	<u>user_agent</u>
img	127.0.0.1	gvfs/1.12.1
css	127.0.0.1	
img	127.0.0.1	
img	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like Gecko)
css	192.168.1.195	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, 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

One Step Forward...



Name	Type	Description
Abraham.Mccoy	Use	
Admin ADM. Administrator	Use	
Alberta.Armstrong	Use	
Alberto.Patterson	Use	
Alfredo.Perkins	Use	
Allan.Reid	Use	
Amos.Edwards	Use	
Angela.Garner	Use	
Angela.Hampton	Use	
Angela.Knight	Use	
Angelo.Richards	Use	
Anthony.Caldwell	Use	
Antoinette.Morrison	Use	
Antonio.Garza	Use	
Arlene.Poole	Use	
Arturo.Abbott	Use	
Becky.Wise	Use	
ben arnold	Use	
Bernadette.Crawford	Use	
Bernice.Lawson	Use	
Bertha.Schultz	Use	

Admin ADM. Administrator Properties

Member Of

Dial-in

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

General


Address

Account

Profile

Telephones

Organization

 Admin ADM. Administrator

First name: Admin

Initials: ADM

Last name: Administrator

Display name: AdminADM.Administrator

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

Important!

adminadmin @Win.Lab

winlab\	adminadmin
---------	------------

Log On To...



Logon Hours for Admin ADM. Administrator

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

All

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

OK

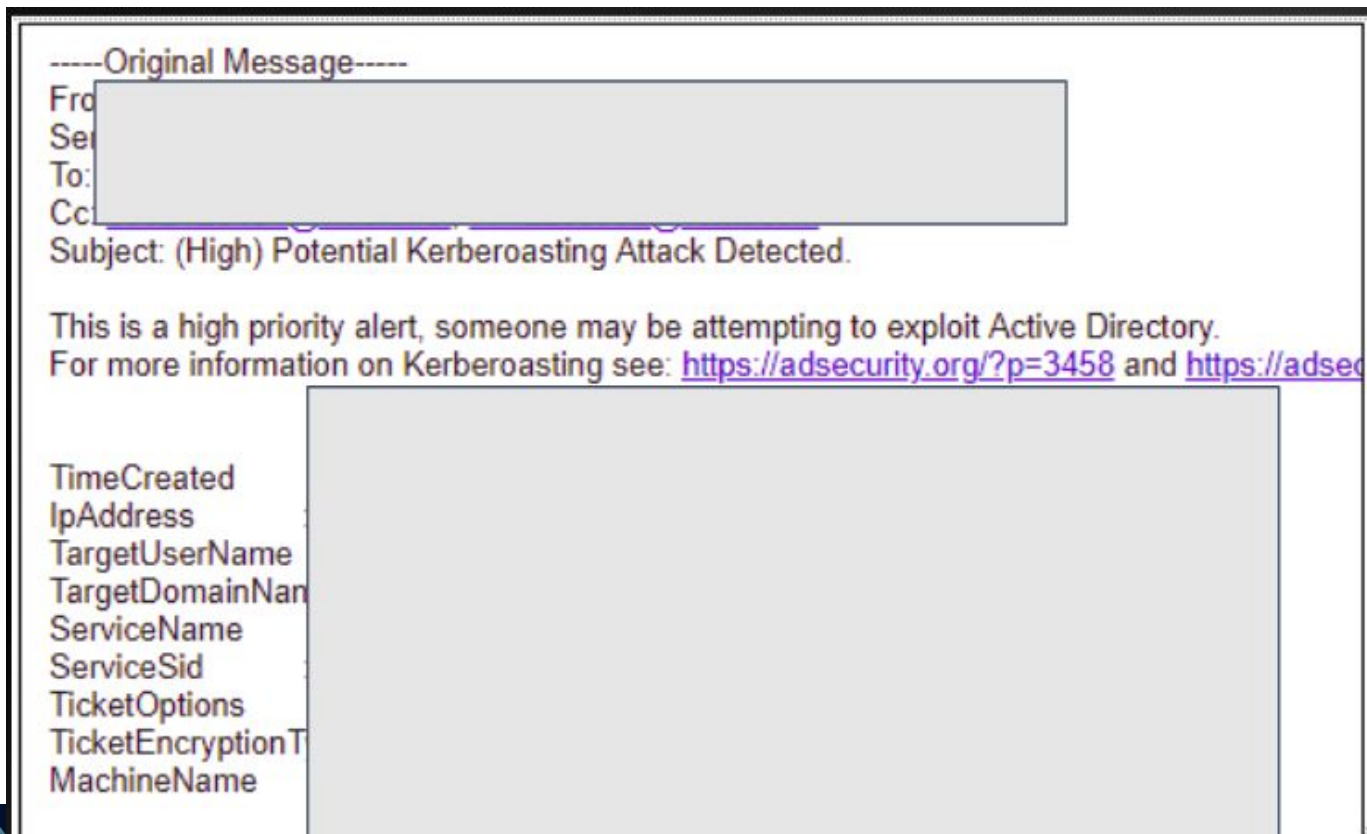
Cancel

☐ Logon Permitted

☒ Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

Kerberoasting



We Love Adding This...

- **Effective Use of Traps:** Multiple hosts on the domain were installed as traps. Activities conducted by BHIS revealed that these traps were vulnerable to multiple insecurities and they made tempting targets. Any interaction with these hosts triggered alerts to the customer and these were reported to BHIS during the test. While these should not be relied on as a sole source of protection, they do provide an added layer of defense-in-depth.
- We love it when testers cry. I collect their tears... It makes the best wine.

Attribution

- Dealing with TOR
- Canarytokens

- **Lab: Canarytokens**

- Word Web Bugs (or Honeydocs)
- **Lab: Word Web Bugs**
- Nova
- **Lab: Nova**
- Infinitely Recursive Windows Directories
- **Attack**
- **Capstone Exercise!**

