



DEFENSESTORM

Threat & Vulnerability Management

Bob Thibodeaux

Director – Security Operations, DefenseStorm

Bob@DefenseStorm.com



- Founded in 2014
- Designed for Credit Unions and Community Banks
- **Security Data Platform:** Watches everything on your network and matches it to your policies, ensuring that you are both secure and compliant

Vulnerability & Penetration Testing

Does your organization...

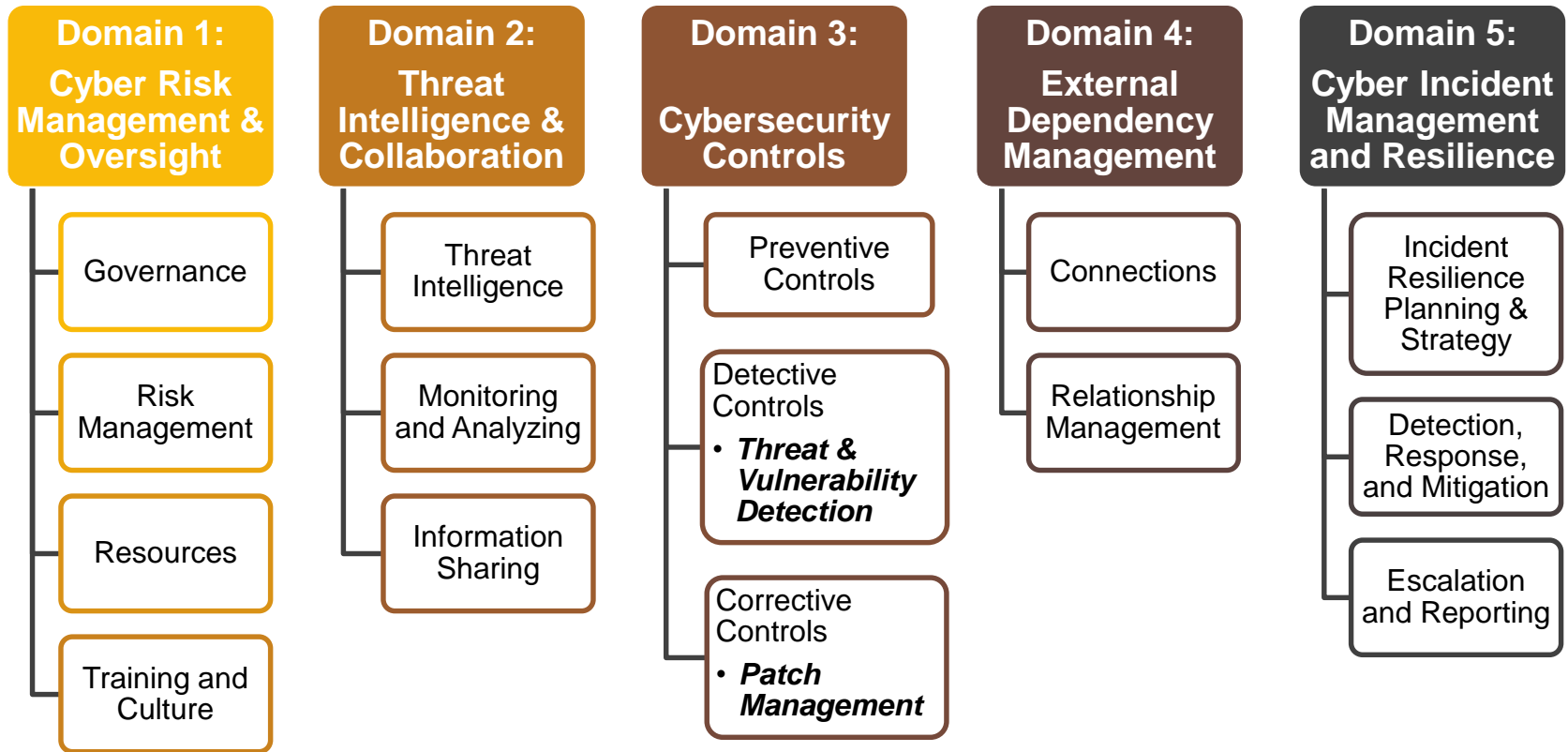
- Have a Threat and Vulnerability Program in place?
- Understand the consequences when if a Threat and Vulnerability Program is not in place?
- Know how to get started to build such a program?



Agenda

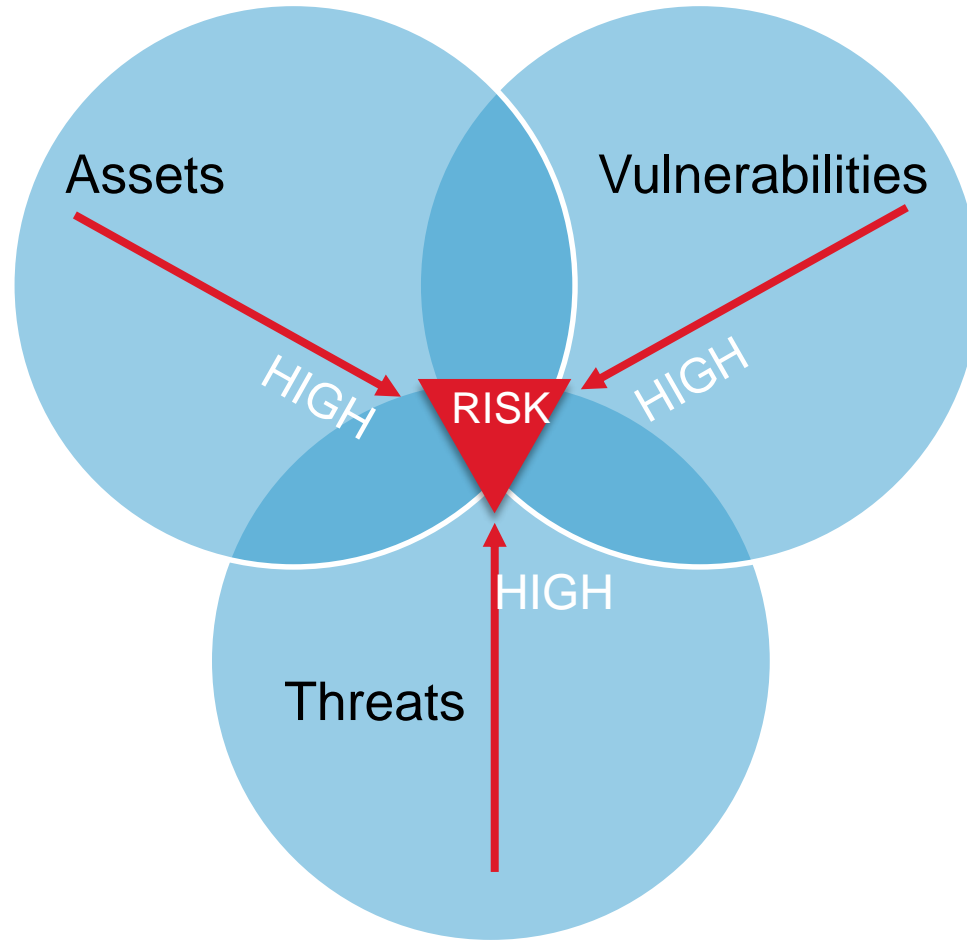
- FFIEC Cybersecurity Domains
- Threat Actors
- Cyber Kill Chain & Exploit Example
- Insider View of the Network
- Threat & Vulnerability Management

FFIEC Cybersecurity Domains



Threat & Vulnerability Management

Risk Management Function



Threat Actors

Who are they and what are their motives?

Cyber Criminals

Financial Gain

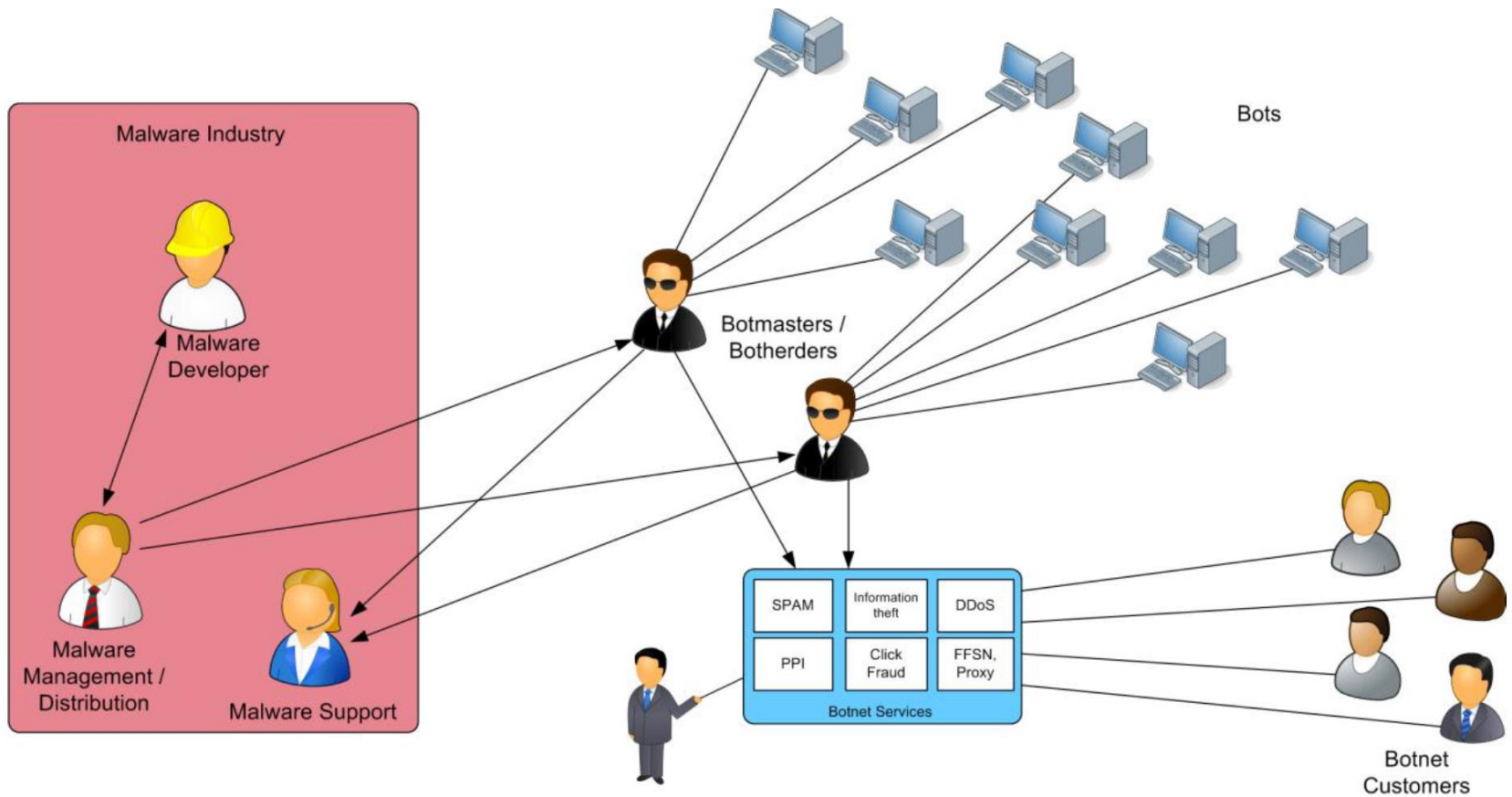


Figure 5: Simplified role model of the malware economy.

State-sponsored Actors

Espionage

THREAT Toons™

by: Alex Savchuk




Olympic Hacking

Hacktivists

Ideology

Operation OPICARUS: Anonymous & Ghostsquad Alliance

- Hacktivists Shut Down Central Bank of Cyprus with DDoS Attack
- Hacktivists Shut Down 3 More Banking Websites
- *Anonymous* Takes Down 9 Banks in 30-day Cyberattack



"We must strike at the heart of their empire by once again throw (sic.) a wrench into the machine, but this time we face a much bigger target – the global financial system. This time our target is the Global Banking Cartel as a whole.

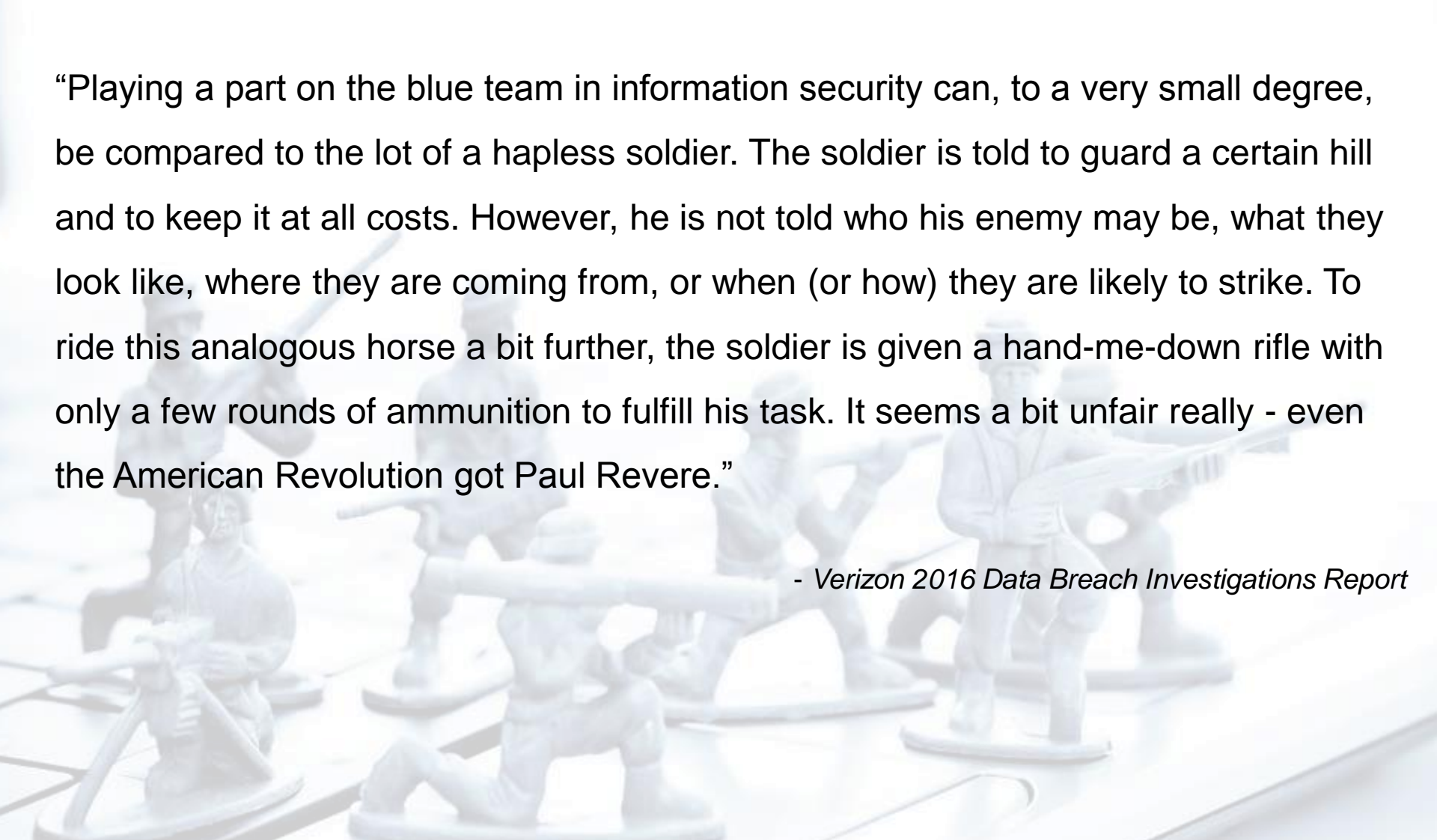
*We are anonymous. We are legion.
We do not forgive. We do not forget.
Operation Icarus, engaged.
Expect us."*

Anonymous on Operation Icarus

Insiders

Malicious or Accidental





“Playing a part on the blue team in information security can, to a very small degree, be compared to the lot of a hapless soldier. The soldier is told to guard a certain hill and to keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike. To ride this analogous horse a bit further, the soldier is given a hand-me-down rifle with only a few rounds of ammunition to fulfill his task. It seems a bit unfair really - even the American Revolution got Paul Revere.”

- Verizon 2016 Data Breach Investigations Report

THE BLUE TEAM MUST BE A NINJA FORCE



The Cyber “Kill Chain”

Reconnaissance

- Harvesting email address, social networking, port scans

Weaponization

- Coupling exploit with backdoor into deliverable payload

Delivery

- Delivering weaponized bundle to the victim via email, web, USB, etc.

Exploitation

- Exploiting a vulnerability to execute code on victim system

Installation

- Installing malware on the asset

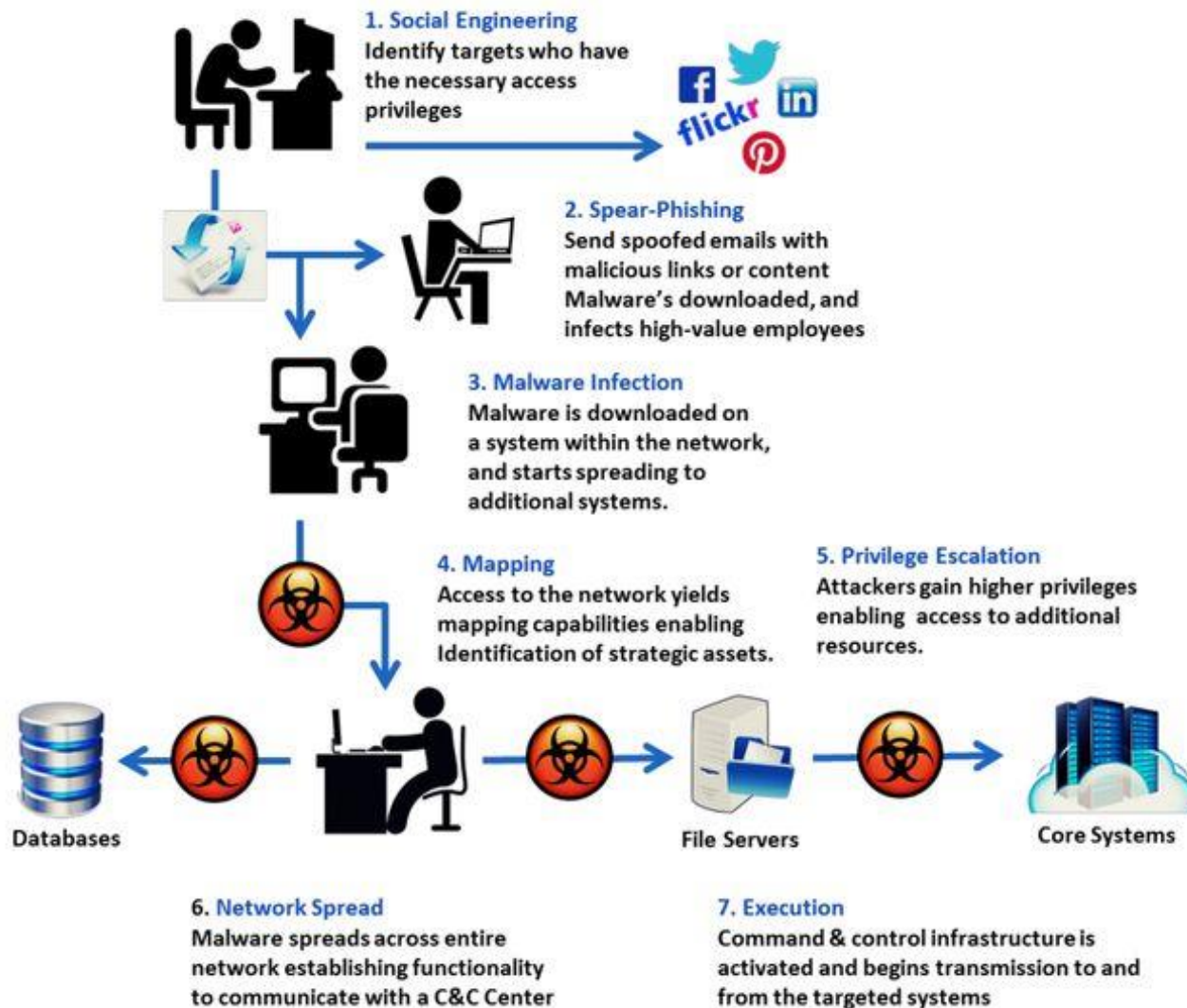
Command & Control

- Command channel for remote manipulation of the victim

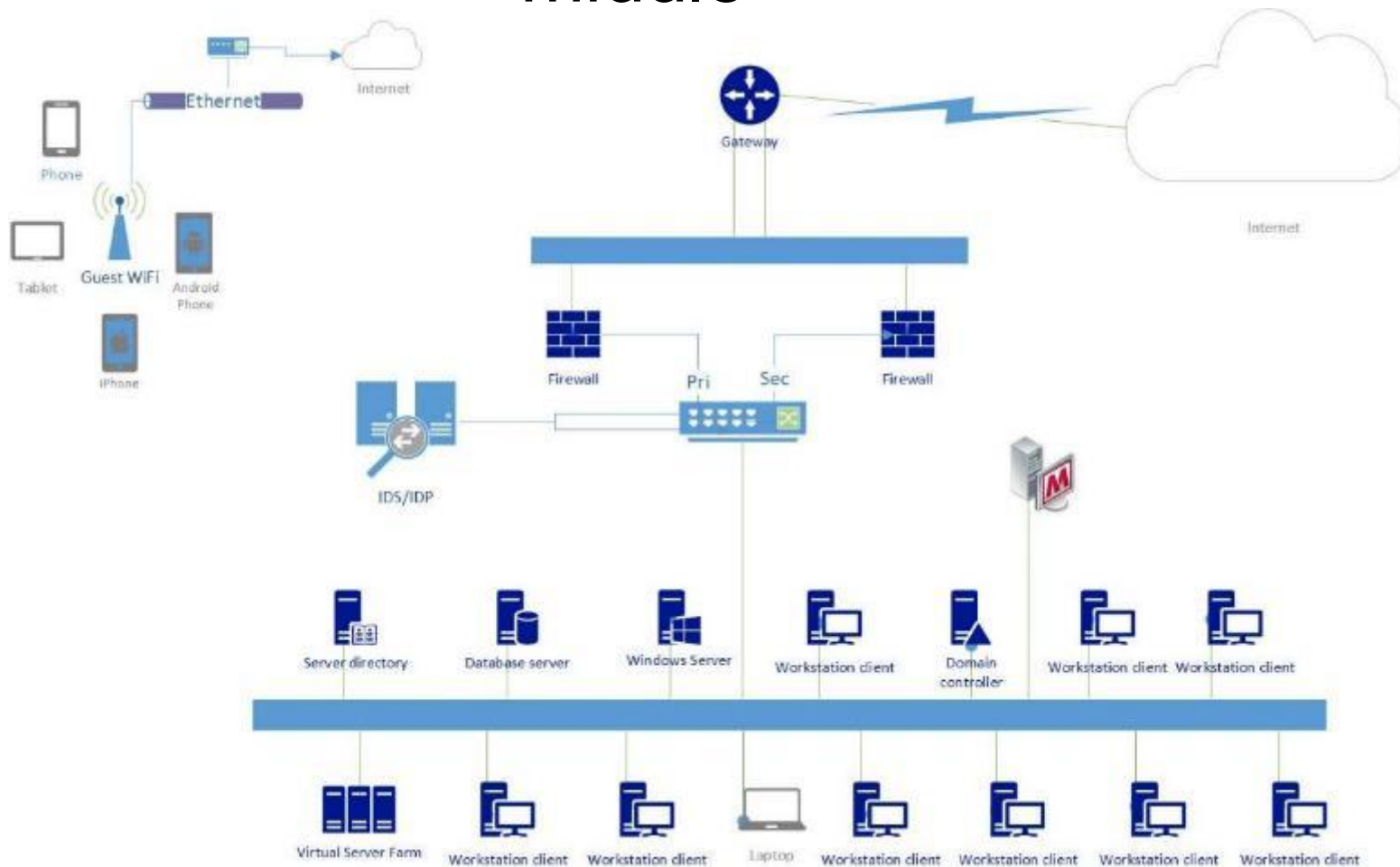
Actions on Target

- With “Hands on Keyboard” access, intruders accomplish goal

The Seven Steps of an APT Attack



Now that we are in--soft in the middle



A Predator's Assessment



"Oh, hey! I love these things!...Crunchy on the outside and chewy center!"

NMAP—Network Mapping Tool Output

Starting Nmap 7.01 (<https://nmap.org>) at 2016- -04 07:52 PST

Nmap scan report for

Host is up (0.0035s latency).

Not shown: 98 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 5.4 (protocol 2.0)
--------	------	-----	----------------------------

443/tcp	open	ssl/http	SonicWALL firewall http config
---------	------	----------	--------------------------------

MAC Address: 00:17: : : (SonicWALL)

Aggressive OS guesses: SonicWALL SonicOS Enhanced 5.2 (96%), Apple AirPort Express WAP or AMX NI-3100 controller (VxWorks) (93%), SonicWALL NSA 220 firewall (SonicOS Enhanced 5.8) (93%), Asus RT-AC66U router (Linux 2.6) (90%), Asus RT-N16 WAP (Linux 2.6) (90%), Asus RT-N66U WAP (Linux 2.6) (90%), Tomato 1.28 (Linux 2.6.22) (90%), Ricoh Aficio SP 4100N printer (89%), SonicWALL TZ 190 firewall (SonicOS Enhanced 4.0) (88%), Xerox ApeosPort-IV C3370 printer (88%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Device: firewall

User View via Web Interface



The screenshot shows the SonicWall Network Security Login web interface. At the top, there is a dark blue header with the SonicWall logo on the left and the text "Network Security Login" on the right. Below the header, the main content area is white with a decorative wavy pattern in the background. The login form consists of three input fields: "Username:" with a text box, "Password:" with a text box, and "Language:" with a dropdown menu currently set to "English". Below these fields is a "Login" button. In the bottom right corner, there is a link that says "Click [here](#) for sslvpn login".

Default account is admin & password

NMAP—Network Mapping Tool Output

```
Nmap scan report for [REDACTED]
Host is up (0.0089s latency).
Not shown: 91 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http            Microsoft IIS httpd 5.0
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows 98 netbios-ssn
443/tcp   open  https?
445/tcp   open  microsoft-ds   Microsoft Windows 2000 microsoft-ds
1025/tcp  open  msrpc           Microsoft Windows RPC
1026/tcp  open  LSA-or-nterm?
1027/tcp  open  msrpc           Microsoft Windows RPC
1433/tcp  open  ms-sql-s       Microsoft SQL Server 2000 8.00.194; RTM
MAC Address: 00:13:[REDACTED]:[REDACTED]:[REDACTED] (Dell)
Device type: general purpose
Running: Microsoft Windows 2000
OS CPE: cpe:/o:microsoft:windows_2000::sp4
OS details: Microsoft Windows 2000 SP4
Network Distance: 1 hop
Service Info: OSs: Windows, Windows 98, Windows 2000; CPE:
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98,
cpe:/o:microsoft:windows_2000
```




End-of-life Windows and SQL

Vulnerability Scanner Results

Summary

Critical	High	Medium	Low	Info	Total
3	1	5	1	39	49

Details

Severity	Plugin Id	Name
Critical (10.0)	11214	MS02-061: Microsoft SQL Server Multiple Vulnerabilities (uncredentialed check)
Critical (10.0)	15910	Microsoft W3Who ISAPI w3who.dll Multiple Remote Vulnerabilities
Critical (10.0)	47709	Microsoft Windows 2000 Unsupported Installation Detection
High (7.5)	34460	Unsupported Web Server Detection
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	56210	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials
Medium (5.0)	56211	SMB Use Host SID to Enumerate Local Users Without Credentials
Medium (5.0)	57608	SMB Signing Disabled

Enum--Windows Tool Output

Active Directory Password Policy (unauthenticated)

```
enum -U -P 192.168.X.14
server: 192.168.X.14
setting up session... success.
password policy:
  min length: 8 chars
  min age: 30 days
  max age: 90 days
  lockout threshold: 5 attempts
  lockout duration: 60 mins
  lockout reset: 60 mins
```

NMAP—Network Mapping Tool Output

```
Nmap scan report for [REDACTED]
Host is up (0.0026s latency).
Not shown: 94 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    closed ssh
80/tcp    open  http        VMware ESXi Server httpd
427/tcp   open  svrloc?
443/tcp   open  ssl/http    VMware ESXi Server httpd
8000/tcp  open  http-alt?
8080/tcp  closed http-proxy
MAC Address: 14:02:[REDACTED]:[REDACTED]:[REDACTED]:[REDACTED] (Hewlett Packard Enterprise)
Aggressive OS guesses: VMware ESXi 6.0.0 (96%), VMware ESXi 5.0 - 5.5
(96%), VMware ESXi 5.5 (94%), VMware ESXi 4.1 (92%), Crestron XPanel
control system (92%), FreeBSD 7.0-RELEASE-p1 - 10.0-CURRENT (92%),
FreeBSD 5.3 - 5.5 (90%), FreeNAS 0.686 (FreeBSD 6.2-RELEASE) or VMware
ESXi Server 3.0 - 4.0 (90%), FreeBSD 8.0-RELEASE (90%), VMware ESX
Server 4.0.1 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: [REDACTED]; CPE:
cpe:/o:vmware:esxi
```


Vulnerability Scan Report

Summary

Critical	High	Medium	Low	Info	Total
2	2	4	2	26	36

Details

Severity	Plugin Id	Name
Critical (10.0)	86947	VMware ESXi 5.5 < Build 3029944 OpenSLP RCE (VMSA-2015-0007)
Critical (10.0)	88906	ESXi 5.5 < Build 3568722 / 6.0 < Build 3568940 glibc DNS Resolver RCE (VMSA-2016-0002) (remote check)
High (8.5)	86122	OpenSSH MaxAuthTries Bypass
High (7.1)	81085	ESXi 5.5 < Build 2352327 Multiple Vulnerabilities (remote check) (POODLE)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.6)	87942	ESXi 5.5 < Build 3248547 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

NMAP—Network Mapping Tool Output

```
Nmap scan report for [REDACTED]
Host is up (0.0044s latency).
Not shown: 97 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Mocana NanoSSH 5.3.1 (protocol 2.0)
23/tcp    open  telnet
80/tcp    open  http     eHTTP 2.0 (HP switch http config)
MAC Address: 40:A8:[REDACTED]:[REDACTED]:[REDACTED]:[REDACTED] (Hewlett Packard)
Device type: switch
Running: HP embedded
OS CPE: cpe:/h:hp:switch_2530 cpe:/h:hp:switch_2920
cpe:/h:hp:switch_5406z1
OS details: HP 2530, 2920, or 5406z1 switch|
Network Distance: 1 hop
Service Info: Device: switch
```

User View via Web Interface

The screenshot displays the HP Web Management Platform interface for configuring a port. The left sidebar shows the navigation menu with 'Network' and 'VLAN' highlighted. The main content area is titled 'Web Management Platform' and shows the 'Modify Port' configuration page. The 'Modify Port' button is highlighted in the top navigation bar. The 'Select Ports' section shows a grid of ports for an HP V1910-24G switch. The 'Select membership type' section has 'Untagged' selected. The 'Selected ports' section shows 'Untagged Membership'.

Configured with no authentication

Vulnerability Scan Report

Summary

Critical	High	Medium	Low	Info	Total
0	1	2	2	18	23

Details

Severity	Plugin Id	Name
High (7.5)	41028	SNMP Agent Default Community Name (public)
Medium (5.8)	42263	Unencrypted Telnet Server
Medium (5.0)	76474	SNMP 'GETBULK' Reflection DDoS
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled

SNMPWalk Command Line Output

ASN 1 Notation anyone?

```
SNMPv2-SMI::enterprises.77.1.2.18.0 = Counter32: 0
SNMPv2-SMI::enterprises.77.1.2.19.0 = INTEGER: 0
SNMPv2-SMI::enterprises.77.1.2.21.0 = INTEGER: 0
SNMPv2-SMI::enterprises.77.1.2.22.0 = INTEGER: 15
SNMPv2-SMI::enterprises.77.1.2.24.0 = INTEGER: 5
SNMPv2-SMI::enterprises.77.1.2.25.1.1.5.71.117.101.115.116 = STRING: "Guest"
SNMPv2-SMI::enterprises.77.1.2.25.1.1.6.116.101.115.116.120.112 = STRING: "testx
p"
SNMPv2-SMI::enterprises.77.1.2.25.1.1.13.65.100.109.105.110.105.115.116.114.97.1
16.111.114 = STRING: "Administrator"
SNMPv2-SMI::enterprises.77.1.2.25.1.1.13.72.101.108.112.65.115.115.105.115.116.9
7.110.116 = STRING: "HelpAssistant"
SNMPv2-SMI::enterprises.77.1.2.25.1.1.16.83.85.80.80.79.82.84.95.51.56.56.57.52.
53.97.48 = STRING: "SUPPORT_388945a0"
SNMPv2-SMI::enterprises.77.1.2.26.0 = INTEGER: 0
SNMPv2-SMI::enterprises.77.1.2.28.0 = INTEGER: 0
SNMPv2-SMI::enterprises.77.1.3.1.0 = Counter32: 0
SNMPv2-SMI::enterprises.77.1.3.2.0 = Counter32: 0
SNMPv2-SMI::enterprises.77.1.3.3.0 = Counter32: 0
SNMPv2-SMI::enterprises.77.1.3.4.0 = Counter32: 0
SNMPv2-SMI::enterprises.77.1.3.5.0 = Counter32: 0
SNMPv2-SMI::enterprises.77.1.3.7.0 = INTEGER: 0
SNMPv2-SMI::enterprises.77.1.4.1.0 = STRING: "WORKGROUP"
End of MIB
root@bt:~# _
```

Getting Started

The Foundation for Threat &
Vulnerability Management

FFIEC Domains

Threat & Vulnerability Management

FFIEC Domain	Baseline/Evolving	Advanced/Innovative
3. Cybersecurity Controls: Preventative Controls--Threat & Vulnerability Detection	E-Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices	A-Vulnerability scanning is rotated among environments to scan all in a year cycle. I—Vulnerability scanning is performed weekly across all environments.
3. Cybersecurity Controls: Corrective Controls—Patch Management	<p>B-A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. Patch testing before deployment. Patch management reporting.</p> <p>E-A formal process is in place to acquire, test, and deploy software patches based on criticality. Systems are configured to retrieve patches automatically.</p>	<p>A-Patch monitoring software is installed on all servers to identify any missing patches for the operating system software, middleware, database, and other key software.</p> <p>The institution monitors patch management reports to ensure security patches are tested and implemented within aggressive time frames (e.g., 0-30 days).</p>

Network & Port Scanning



Regular network and port scanning can be simple

Nmap can be used to scan your network(s) daily or weekly

Convert .nmap text format to CSV using Nmap to CSV script

Import into your favorite spreadsheet program

Sort/Report away

Network & Port Scanning



Verify your scan results to look for unsecure protocols or services

Telnet	FTP	Rsync	SNMP version 1 or 2	Unnecessary services exposed
--------	-----	-------	---------------------------	------------------------------------

Vulnerability Scanning



Weekly Scanning Using OpenVAS or Nessus

- Authenticated scans using agent on hosts is best option (Not required)
- Configure weekly scans to occur at the same day/time each week
- Schedule the time to optimize scanning (all hands on deck)
- Reports can be created in PDF, CSV in summary or detail
- Remediate all critical/high vulnerabilities first
- Then perform risk assessment on the medium and lower vulnerabilities

Risk Treatment Options Include Risk Acceptance

- Some vulnerabilities are not being exploited in the wild
- Consider exposure as well as vulnerability rating



External Systems Vulnerability Scan Options

- Pen Testing Vendor/Partner (Periodic)
- Qualys SSL Server Testing Site (Free)



What to Patch? Not Everything!

...Remember this is a risk management process

Sunset end of life systems! (Windows XP, Server 2003, etc.)

Restrict use of Adobe Flash Player & Quicktime for Windows

Threat & Vulnerability Management

- Participate in Patch Tuesday and out of cycle updates for Windows

- Patch these non-Windows applications always:

- Oracle Java
- Adobe Acrobat Reader
- Firefox (Mozilla)
- Chrome
- Your Browser



<https://www.uscert.gov/ncas/alerts/TA15-119A>

Threat & Vulnerability Management

External Systems

OpenSSL, SSL/TLS, Weak RSA key exchange, etc.

SSH Signal Handling, SSH v1

Windows HTTP.sys Vulnerability

Apache HTTP Server

End of life PHP

Physical Security

Protecting the Data Center
& Other Critical
Infrastructure

Threat & Vulnerability Management

Facilities Security



Threat & Vulnerability Management

Facilities Security Attack Tools

- Covert systems administration from anywhere
- Small form factor computer with full scripting capabilities
- Supports Metasploit attack platform



Threat & Vulnerability Management

Facilities Security Attack Tools

- Keystroke injection attack platform
- Small form factor computer with full scripting capabilities
- Seen as a USB Keyboard by most operating systems

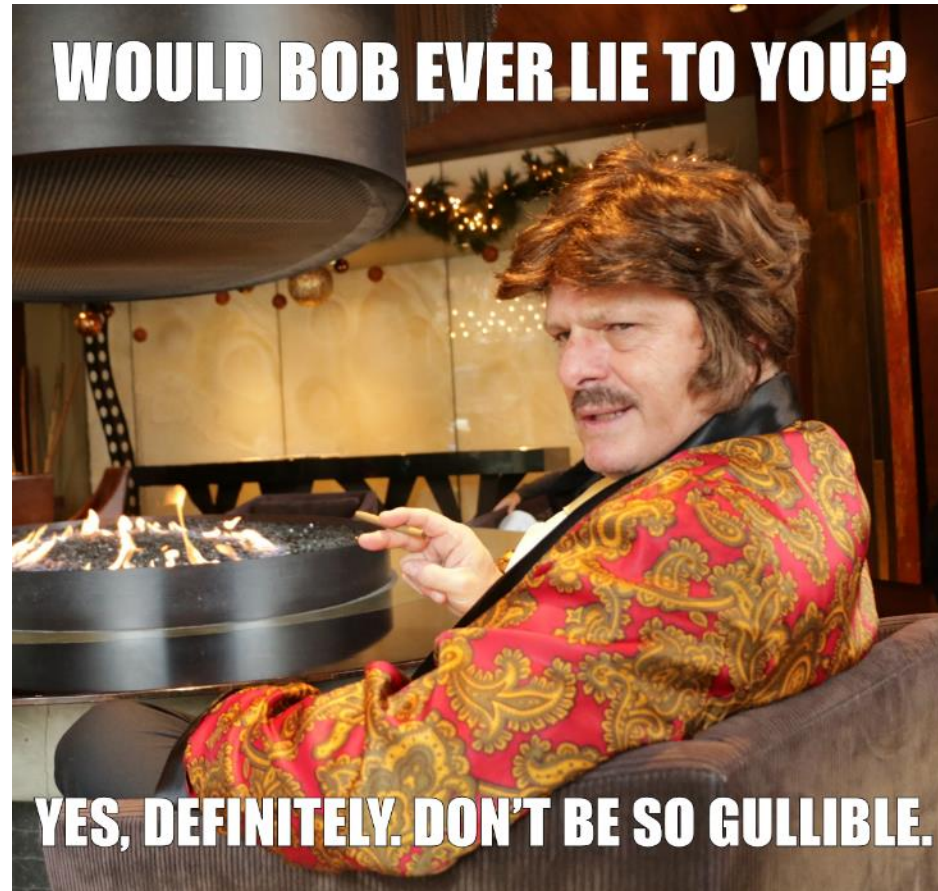


Summary



- FFIEC Cybersecurity Domains
- Threat Actors
- Cyber Kill Chain & Exploit Example
- Insider View of the Network
- Threat & Vulnerability Management

Questions?



Appendix 1--Tools & Reference



- Open Source

- Kali Linux 2016.2—Security Tools (www.kali.org)
- Nmap—The Network Mapper (<https://nmap.org>)
- OpenVAS—Vulnerability Scanner (www.openvas.org)
- Enum—Windows Enumerator (www.microsoft.com)
- NmaptoCSV—Converts NMAP file format to CSV (<https://github.com/maaaaz/nmaptocsv>)

Appendix 1--Tools & Reference



- Commercial
 - GFI Languard
 - Tenable Nessus
 - ManageEngine-Desktop Central
 - Pwnie Express—Pwnie Pulse
 - USB Rubber Ducky (hak5.org)
 - LAN Turtle (hak5.org)



Questions?



DEFENSESTORM