- ***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

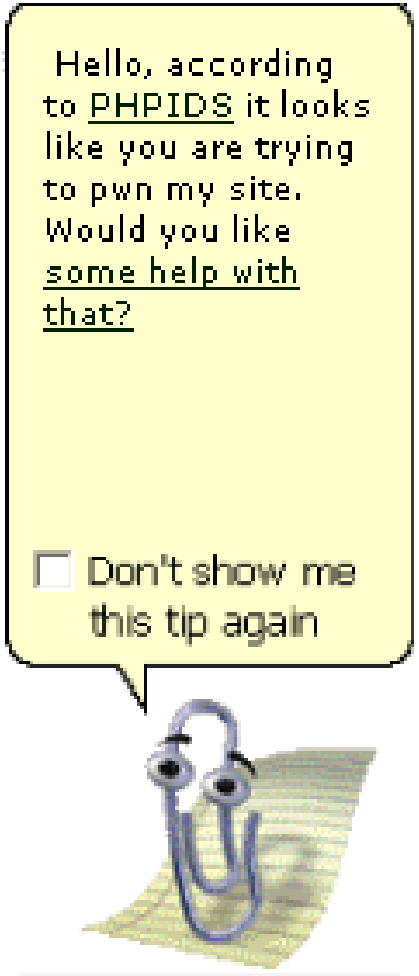
Annoyance

- ***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

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
```

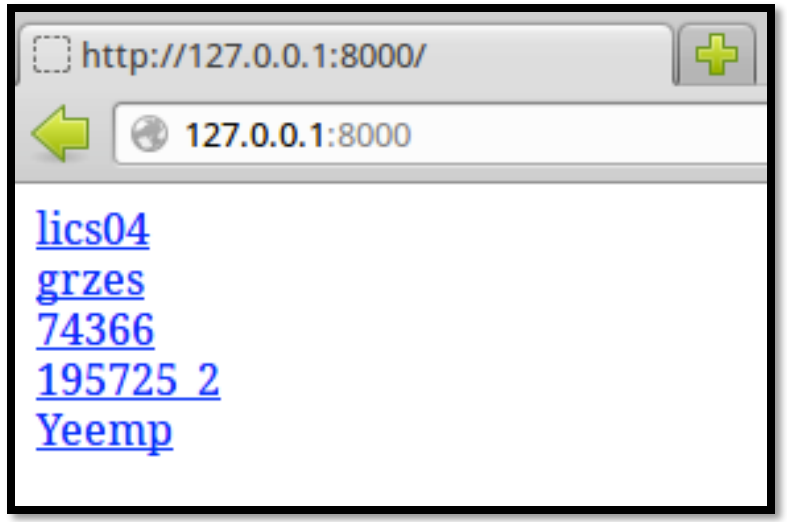
- Many testers use the Ron Popeil testing methodology
  - "Set it and forget it!"
- This would lead to a fun surprise when the testers come back

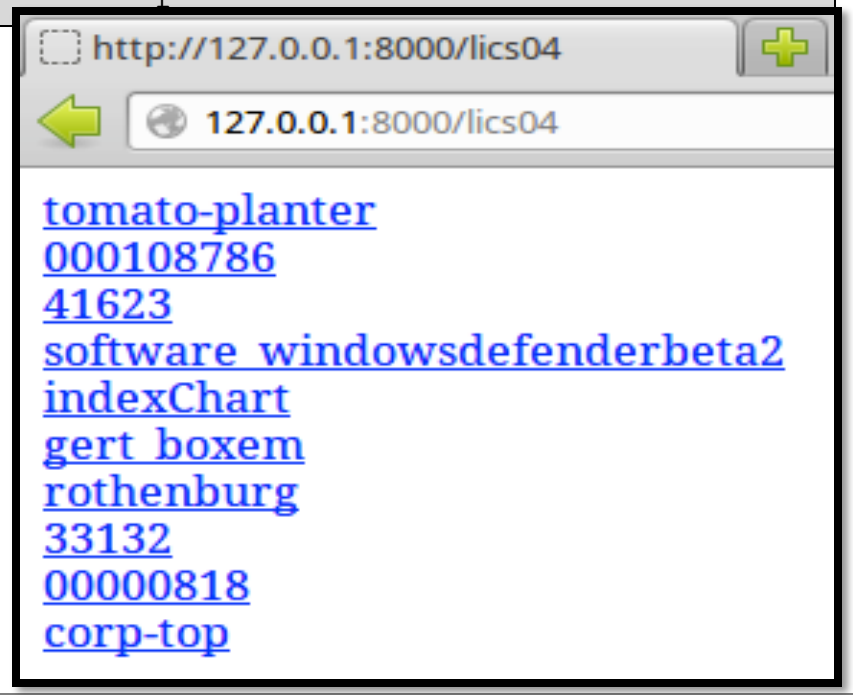
Lab: Spidertrap - Passing in a Directory List

- 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)

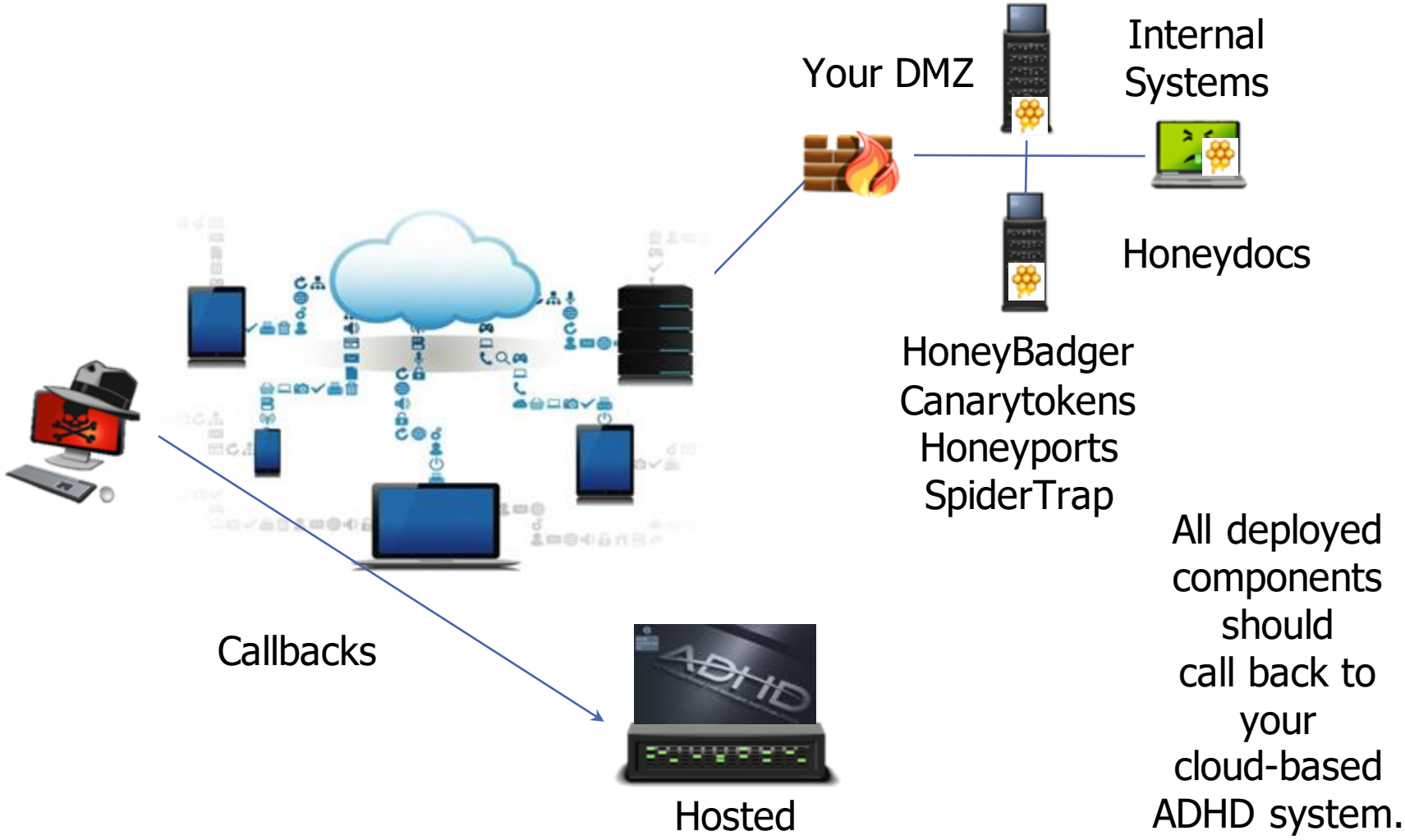
Burner Phones

- 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 warrant
- 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 (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.

PowerShell Honeyports!

- Get it here:
- https://github.com/gfoss/PowerShell-Honeyport
- Save to the C:\tools directory

https://github.com/gfoss/PowerShell-Honeyport

Product Team Enterprise Explore Marketplace Pricing Search Sign in Sign up

gfoss / PowerShell-Honeyport Public

forked from Pwdrkeg/honeyport

Notifications Fork 23 Star 6

Code Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Code

This branch is 1 commit ahead, 2 commits behind Pwdrkeg/honeyport:master. Contribute

gfoss Added Termination Function ... e954a83 on Jun 24, 2015 9 commits

README.md	Log Only Option	7 years ago
honeyport.ps1	Added Termination Function	7 years ago

README.md

.SYNOPSIS Block IP Addresses that connect to a specified port.

.DESCRIPTION Creates a job that listens on TCP Ports specified and when a connection is established, it can either simply log or add a local firewall rule to block the host from further connections. Writes blocked/probed IPs to the event log named HoneyPort.

.PARAMETER Ports List of Ports to listen in for connections.

.PARAMETER WhiteList List of IP Addresses that should not be blocked.

.EXAMPLE Example monitoring on different ports PS C:> .\honeyport.ps1 -Ports 70,79 -Verbose

.EXAMPLE Example monitoring on different ports and add whitelist of hosts PS C:> .\honeyport.ps1 -Ports 4444,22,21,23 -WhiteList 192.168.10.1,192.168.10.2 -Verbose

.EXAMPLE Example monitoring on one port and blocking on full TCP connect PS C:> .\honeyport.ps1 -Ports 21 -Block

.NOTES Authors: John Hoyt, Carlos Perez Original Script Modified By: Greg Foss

About

A powershell script for creating a Windows honeyport.

Readme
6 stars
1 watching
23 forks

Releases

No releases published

Packages

No packages published

Languages

PowerShell 100.0%

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