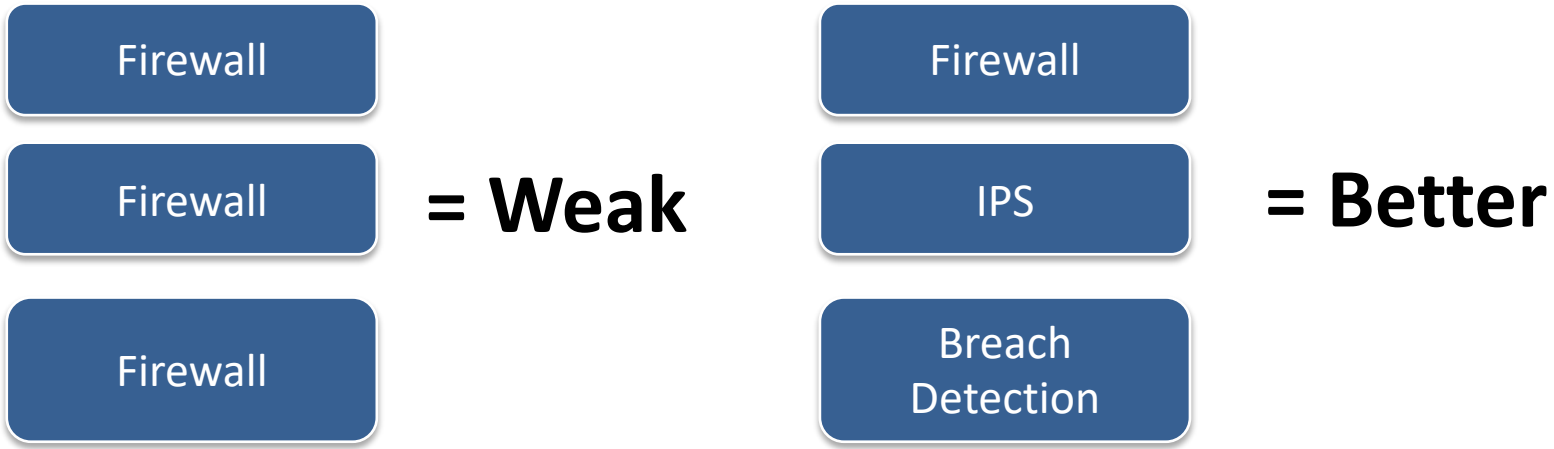
CompTIA Cybersecurity Analyst+ (CySA+)
Day 2

Security Architectures

Pearson

Defense in Depth

- Layering defenses
- Best practice use different capabilities according to kill chain
- Should apply to all areas of network



Defense in Depth

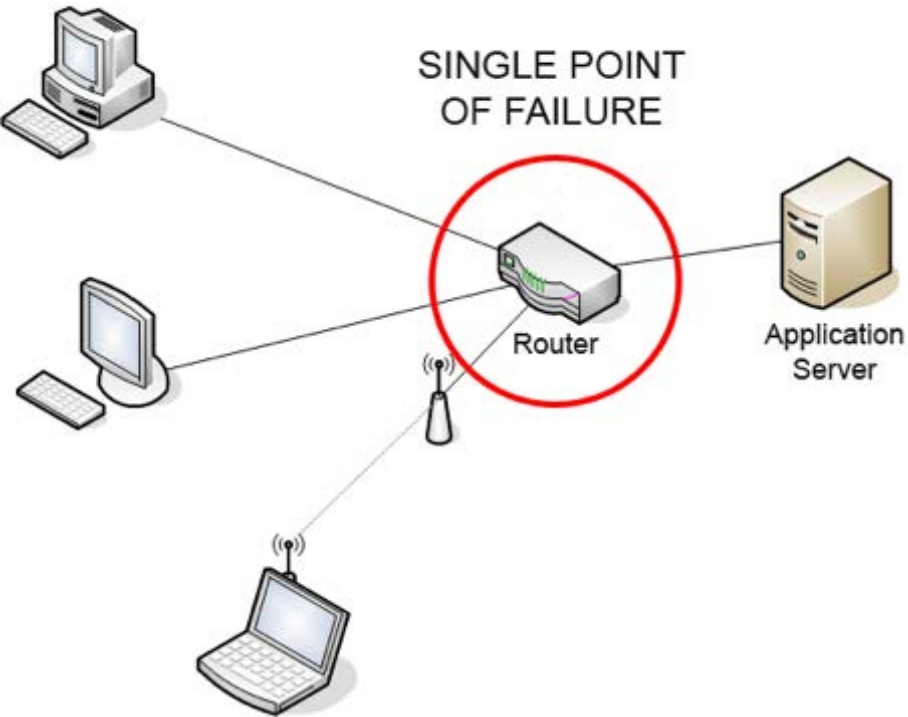
- Leverage different security levels when using the same technology

Perimeter Firewall	**Trust 0 outside | 50 DMZ | 100 inside**
Internal Firewall	**Segment employees, HR, Guests, etc.**
Data center Firewall	**Segment data center resources / applications**

Identifying Threats 101

- Signature Analysis - Known threats
- Trend Analysis – Large-scale changes to baseline (typically not security related)
- Heuristic Analysis – Behavior focused for unknowns
- Regression Analysis – Statistical modeling (X Y scale)
- Anomaly Analysis – Difference from established patterns

Single Point of Failure



- Remediate with redundant systems
- Add different routes and system types
- The more difference, the more HA

Ex) Joey needs to ensure a vulnerability in this router isn't abused. Best would be having a second network with different vender router for HA but likely too costly.

Whitelisting and Blacklisting

- Blacklisting – Blocking specific software from being installed
- Whitelisting – Prevents software that is not on a preapproved list
- Signature based – One specific threat

Network Security Technology

- **Firewall** – North South / East West
- **Content Filters / Application Layer Firewalls** – User / Application Data
- **Access Control** – Who and what is accessing network
- **IPS/IDS** – Signature and some behavior detection
- **Honey Pot** – Monitor traps
- **NetFlow** – Leverage network traffic for indications of compromise
- **Network Baselines** – Tools used to verify normal and unknown traffic

Network Security Focus Concepts

Firewalls – Provide perimeter security around protected area

Network Access Control (NAC)

1) Limit network access to authorized systems and people.
2) Ensure systems meet security requirements

Segmentation – Isolate different Network

Detecting Network Threats

- Need method to see traffic
  - Inline – direct real-time live traffic
  - SPAN port – copy of traffic

Attackers do the same to sniff traffic!

Firewall 101

- **Packet Filter** – Simply checks the characters of each packet against firewall rules
- **Stateful Inspection** – Beyond packet filters also viewing state of connection. (What today's standalone firewalls do)
- **Next Gen** – Beyond stateful including applications, users and context
- **Web Application Firewall** – Specialized for web application attacks such as SQL injection and cross site scripting

Proxy vs. Application Layer Firewall

Proxies

- Internet bound ports (80, 443)
- Cache traffic
- Higher performance (example HTTPS decryption)

Application Layer Firewalls

- All ports and protocols
- View near real time traffic / no cache
- Typically part of “Next Gen” platforms

- Both typically offer security detection and content filtering capabilities
- Security value depends on model and installation

Application Layer Firewall (Next Gen)

- All ports and protocols
- View near real time traffic / no cache
- Typically part of “Next Gen” platforms
- Sometimes called UTM (with other features)

Palo Alto – Cisco Firepower – Checkpoint - Fortinet

Recommending Different Firewalls

Key Concept

Network Firewall

- Port protection – Control what can come in and out
- Packet filtering, proxy and stateful packet inspecting network traffic

Host Firewall

- Program control – What the host computer can talk to
- Enforcing host security policies (example control what programs can talk to)

Web Application Firewall

- App controls - Intercept and mangle requests and responses to web applications
- Granular control for applications (Facebook games only vs. all of Facebook)
- Inspecting the XML/SOAP, HTTP/HTTPS and layer 7 attacks (SQL / XSS)

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

Intrusion Detection and Prevention

Signature Detection – Looking for known attack patterns
Threat Detection – Looking for malicious behavior
Anomaly Detection – Looking for unknown or unusual behavior

Intrusion Detection System = Passive (can't block attacks) and can be inline or off mirror port

Intrusion Prevention System = Can block attacks and must be deployed inline

Can be host (software) or network (appliance / virtual)

Detecting File Signatures Within Packets

- Looking for a specific file, action, content, etc.
- Scan packets for content i.e. **http contains "*something*"**
- File types have magic numbers
  - http://asecuritysite.com/forensics/magic

Example GIF = 47 49 46 39 as well as GIF8 will always be at start

http contains "\x47\x49\x46\x39" or http contains "GIF8"

77.72.118.168	192.168.47.171	HTTP	97 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
77.72.118.168	192.168.47.171	HTTP	97 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)

Know When To Recommend IPS

- Firewalls control traffic while IPS looks for attack behavior
- Blocking known threats from a “network view”. Host IPS would defend hosts but exam will probably view host threats as Anti-Virus
- Understand “North South” and “East West” recommendations
  - Internet-based attacks vs. internal attacks, like inside the Data Center

Host IPS

Signature Detection – Looking for known attack patterns
Threat Detection – Looking for malicious behavior
Anomaly Detection – Looking for unknown or unusual behavior

- **Typically deployed with Anti-Virus and other bundles**
- **Best Practices – Share threat data with network IPS**

Exam: Make sure question isn't Anti-Virus before selecting Host IPS

McAfee – Sophos – Symantec – ClamAV – etc.

Antivirus

File Base Signatures – Known malicious files
File Behavior – Some file analytics
File Modification Detection – Limited encoding detection

Typically older threats – Trojans, viruses, and worms

Targets KNOWN threats
Exam: Think host threats (malicious programs)

Antimalware

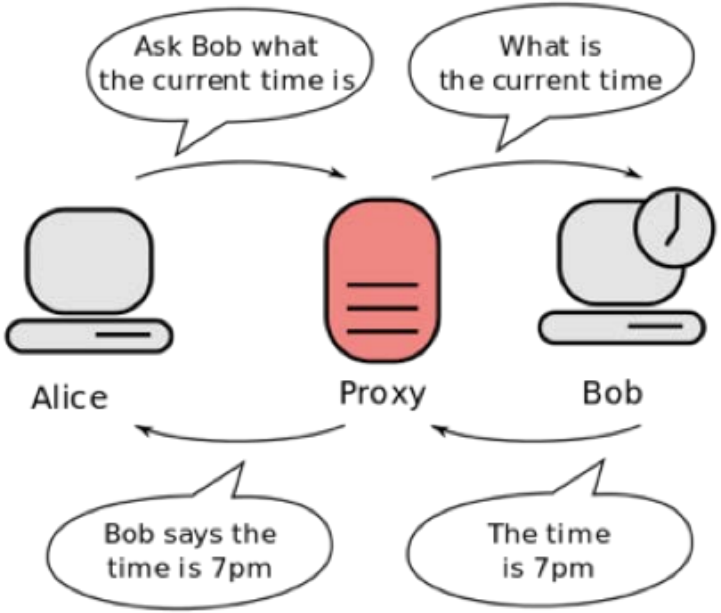
- Protects against infections caused by malware, viruses, worms, Trojan horses, rootkits, spyware, keyloggers, ransomware, and adware
- Typically more complete than antivirus (newer threats)
- May be called **File integrity** solution or **breach detection** on test

Virus – Code capable of copying itself and damages computer

Malware – Umbrella term for various malicious software

Intercepting Messages - Proxy

- Display and modify HTTP and WebSockets messages that pass between the proxy clients and web server.



Types of Proxies

- **Open Proxy** – Accessible by anybody on the Internet
  - Can conceal user IP
  - Typically done directly from host or using WCCP routing

- **Reverse Proxy** – Proxy appears to clients as ordinary server. Requests are forwarded to one or more servers, which handle requests

- **Man-in-the-middle** – Attacker captures traffic via ARP poisoning, going in-line, DNS spoofing, STP mangling, etc.

Common Architecture Challenges

Single Point of Failure

- High availability / redundant systems can remediate this

Users

- Layer 8 can't be controlled

Authentication and Authorization

- Multifactor authentication and account management can help

Data validation / Trust

- Validating data integrity can remediate it
- Include boundary checks and encryption

Maintaining Security Design

- Scheduled Review and Validation
- Continue Improvement
- Retirement of Process
  - Policy is no longer relevant
  - Suspend or replaced by newer policy
  - Policy needs to be removed

Enhanced Mitigation Experience Toolkit (EMET)

- Microsoft solution for extra malware defense
- Breach detection
- Free
- Behavior based plus other features such as address randomization (hard to target predictable places in memory)

Not as feature rich as enterprise breach technology

Microsoft Baseline Security Analyzer

- Assesses for missed security updates and less-secure security settings
  - Microsoft Windows, windows components (Internet explorer), SQL server, etc.

- **MBSA** only scans for missing security updates. Critical and optional updates not included.

Network Behavior Analysis

- Monitoring traffic and highlighting unusual actions

- Think beyond signature detection - Baselining

Example: Why is Bob is sales scanning the network for the first time? Could be an infection based on **action** … not signatures

Threat Intelligence

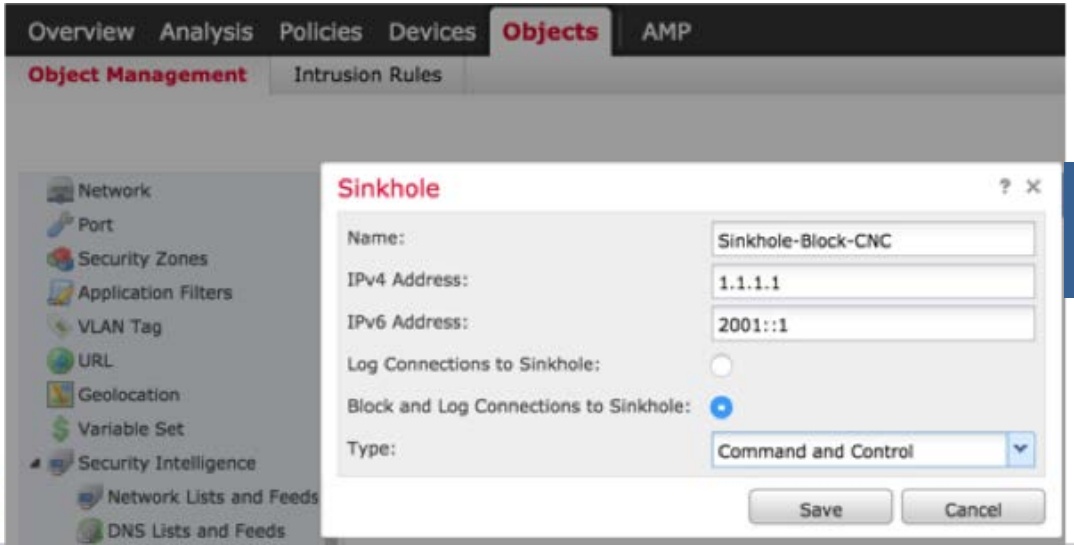
- Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging threat

- Think what "Other Networks" are seeing

Example: Other company data warned us about evil.exe and now raised to a critical threat when seen on our network

Botnet Sinkholes

- Devices that monitor network traffic
- Outgoing traffic to sinkholes is seen, hosts have been compromised
- Major security vendors setup sinkholes from reverse engineering malware or monitoring existing ones.



Change traffic going to bad external source to route here instead!

Routing Sinkholes

- Admins setup internal routing sinkholes to route unwanted traffic
- Many times, routing is sent to a null interface
- This is less processor intensive than blocking traffic

Same as botnet sinkhole but send other types of threats

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

Great for identifying UNKNOWN threats

Protecting Endpoints

- **Hardened Configuration** – Disable unnecessary services
- **Patch Management** – Close vulnerabilities
- **Group Policy (GP)** – Pushing security policy to many endpoints
- **Endpoint Security Software** – Antivirus, host IPS, etc.
- **Password Policies**
- **Host Firewalls**
- **File Integrity Checking –** Notifies changes in files

Know when to recommend these!

Identity

Identity Key Concepts

- Authentication – Who are you?
- Authorization – What can you access?
- Accounting – Record what you do
- Common called AAA

- Multifactor – Using different things to prove identity
- Centralized identity and access management (IAM)
- Directories – Control access level (example LDAP)

Authorization

- **What users can access**

- Could be controlled via VLAN, ACL, SGT, Application Rights, etc.
  - *Can you issue command or ping a server*

- Attackers target highest authorization!

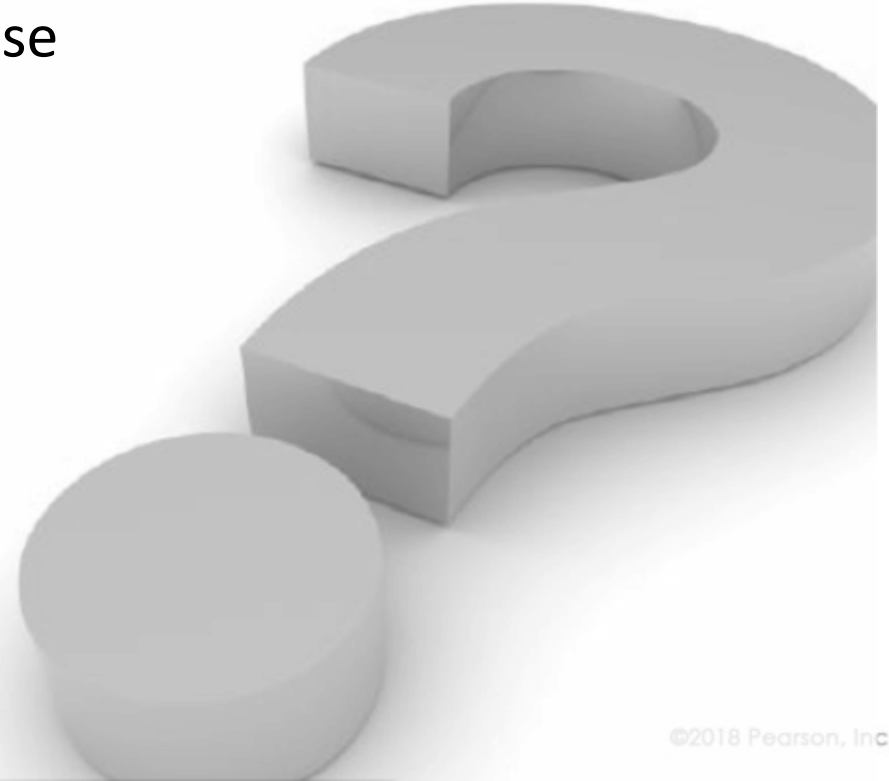
Accounting

- **Tracking what users did and services used**

- Importing for auditing
  - *Authorization control, billing, trend analysis, resource utilization and capacity planning*

Multi-Factor Authentication

- **Something You Know**
  - Password
  - Best Practice – Pass Phrase
- **Something You Have**
  - Token
  - Certificate
- **Something You Are**
  - Finger Print
  - Eye Scanner



Centralized Identity Management

Database / server storing user identity

Typically group into categories

- Employee, Admin, Contractor, HR, etc.

Multi-factor authentication could be used

Referenced by other technologies

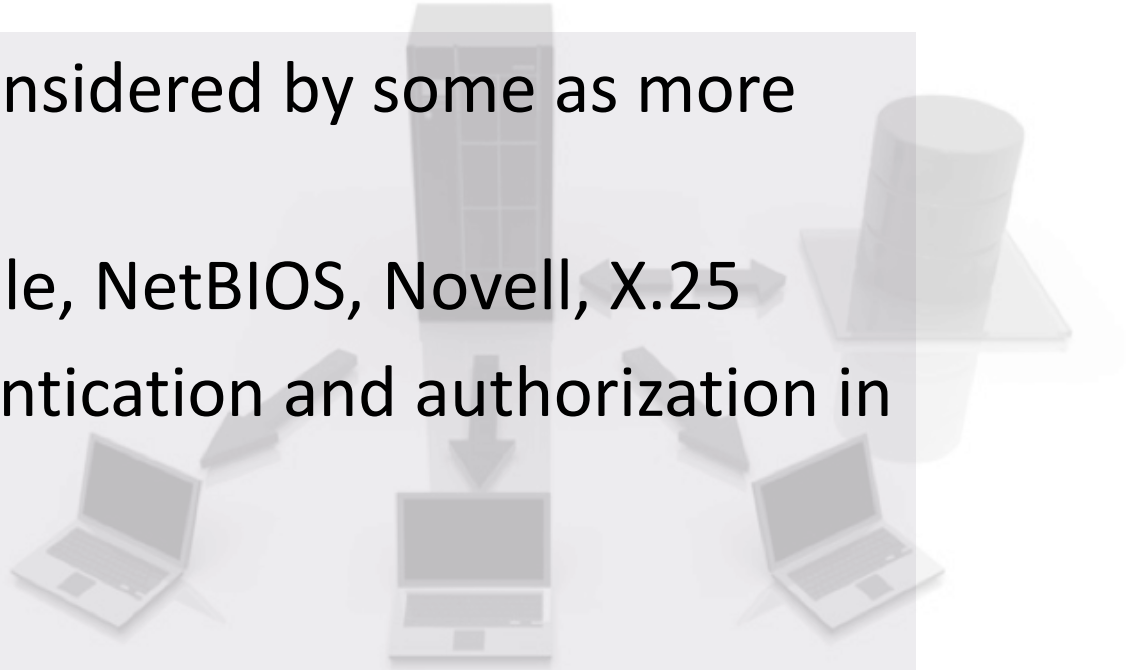
- Example – TACACTS+, Active Directory

Identity Repository Examples

- **Directory services** – Centralized repository for services distribution
- **TACACS+** - Family of protocols handling remote authentication and related services
- **RADIUS** – Centralized authentication, Authorization and Accounting
- **Kerberos** – Ticket based authorization system

TACACTS+

- Uses TCP and considered by some as more reliable
- Supports IP, Apple, NetBIOS, Novell, X.25
- Separates authentication and authorization in a user profile
- Packet payload



Radius

- Uses UDP and IP only
- 802.1x communicates using RADIUS
- Combines authentication and authorization in a user profile
- Often backend for 802.1x
- Password only

Protect Radis with TLS (same for others such as LDAP)

NOTE: SSL is outdated

Note: MD5 and SHA1 are hashing not authentication

Kerberos

- Ticket granting system granting what you can access
- Tickets expire and don’t contain credentials
- Designed for untrusted networks since you are not passing credentials as you are granted access

Note: Radius and authorize you on the network, then Kerberos can grant a ticket for what you can access.

Single Sign-on – Reduce Password Usage

- Login once and credentials passed onto different checkpoints
- **LDAP** and **CAS** (Central Authentication Service) are common
- **OpenID** – Open source standard for decentralized authentication
- **Oauth** – Open authorization standard
- **OpenID Connect** – Authentication Layer
- **Facebook Connect** – Sharing Facebook login to other systems

Shared Authentication

- OpenID Connect
- OAuth
- Facebook Connect

Common attacks against identity

- Impersonation – Act as you
- Man-in-the-middle – modify real identity during transit
- Session hijacking – Takeover authenticated session
- Cross-site scripting – Bypass authentication
- Privilege escalation – Gain unauthorized privileges
- Rootkits – Own system with root access

Example Attacks

- **Impersonation** – Abuse Oauth open redirect to take the identity of a legitimate user's access.
- **Session Hijack** – Attacker copies an authorized session and later pastes it in his/her browser to get access
- **Golden Ticket** – Own the AD system and serve yourself a lifetime pass
- **Cross-site scripting** – Place script on website that sends authorized session to the attacker
- **Pass the hash** – Session hijack where you copy while MiTM

LDAP and Kerberos Attacks

LDAP

- Insecure connections (bindings)
- Poor access control to directories
- Injection such as SQL Injection
- DoS

Kerbose

- Kerberos ticket reuse
- Ticket granting ticket (TGT) attacks
- Administration account attacks
- Golden ticket - lifetime ticket

Radius and AD Attacks

Radius

- Session replay
- Capture shared secret
- Attacking credentials
- DoS

Active Directory

- Stealing credentials
- Privilege escalation
- Domain right abuse
- Protocol abuse
- Malware
- Older version
- Service accounts

Defending Concepts

Kerberos or RADIUS IE Database

- ACLs to limit account or user access
- Protect server (segmentation, multifactor authentication, password rotation)

Oauth IE Motion

- TLS to encrypt traffic in motion
- Don’t use weaker SSL
- Prevent brute force

Permissions

Least Privileges Principle: Limit access to the minimal level that will allow normal functioning

- Only administrators access sensitive systems
- Only authorized systems (validate with certificates, MAC, etc.)
- Only authorized gold images
- Divide keys to kingdom between more than one user

File Permission

Example: Chmod 777 –Rv

set anything in folder to read / write / execute for owner, group and other. This means all security is being removed!

Example -rw-r--r-- 1 joey users 1892

(right to left) 1892 bits file, group users, user joey, 1 file, Joey can read / write, group and outsiders (RDP) are read only

File Permissions

Example: -rwxr-xr-x 1 root root

Only root group and owner exist for file. This file can be executed by group, file owner and others. Only root can write

Example -rwxr--r-- 1 root root

Only root, the owner of file can use this program. No permissions for any other user

Passwords

Pearson

Cracking Passwords 101

- Cracking tool has a word list or rainbow table
- The wordlist is hashed or encrypted
- The target hash is compared against hash list
- When match occurs, display the unencrypted word matching the hash

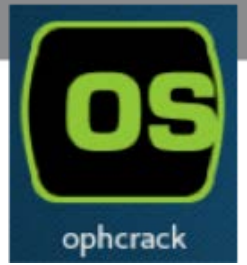
Hashes can be obtained by sniffing the network or directly from the Windows SAM (c:\windows\system32\config\SAM) or Linux shadow file.

Or you can use other tactics such as social engineering to trick users to enter their passwords in the clear.

Type of Password Attacks

- Dictionary Attack
- Brute Force Attack
- Rainbow Table Attack
- Phishing
- Social Engineering
- Malware
- Offline Cracking
- Guess

Cracking Password



Create Password Hash Example

- Echo –n “password phrase” | md5sum | tr –d “ –” >> hashes
- Or search the internet for “password hash generator”

Ophcrack

- Load hash or select single hash
- Select wordlist

Download tables from http://ophcrack.sourceforge.net/tables.php

John the Ripper

Open john using “john” or GUI option

John –w<optional word list> <media location>

```
root@kali:~# john -w:/media/root/SP/mangled.lst /media/root/SP/hashexample.txt
```

Show Results

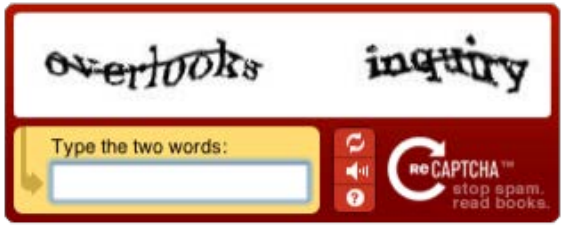
John —show <media location>

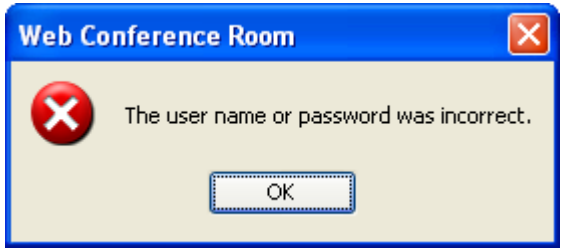
```
root@kali:~# john -show /media/root/SP/hashexample.txt
0 password hashes cracked, 6 left
root@kali:~#
```

Example Word List:
https://www.dropbox.com/s/igykysa87e8dth4/mangled.lst?dl=0

Defense Against Brute Force

- CAPTCHAs
- Login Throttling
- Failed Login Account Lockout
- Unique URLs
- Limit accepted IP ranges





Don’t return informative errors such as “wrong user name” or “wrong password”

Context-Based Authentication

Make decisions based on the user, system, or other information

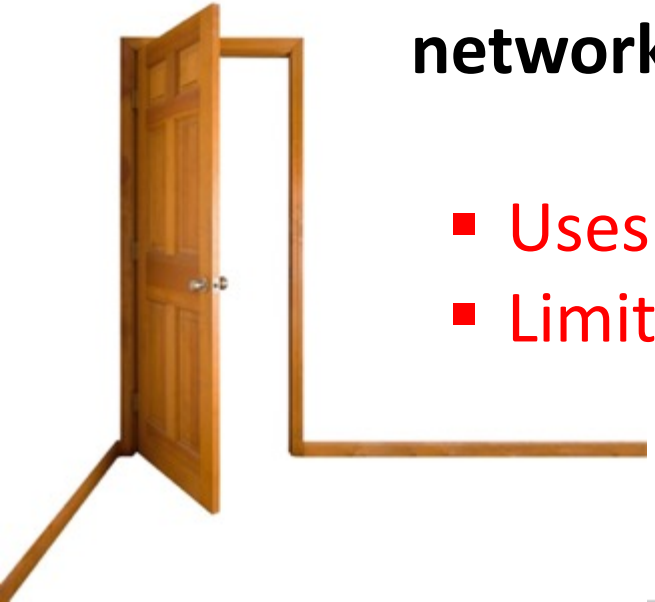
- User roles
- IP Address reputation
- Time of day

- Location check
- Frequency of access
- Device based

Access Control

Access Control

- **Basic concept** – Evaluate systems that access the network
- Typically not focused on systems **on the network**



  - Uses other technology (IPS, Breach)
  - Limited inside visibility

Manual Access Control Challenges

- Port Security is tough to deploy
  - Sticky MAC
  - Manual assign addresses
- Error disable for a violation
  - Manually reset port
- Security challenges
  - Spoofing MAC addresses
  - Missed ports
  - Reporting

Network Access Control Terminology

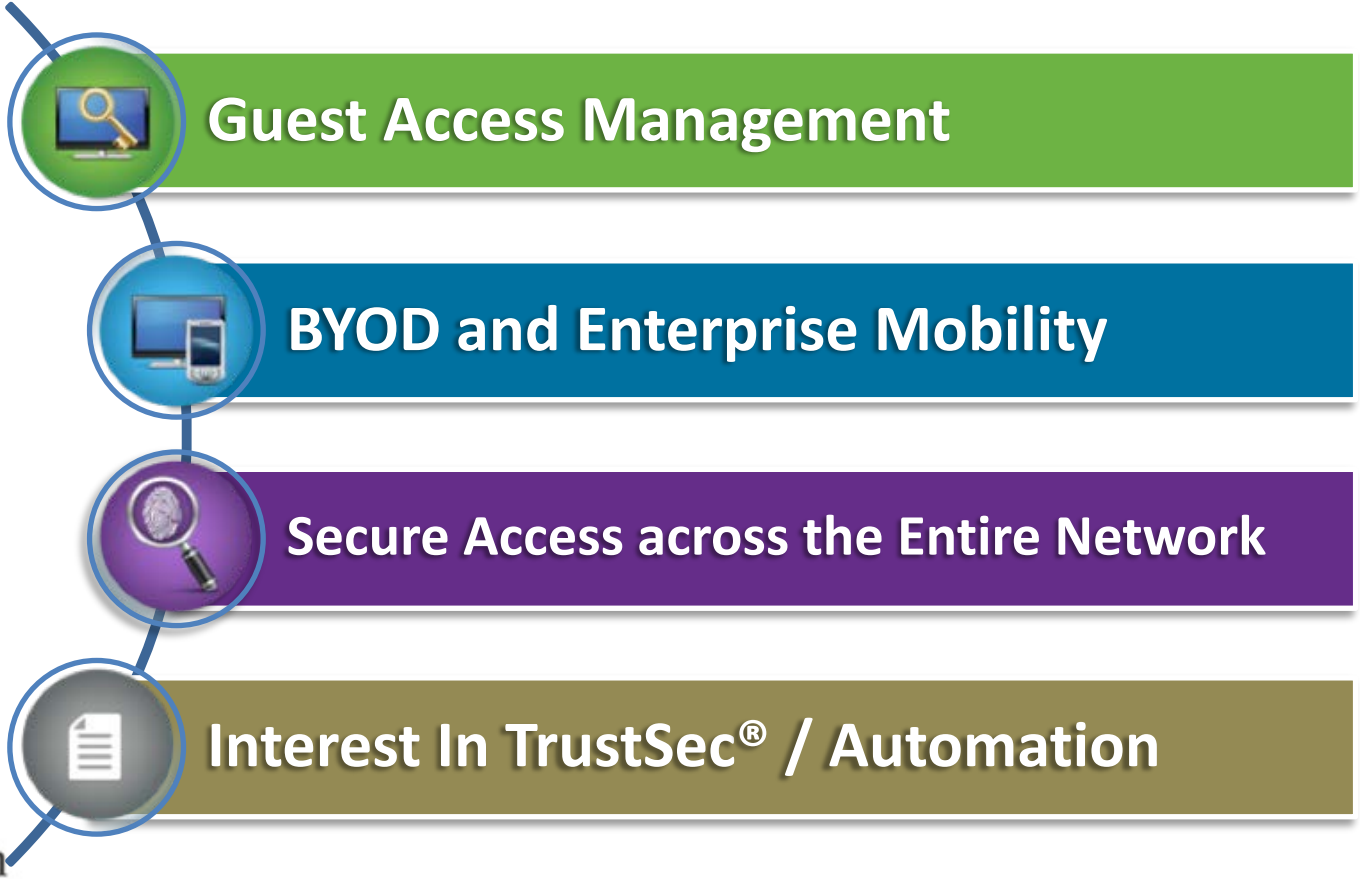
Port Security – Manual enable port controls on switch per port

Automated Access Control – Automatically adjust security
Options: SNMP, 802.1x, ARP Poisoning, other

Profiling – Examine traffic to fingerprint devices

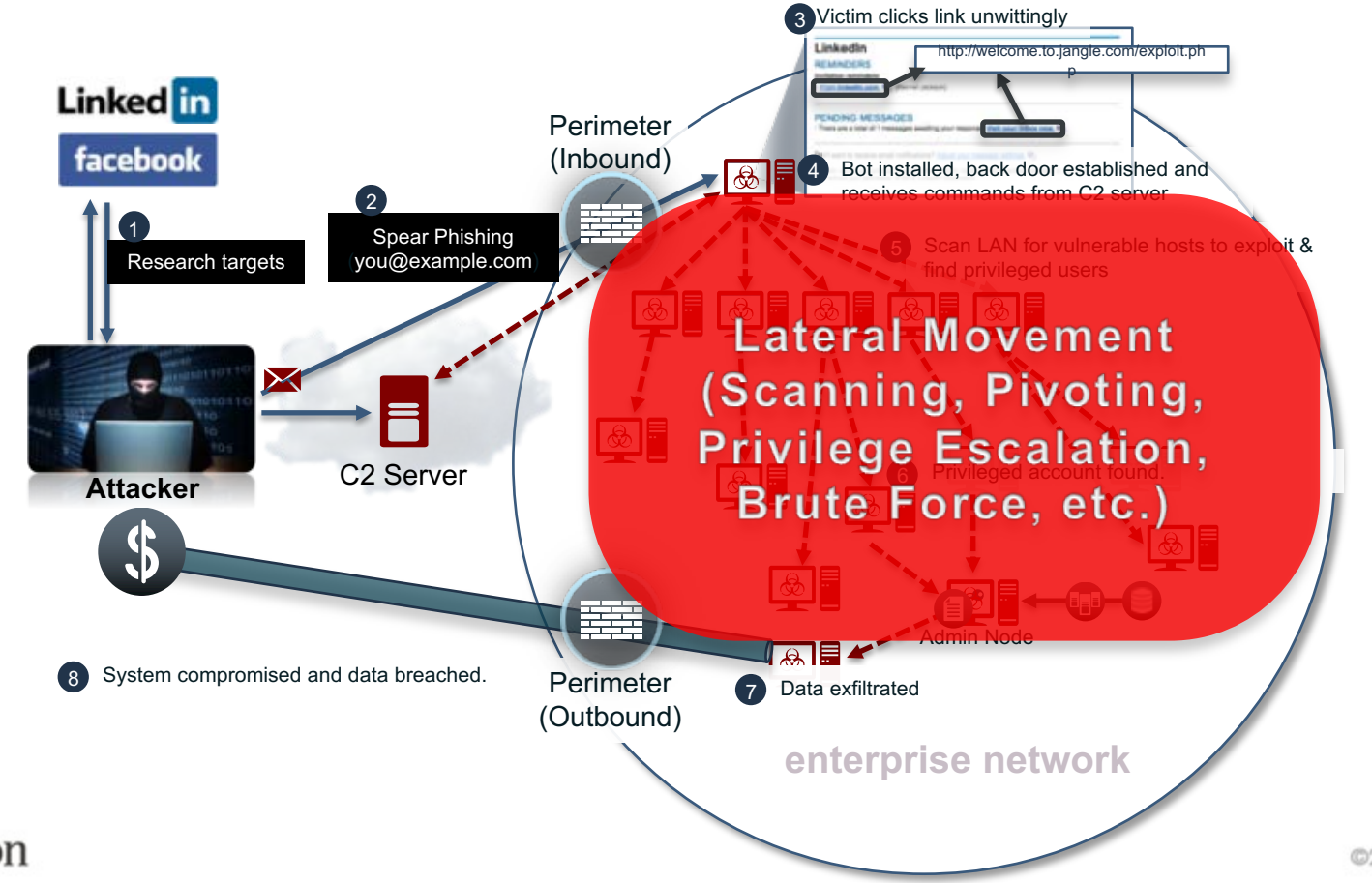
Posture – Evaluate endpoints for risk

Top Access Control Goals



Pearson

Targeted Attacks and Lateral Movement (Without Segmentation)



Traditional Network Segmentation Techniques

Layer 2 Segmentation

- VLANs / Wireless SSIDs
- Private VLAN / Port Security
- Transparent Stateful Firewall

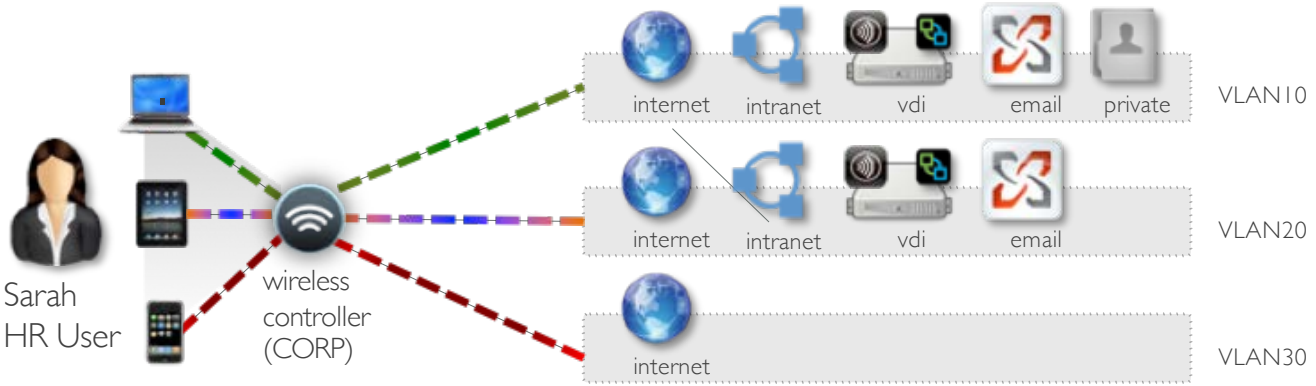
Layer 3 / Virtual Private Networking

- VRF (Virtual Routing & Forwarding)
- EVN / MPLS / Others
- Stateful Firewall

Stateless Access Control Lists

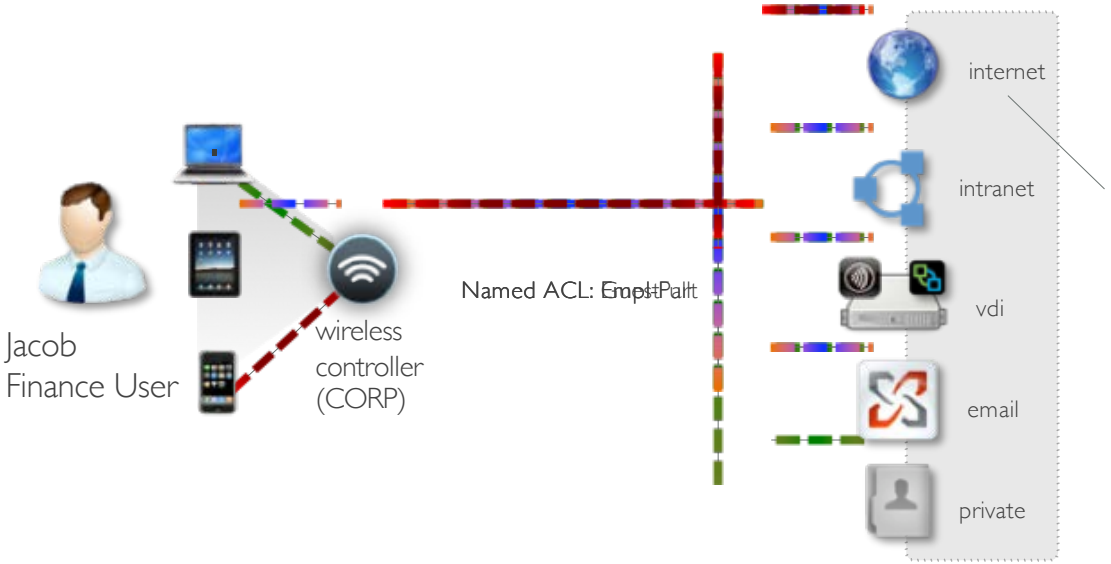
- Router / Switch L2 or L3 ACLs
- Wireless AP / Controller ACL

Enforcement Options VLAN ASSIGNMENT



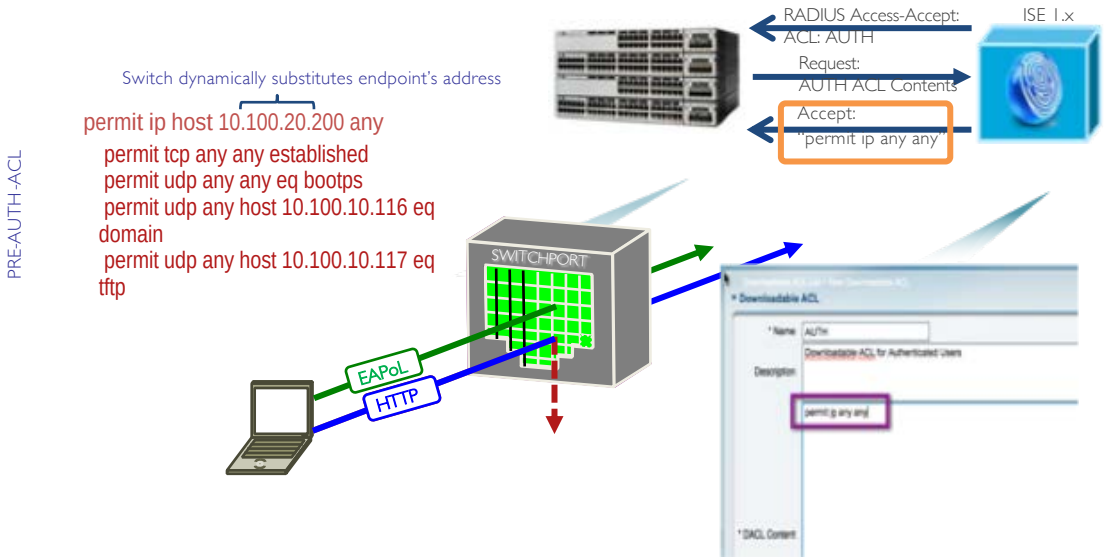
Sarah joins her personal laptop to CORP wireless SSID and successfully completes
Authorization Policy, she is placed on VLAN 30. This particular VLAN has access
to all corporate resources including access to most corporate resources.

Enforcement Options ACL'S



Jacob joins his corporate laptop to the CORP wireless network. His connection is dynamically provisioned with Empl-Full ACL, allowing full access to the corporate resources.

Downloadable (Dynamic) Access Control List (dACL)



- Contents of dACL are arbitrary
- Can have as many unique dACLs as there are user permission groups
- Same principles as pre-auth port ACL

Access Control Remediation / Eradication

- **Quarantine** – Limit or deny network access
- **Isolation –** Put into a separate VLAN or take off the network to limit risk
- **Patch / Upgrade –** Windows / AV update
- **Software Link –** Offer software

Agent vs. Agentless

Agent

- Auto remediation
- Single sign-on
- Quick assessment
- Installed
- Typically employees
- Requires install privileges
- Sometimes built into other agents (example Anyconnect)

Agentless

- Manual remediation
- Manual sign-on
- Longer assessment
- Java / Active X
- Typically guest or contractors
- Doesn’t require anything to be installed
- Typically ran within the web browser

Context-based Authentication Challenges

- **Time** – What time is the device accessing
- **Location** – What part of the network (LAN, VPN, Wireless)
- **Frequency** – How often is access needed
- **Behavioral** – User trends (traveling, data access, etc.)

Time Challenges

- **Daily Spike Times**
  - Morning when people come to work
  - Lunch time return
- **Seasonal Spike Times**
  - Holiday season for retail
- **Events**
  - Conference with lots of guests

Location Challenges

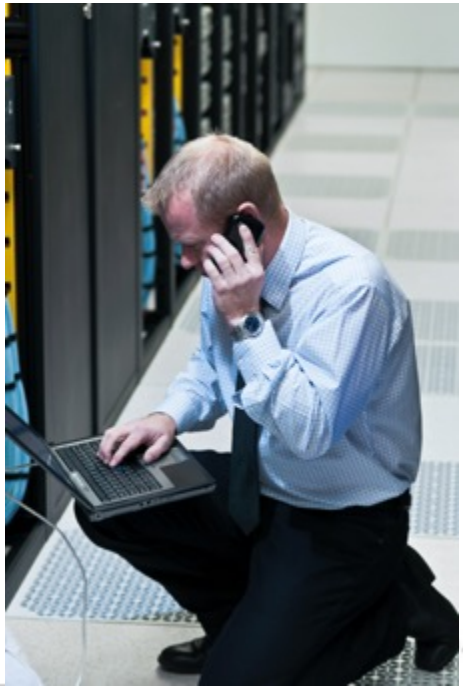
- **Separated AD Forests**
  - User travels between locations
  - HA design challenges
- **Remote vs. Local**
  - VPN from work challenge
- **Wireless Roaming**
  - Skateboarder challenge

Frequency Challenges

- **Rapid Requests**
  - Skateboarder again!
- **Heartbeat Technologies**
  - Too much delay could break something
- **Delayed Requests**
  - Deployed soldier returns

Behavior Challenges

- **Policy Exceptions**
  - Open ports, permit software, provide access, etc.
- **Road Warriors**
  - Need internal access anywhere
- **Privilege Changes**
  - User to administrator in AD
- **Internet of Everything**



Challenge Highlights

- Morning and post lunch
- Events (conferences)
- Guests
- Compliancy
- AD Forests

- Remote users
- **Rogue devices**
- Blind spots
- Special access
- IoE

Identifying Assets

- Profiling technology can auto identify assets

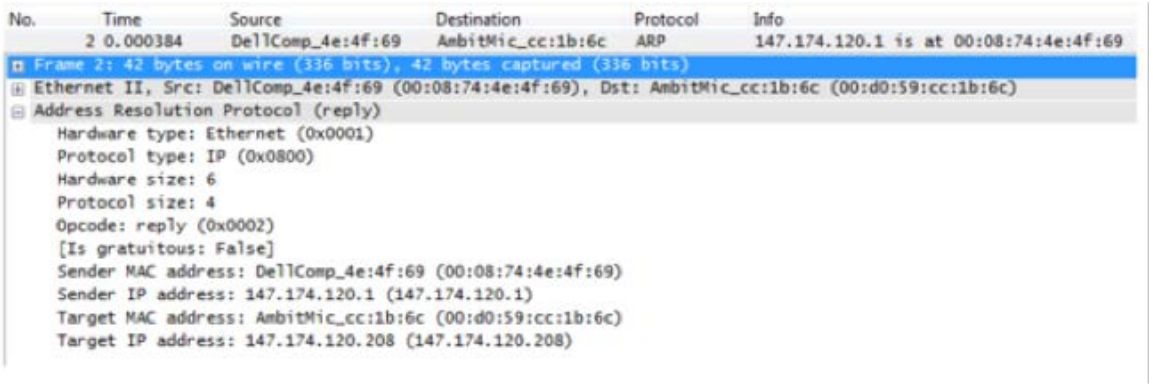
- Protocols that can be used by profiling

  - NetFlow – Collects data about packets
  - DHCP – DHCP probe listening for packets from IP Helper
  - DHCPSPAN – Collecting DHCP packets
  - Radius – Session attributes as well as CDP, LLDP, DHCP, etc.
  - DNS – Look up FQDN
  - SNMP – Linkup / down and MAC notification

DHCP Fingerprinting

- DHCP Fingerprinting – Detect end device OS based on DHCP exchange packets

- Option 55 Parameter request list



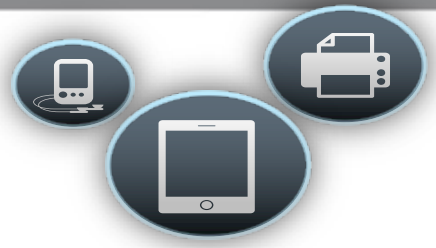
- https://fingerbank.inverse.ca/

Port Scanning for Devices - NMAP

- -sV = (Version detection)
- -A = Enables a bunch of stuff including version detection
- --allports = Include all ports in scan

```
# nmap -sV -O -v 129.128.X.XX

Starting Nmap ( http://nmap.org )
Nmap scan report for [hostname] (129.128.X.XX)
Not shown: 994 closed ports
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          HP-UX 10.x ftpd 4.1
22/tcp    open     ssh          OpenSSH 3.7.1p1 (protocol 1.99)
111/tcp   open     rpc
445/tcp   filtered microsoft-ds
1526/tcp  open     oracle-tns   Oracle TNS Listener
32775/tcp open     rpc
No exact OS matches for host
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: HP-UX
```

Profiling



Active Scanning

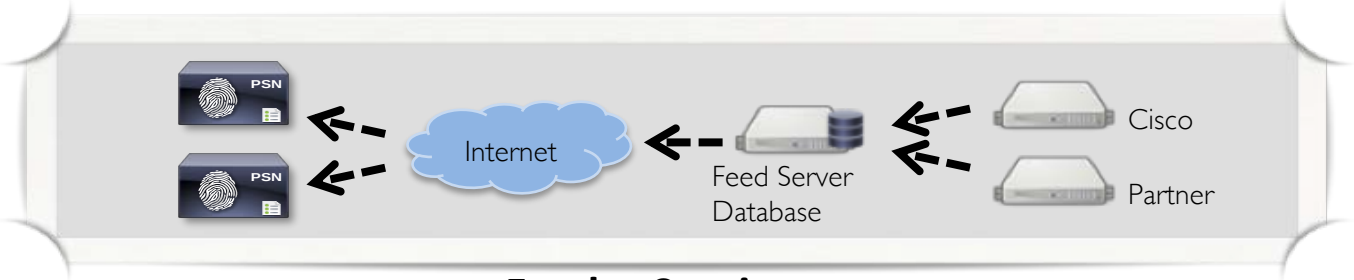
ISE collects device data to determine what it is

Integrated Scanning

Cisco Wireless Controllers & Switches offer integrated device profiling*

Device Feeder Service

New content dynamically added



Feeder Service

Challenge: Detecting Virtual Servers

Option 1) MAC Address – Check if they belong to Vmware or other virtual company

- ARP table can be used once you ping a system

Option 2) Check the Process Names

- Vmware-vmx

Reading Authentication Logs

- Depends on type of authentication
  - Centralized – AAA or NAC as examples
  - Local – Port security as an example
  - Factors (Are, Know, Have)
- Or very basic like Port Security (Yes or No)

Port Security Log Error

```
PM-4 ERR DISABLE: psecure-violation error detection on Fa0/1
PORT_SECURITY -2-PSECURE_VIOLATION: Security Violation occurred
```

Login Examples

Invalid User Login Attempt

Jul 9 10:51:24 joey sshd[19537]: Invalid user admin from hackme.lab.net

OR

Jul 9 10:53:24 joey sshd[12914]: Failed password for invalid user test-inv from hackme.lab.net

OR

Jul 9 10:53:24 aamir sshd[3251]: User aamir not allowed because listed in DenyUsers

Accepted Login

May 20 20:22:28 joey sshd[8813]: Accepted password for root from 192.168.10.185 port 1066 ssh2

OR

May 20 20:22:28 joey sshd[23857]: [ID 702911 auth.notice] User test1, coming from 192.168.2.185, -authenticated.

OR

Oct 12 08:05:46 hostname auth|security:info sshd[323808]: Accepted publickey for usr1 from 2.3.4.5 port 37909 ssh2

Policy + Controls

Pearson

Policies

- Rules to unify security standards across the company
- Should be back by C-level and have ramifications if violated – IE these are management's intent (CISO)
- Compliance is mandatory
- **Contain standards, procedures and guidelines**

Security Policies Include

- **Information security policy** – High-level authority and guidance
- **Acceptable use policy (AUP)** – What is permitted
- **Data ownership –** Ownership of information and usage
- **Data classification policy –** How data is classified
- **Data retention policy –** How long data is held and destroyed
- **Account management policy –** User account lifecycle
- **Password policy –** Password rules

Standards

- Mandatory requirements aimed at enforcing policies
- Ex) Configuration settings, operating systems, controls that must be enforced, and so on
- Approved at lower level and change often

Standards enforce Policies

Procedures and Guidelines

Procedures

- Specific to security documents. Think "Playbook"
- **Step-by-step document** detailing what is to be done and how

Guidelines

- Think optional or "helpful advice"

Exceptions / Compensating Controls

- Process to break rules
- Compensating controls mitigate risk that comes with the exception to the security standard

- Business or technical justification
- Scope and duration
- Risks associated with exception
- Specific standard that requires exception

Acceptable Use Policy

Approved Use

- Accessing the internet
- Downloading content
- Bringing corporate computers home
- Social media

Not Approved

- Adult Material
- Shareware
- Personal computers on corporate network
- Cloud storage

Data Owner Policy

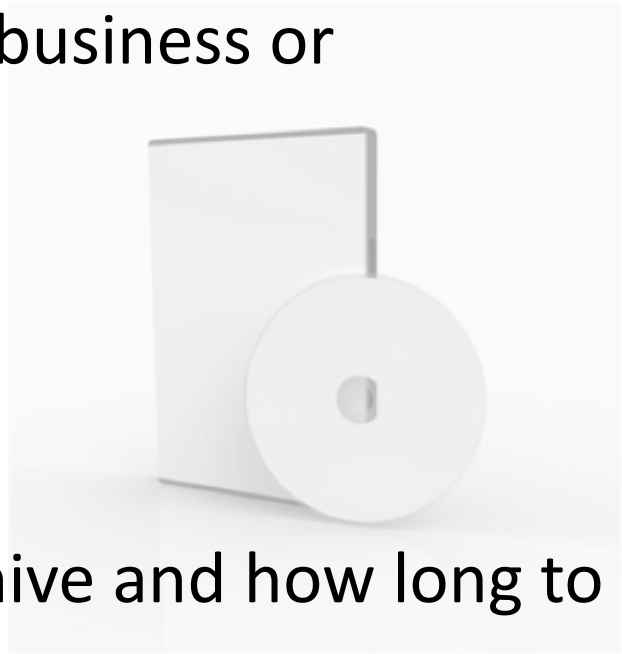
- Responsible and accountable for protection and classification of specific data
  - Typically delegates responsibility to custodians
  - **Decides security controls (sets parameters and labels data)**

- **Data Custodian** – (Administrators) Implementing security to meet data owners' requirements and performs backups

- **Data processor** – users that access the data

Data Retention Policy

- How long data must be stored for business or compliance reasons
  - Comply with regulations
  - Recover data when needed
  - Typically three years



- Need to specify which data to archive and how long to keep it

Data Classification

- Classifying data and ensuring CIA
- Encryption (**Data at loss** vs. **Data at rest**)
- Data lifecycle
- Data handling requirements

Confident – Classified – Secret – Top Secret - Public

Account Management Policy

- Ensuring all accounts within a particular OS or application following certain guidelines

  - *Must have password that adheres to guidelines*
  - *Must only be used for least privilege tasks*
  - *Possible training before account is permitted*
  - *Certain approval may be required*
  - *Account modification must require specific approval*
  - *Do not email passwords*

Data Classification Example

*** COMPANY Highly Confidential - Controlled Access ***

Unauthorized disclosure of any information contained within this Security Advisory is a violation of COMPANY Code of Business Conduct and may be considered cause for immediate termination of employment.

Contact Internal support at companysupport@company.com if you have any questions regarding the receipt or use of this information.

Security Controls

Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to information, systems, or other assets.

- **Preventive Controls –** Before the event
- **Detection Controls –** During the event
- **Corrective Controls –** After the event

- **System Specific –** Only for a particular system
- **Common Controls –** For multiple systems
- **Hybrid Controls –** For both system specific and common characteristics

Control Selection

- Select a set of **baseline security controls**
  - Based on external and internal requirements
- Controls selected based on impact level of information system
- Data owners and IT architects typically responsible for control selection

Example – Controls related to PCI DSS are external and high impact level

Physical Controls

Security measures used to deter or prevent unauthorized access to sensitive material

- Fences
- Man traps
- Doors and Locks
- Closed-circuit surveillance cameras
- Picture IDs
- Motion alarms

Logical Controls / Technical Controls

Controlling access over a network.

- Encryption
- Logical segmentation
- Authentication
- Access Control Lists (ACLs)
- Smart cards
- File integrity auditing software

Administrative Controls

Human factors of security, meaning all levels of personnel within an organization. Determines who has access to what resources.

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel registration and accounting
- Personnel recruitment and separation strategies
- Planning configuration of devices

Continuous Monitoring

- Process and technology used to enforce ongoing awareness of information security within an organization including latest vulnerabilities, threats and risk management
- Monitoring for threats at all times
- Popular for SIEM and breach detection

Compliance

Due Diligence

- Review of the governance, processes, and controls used to secure information assets
- Obligation that may exist between state and corporate actors
- Fines and other penalties for those that don’t follow

Regulatory Compliance

- An organization's adherence to laws, regulations, guidelines and specifications relevant to its business
- Often required and have financial and legal enforcement including federal fines
- EX) FISMA requires vulnerability scanning of GOV devices

PCI DSS – HIPAA – FISMA - SOX

Compliant does **NOT** mean secure

- Standards fall behind current technology trends
- Compliance could delay updates
- Standards do not account for all threats
- Sometimes false sense of security!!!!

Standards Frameworks

- Compliance for specific markets, technology and standards
- Documented processes used to define policies and procedures around implementing and managing information security controls

NIST- ISO – COBIT – SABSA – TOGAF - ITIL

Financial and Education Frameworks

- Gramm-Leach-Bliley Act (GLBA) – Security programs for financial institutions
- Sarbanes-Oxley (SOX) – Financial records of publicly traded companies
- The Family Education Rights and Privacy Act (FERPA) – Security for education institutions

National Institute of Standards and Technology (NIST)

- Group within U.S. Commerce Department
- Develops cybersecurity standards, guidelines, tests and metrics for protection

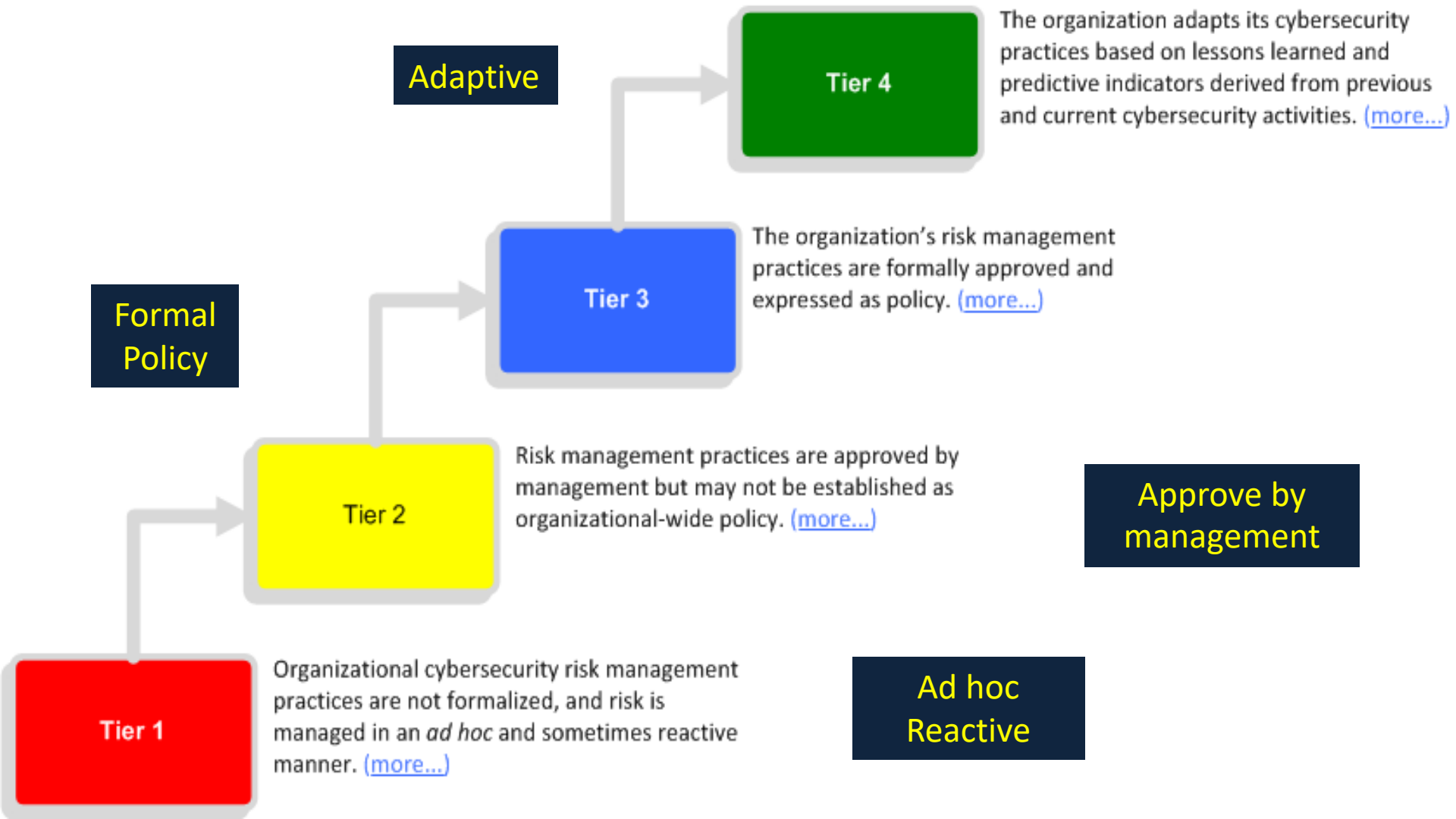
Publishes framework – Cybersecurity framework

- Follows U.S. President's executive order *Improving Critical Infrastructure Cybersecurity* from 2013
- **Voluntary** but structured well and widely accepted

NIST 2014 Standard Objectives

- Describe your current cybersecurity posture
- Describe your target state for cybersecurity
- Identify and prioritize ways to improve and be repeatable
- Assist process towards your target state
- Communicate cybersecurity risks among internal and external stakeholders

NIST Framework Focus **= Identify – Protect – Detect – Respond - Recover**


Adaptive
Tier 4
The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. (more...)
Formal Policy
Tier 3
The organization's risk management practices are formally approved and expressed as policy. (more...)
Tier 2
Risk management practices are approved by management but may not be established as organizational-wide policy. (more...)
Approve by management
Tier 1
Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. (more...)
Ad hoc Reactive

International Organization For Standardization (ISO)

- Global network of the world's leading standardizers
- 163 Countries
- Various standards for health, technology, process, etc.

ISO/IEC 27001 Information Security Management – Approach to manage and secure sensitive company information including people processes and IT Systems.

- **Voluntary** but accepted as de facto framework for information security implementation.
- Can get certified for this

ISO Categories

- Information security policies
- Human resource security
- Organization of information security
- Access control
- Asset management
- Cryptography
- Physical and environmental security
- Operational security
- Communication Security
- System acquisition, development and maintenance
- Supplier relationships
- Information security regarding business continuity
- Information security incident management
- Compliance with internal requirements

Control Objectives for Information and Related Technologies (COBIT)

- Set of controls over information technology
- Organized around logical framework of IT-related processes and enablers

COBIT Components

- **Framework** – Organized by IT domains / processes. Links to business requirements
- **Process descriptions** – Common language describing a process model
- **Control objectives** – High-level requirements
- **Management guidelines** – Helps with assigning responsibility
- **Maturity Models** – Assess how well a process addresses a gap

COBIT Example for Maturity

Maturity Level	Process Criteria
0 – Nonexistent	Lack progress
1 – Initial / Ad hoc	Recognized issues exist
2- Repeatable but intuitive	Process developed by different people to do same task
3 – Defined process	Standardized and documented procedures
4 – Managed and measurable	Measure compliance with procedures and take action to improve

Sherwood Applied Business Security Architecture (SABSA)

- Framework and methodology for enterprise security architecture and service management
- Everything derived from a business requirement for security
- Highly customizable to a unique business model

The Open Group Architecture Framework (TOGAF)

- Created and maintained by the opengroup.org
- Framework providing designing, planning, implementing and governing enterprise information technology architecture
- Typically four levels: Business, Application, Data, and Technology

Information Technology Infrastructure Library (ITIL)

- Standardize the selection, planning, delivery and support of IT services to a business
- Desired outcome - Improve efficiency and achieve predictable service levels
- Five core publications or ITIL books (Axelos)
- Not required but nice to show people when ITIL certified

Know when to Recommend

Key Concept

What if your boss or leadership needs a recommendation?

NIST – Government approved cyber framework
ISO - Approach to manage and secure sensitive company information
COBIT - Set of controls over information technology
SABSA - Framework and methodology for enterprise security architecture and service management
TOGAF - Framework providing designing, planning, implementing and governing enterprise information technology architecture
ITIL - Standardize selection, planning, delivery and support of IT services

Processes

Separation of Duties

- **Key security principle** - No one person should be able to affect a breach of security
  - Separation of Duties
  - Rogue employees must use collusion

- Encourages cross training but could slow down process

Dual Control

- Require two people, processes or devices to gain authorized access to a system resource i.e. data, files, etc.
- **Dual Control** is a form of **separation of duties**
- Rogue employees must use collusion to accomplish goals

Cross Training

- Training in more than one role or skill
- Helps with enabling dual control / separation of duties
- Sometimes called “over the shoulder” training

Mandatory Vacation

- **Management security control** – Force employee to take at least a week of consecutive vacation to provide the company time to audit for potential fraudulent behavior

- **Used to detect fraud and collusion**

- Malicious parties could prepare for it

Succession Planning

- Identifying and preparing people who can replace key people
- Encourages cross training
- Important for dual control and separation of duties

People Best Practices

- Enforce the principle of least privileges
- Enforce concepts from this section
- Automation vs. manual enforcement
- Test and train (phishing, etc.)

Stakeholders

- **Human Resources** – Users are typically involved with security incidents. HR will assist with employee actions
  - Termination, employee rights, etc.

- **Legal Resources** – What and how to report. Legal obligations to business and stake holders
  - Requirements to report and legalities with investigation

Stakeholders

- **Marketing** – Public incidents can destroy companies. Marketing must manage how the incident will be exposed
- **Management** – Technical and IT service leaders to represent the technical and operations impact
  - **Should include security and operations**

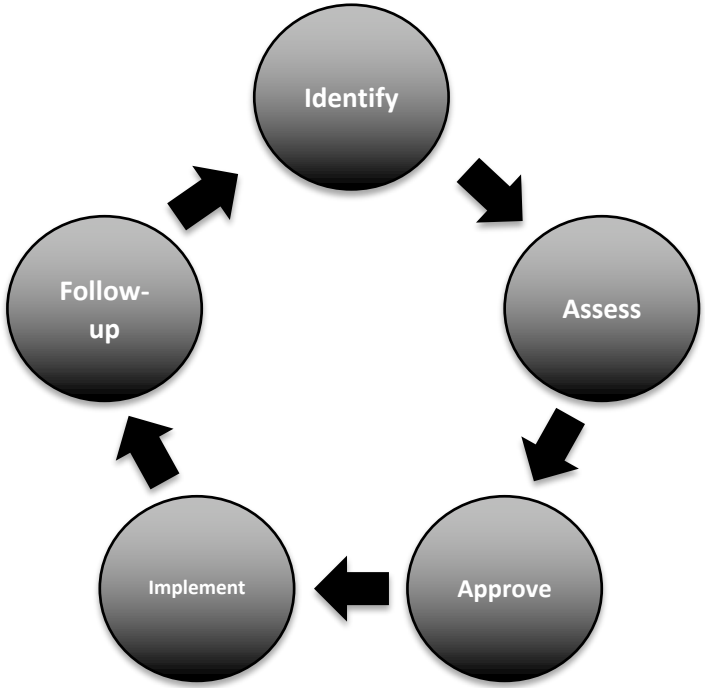
Communication stays within trusted circles

Role-based Responsibilities

- **Technical** – Breakdown of what occurred
- **Management** – Decisions for actions
- **Law enforcement** – Legal actions

- **Response** – Action taken
  - **Retain incident response provider** – Contracted help
  - **Internal resources** – Proactively label skillsets within organizations
  - **Go to legal resources** – Law enforcement and lawyers
  - **Marketing** – Public message

Change Control Process



- **Identify** – What changes to make
- **Assess** – What is impact of change
- **Approve** – Project management and leadership should get approval
- **Implement** – Execute plan
- **Follow-up** – Verify work is done and re-assess impact of changes

Incident Response

Incident Response

Organization approach to addressing and managing the aftermath of a security breach or attack

Communication is Critical

Keep it within trusted circles

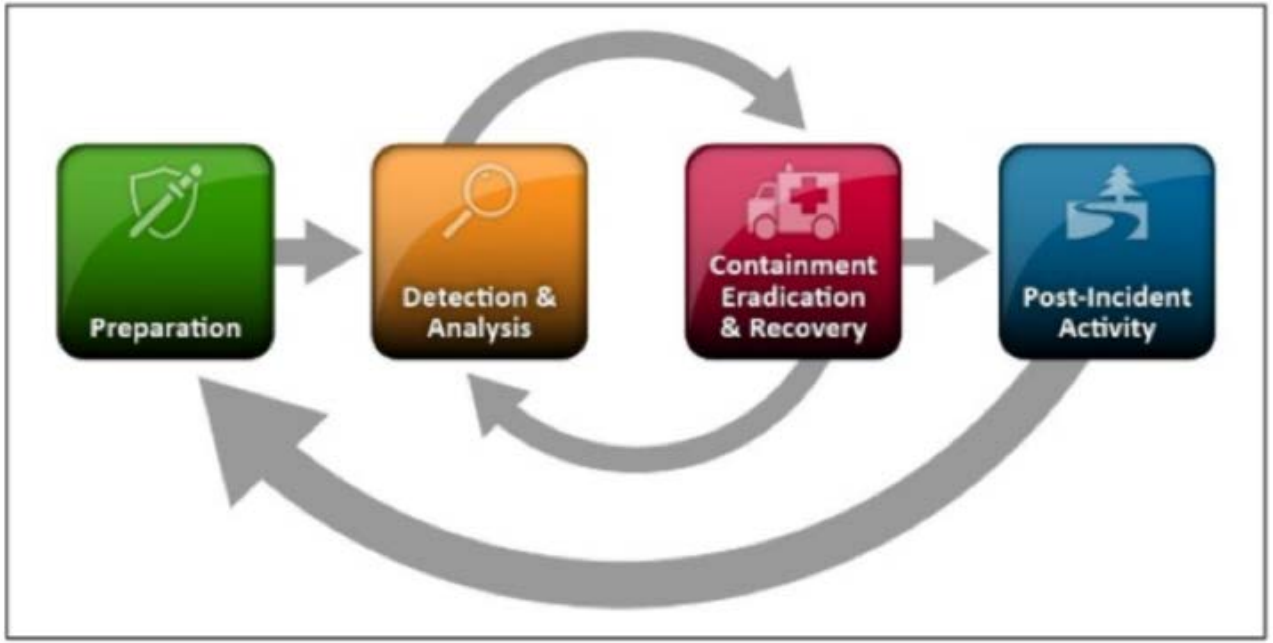
Incident Response

- **Preparation:** Prepare for potential incidents
- **Identification:** Determine if a security incident has occurred
- **Containment:** Isolate the incident to prevent further damage
- **Remediation:** Identify root cause and remove impacted systems
- **Recovery:** Return systems back to product that are no longer a threat
- **Learn:** Benefit from the incident by looking to improve security

Note: Identifying source of attack is not important!
Root cause is much more important!

NIST SP 800-61

The incident response life cycle



Preparation

- Build your incident response program foundation
- Hire people for your team
- Build and enforce strong defenses to reduce risk of breach
- Identify hardware, software and other tools that will be used for investigations
- This phase will continue to adjust based on outcomes from the last phase.

Detect and Analysis 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.

- Network **profiles** and **baselines** are a huge help!
- Event correlation ties multiple events to the true risk/attack
- Threat intelligence improves known vulnerabilities and attack data
- **Reponses teams** classify the severity of the invent!!!!

Contain, Eradicate and Recovery

- **Scope** - Choose your containment strategy depending on the breach
- **Contain** – Prevent the breach from spreading
- **Eradicate** – Remove the contained threat
- **Recovery** – Return back to a operational state

Containment Strategy

Segmentation – Least privilege for each segment so only lateral devices can be impacted (ex – printers infecting printers

- NAC can move infected systems to quarantine segments
- Best practice to proactively properly segment the network

Isolation – Completely cut off the attacker or network

Removal – Depends on the type of breach

- Sanitization
- Reconstruction / reimaging
- Secure disposal

Removal

Depends on the type of breach

- Sanitization
- Reconstruction / reimaging (best option verse cleaning)
- Secure disposal

Next validation is critical as removal isn't always 100%

- Permissions validation
- Patching
- Scanning
- Verify communications and logging to ensure no post compromise

Recovery

- Check that only authorized accounts exist
- Verify permissions for all accounts
- Perform vulnerability scans
- Verify logging is working
- Patch any weakness

Patching Priorities

Start with the infected system, then work outward

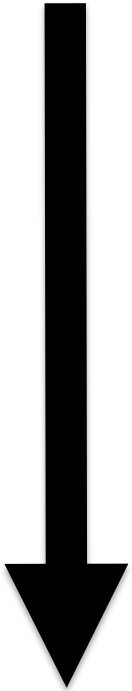
Directly Infected

Connected / Close System

Rest of the network

Secure Disposal – NIST 800-88

- **Clear** – Using common read and write commands or using factory restore options
- **Purge** – Overwriting with 0's, block erasing, degaussing using magnets, etc.
- **Destroy** – Drill into the drive, melting, hammering, etc.



Post Incident - Lessons Learned Report

Grade the incident response. Assign actions to improve

Success

- Operational success
- Identification of threat
- Recovery time
- Security technology used
- Reaction highlights

Failures

- Process breakdown
- Missed threats
- Delays in recovery
- Technology changes
- Areas for improvement

Why Lesson Learned Report?

Post incident process summarized

- Containment techniques
- Eradication techniques
- Validation
- **Corrective action**
- Incident summary report

Best facilitated by a external party!

Attacker identity or source is not important

People Involved with Lessons Learned

Only Trusted People View This!

- Assessment of goals and objectives
- Identification of activities or areas needing additional effort
- Identification of effective activities or strategies
- Comparison of costs and results of different activities
- Assessment of the roles of organizations in the project and the interactions among the organizations

Management – HR – Leadership – Data Owners

Incident Summary Report

Explain the situation from an Operational and Technical viewpoint

Operation Questions

- What happened
- When it occurred
- Business impact
- Who was engaged
- Current status

Technical Questions

- Associated vulnerabilities
- Required patches
- What systems are impacted
- Existing risk
- Technology needed

Incident Response Document

- Organization's approach to addressing the aftermath of a security breach (**think playbook**)
- Goal is to limit damage, reduce recovery time and costs
- Critical to have C-Level Sponsorship and test it!
- Develop methods of contact and escalation

Call List / Escalation List

- Who to contact when an incident is identified
- Required people
- Backups when people are not available
- Severity actions
- How to contact
  - Auto dial, conference bridge, email blast

Secure Communication – Know This

- Email alias for key members
- Track communication for status check
- Legal incidents may require reporting
- Record conference calls
- Automated tracking and management services could help

Digital Forensics

What Can Forensics Do?

- **Recover** deleted files
- Determine what system has **malicious files / launched an attack**
- **Trace** the footprint of the attack
- **Track** malware by its signature
- Determine time, place and device used for an **event**
- Track **physical locations** and websites used
- **Crack** passwords

Cyber Crime Investigation Process

- Identify a crime
- Collect preliminary evidence
- Obtain court warrant for seizure if required
- Perform first responder procedures
- Seize evidence at the crime scene
- Transport evidence to forensic laboratory
- Create copies of evidence
- Generate images and exam for evidence

Challenges of Digital Forensics

- The amount of data needed for collection and storage makes it a very difficult and expensive process
- Encryption and mobile data is very hard to collect
- Lack of physical evidence makes crimes harder to prosecute
- Hacking tools make it easier for criminals to hide their tracks

Legally Seizing Evidence

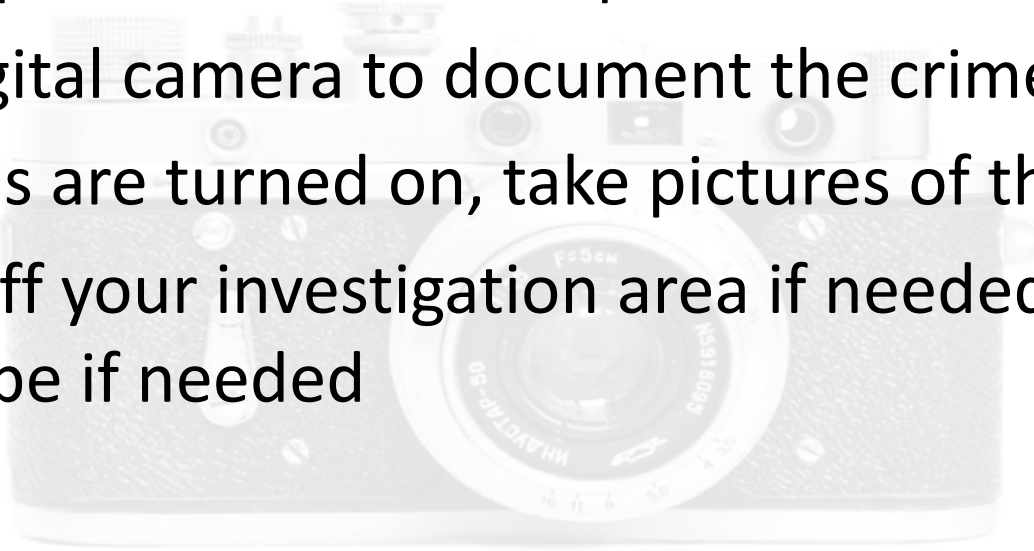
- Assume devices will destroy data
- Use Chain of Custody, disclosure forms, and written permission to take equipment
- Include where equipment goes and work being performed
- Secure equipment until it can be securely stored

Which Comes First? – Need to Know!

- Engage the incident response plan
- Gather systems of interest
- Make a forensic copy
- Investigate the copy
- Report findings
- Prepare for court

Crime Scenes

- Keep a forensics journal
  - Many professionals use a tape recorder
- Use a digital camera to document the crime scene
- If systems are turned on, take pictures of the display
- Border off your investigation area if needed, use crime scene tape if needed



Documentation / Forms

- Asset list of identified devices
- First Responder Report
- Chain of custody forms
- Sign-in document
- Authorization documents
  - Warrants
  - Corporate documents

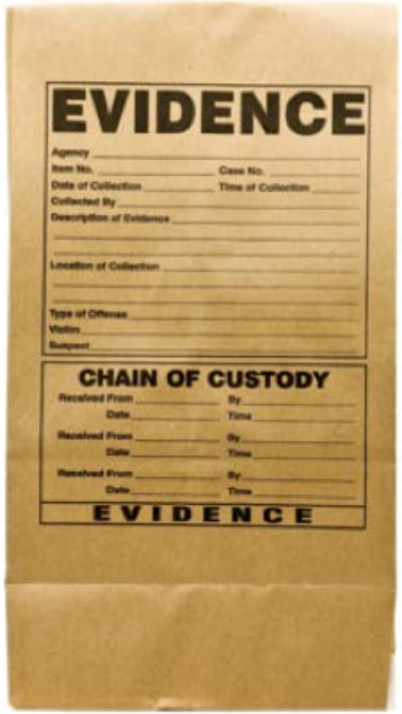
Chain of Custody

- **Chain of custody** = Chronological documentation / paper trail showing seizure, **custody**, control, transfer, analysis, and disposition of evidence, physical or **electronic**

- Expect your chain of custody to be reviewed, questioned, and maybe in court

Chain of Custody Form

- Asset list of identified devices
- First Responder Report
- Chain of custody forms
- Sign-in document
- Authorization documents
  - Warrants
  - Corporate documents



Tamper-proof Seals

- Collected devices should be sealed to validate chain of custody
  - Who collected
  - When and where
  - What is stored
  - Responsible parties

Powered ON and OFF Computers

ON

- Collect the RAM information
- Encrypted data could be unencrypted in RAM
- Identify running processes

OFF

- Leave off
- Make two bit copies

Data Acquisition 101

Static Acquisition

- Device powered off or shutdown
- Non-volatile, usually from hard drives, USB drives, smart phones, slack space, swap files, etc.

Live Acquisition

- Running system
- Volatile – registries, cache and ram
- Collection occurs in real time

Value of Volatile Data

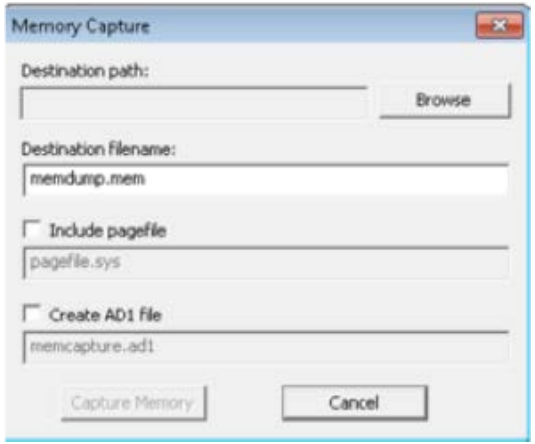
- Running Processes
- Passwords in clear text
- Instant messages
- Executed console commands
- IP addresses
- Trojan Horses

- Unencrypted Data
- Who is logged in
- Attached devices
- System information
- Registry Information
- Open Ports and listen applications

Windows - %SystemRoot%\MEMORY.DMP = Best chance when system is powered off

Widows - Show Me – Capture RAM

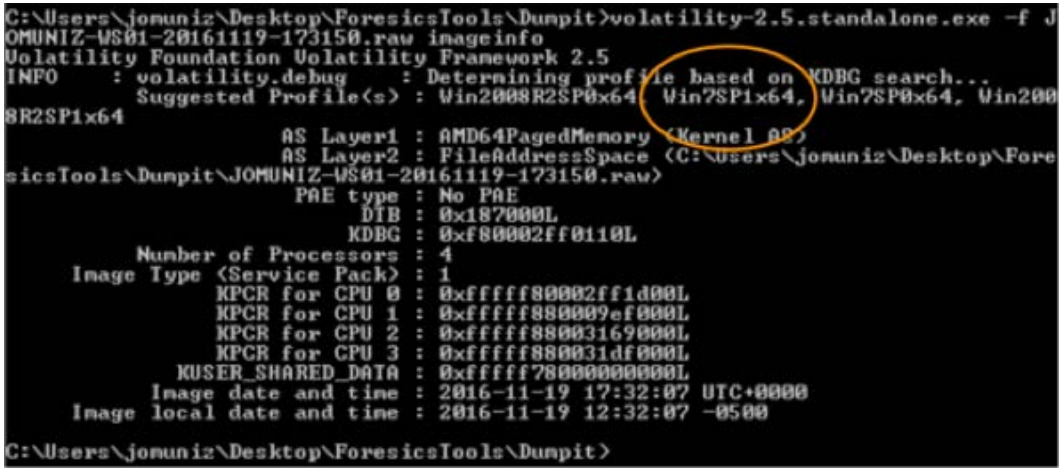
- There is a memory capture option in FTK Imager.
- DumpIT is a simple dump program
- Windows tools
- Many others!!!!




```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

   Address space size:        1442840576 bytes (   1376 Mb)
   Free space size:           2847854592 bytes (   2715 Mb)

   * Destination = \??\C:\Users\jomuniz\Desktop\ForesicsTools\Dumpit\JOMUNIZ-W
01-20161119-173150.raw

   --> Are you sure you want to continue? [y/n]
```

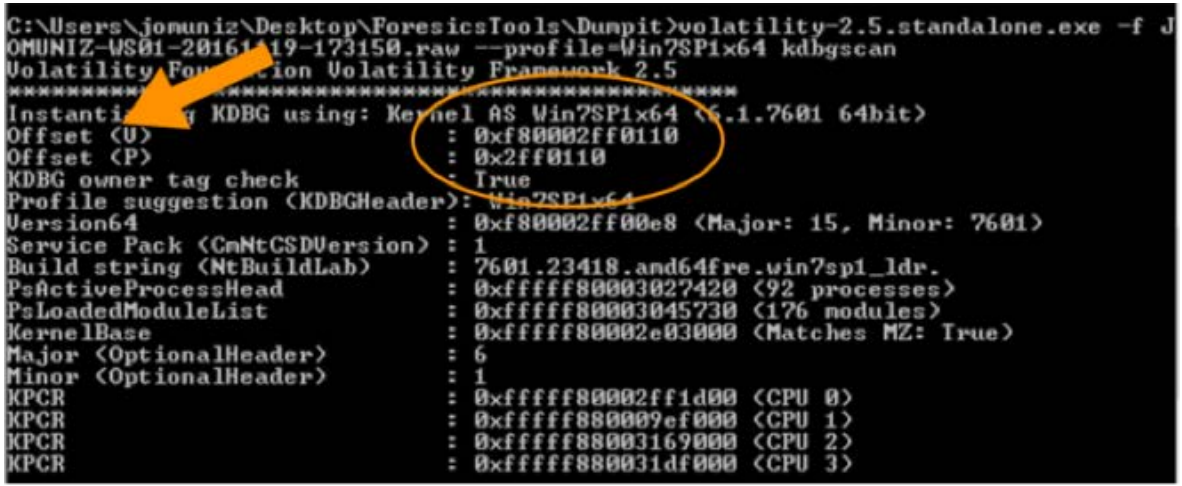
Widows - Show Me – View Process Volatility P1

- Put memory dump in folder with Volatility executable
- Open CMD and launch the following command (assuming volatility 2.5)
- Volatility-2.5.standalone.exe –f <mem dump file.raw> imageinfo
- This shows the type of image



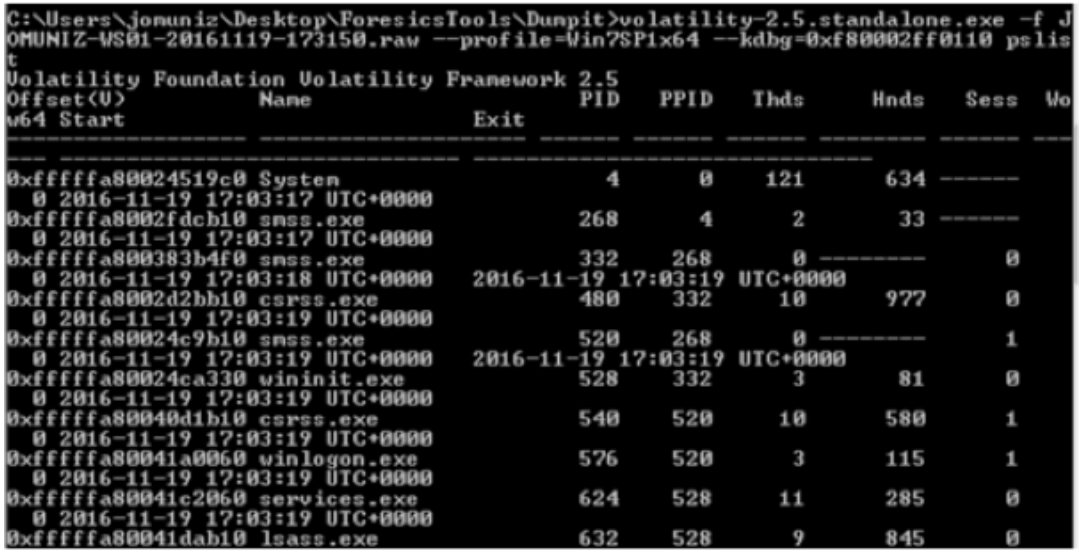
Widows - Show Me – View Process Volatility P2

- Now run the following command
- Volatility-2.5.standalone.exe –f <mem dump file.raw> --profile=<suggested profile> kdbgscan
- The last image showed me its probably Win7SP1x64 so will use that
- Identify and copy the offset so we can use it to get the process list



Widows - Show Me – View Process Volatility P3

- Now run the following command
- Volatility-2.5.standalone.exe –f <mem dump file.raw> --profile=<suggested profile> --kdbg=<off set> pslist
- This will display the current processes. Add > <file.txt> at end to put it in text file



```
C:\Users\jomuniz\Desktop\ForesicsTools\Dumpit>volatility-2.5.standalone.exe -f J
OMUNIZ-WS01-20161119-173150.raw --profile=Win7SP1x64 --kdbg=0xf80002ff0110 pslis
t
Volatility Foundation Volatility Framework 2.5
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wo
w64 Start                       Exit
------------------ -------------------- ------ ------ ------ -------- ------ ---
--- ------------------------------ ------------------------------

0xfffffa80024519c0 System                    4      0    121      634 ------
  0 2016-11-19 17:03:17 UTC+0000
0xfffffa8002fdcb10 smss.exe                268      4      2       33 ------
  0 2016-11-19 17:03:17 UTC+0000
0xfffffa800383b4f0 smss.exe                332    268      0 --------      0
  0 2016-11-19 17:03:18 UTC+0000   2016-11-19 17:03:19 UTC+0000
0xfffffa8002d2bb10 csrss.exe               480    332     10      977      0
  0 2016-11-19 17:03:19 UTC+0000
0xfffffa80024c9b10 smss.exe                520    268      0 --------      1
  0 2016-11-19 17:03:19 UTC+0000   2016-11-19 17:03:19 UTC+0000
0xfffffa80024ca330 wininit.exe             528    332      3       81      0
  0 2016-11-19 17:03:19 UTC+0000
0xfffffa80040d1b10 csrss.exe               540    520     10      580      1
  0 2016-11-19 17:03:19 UTC+0000
0xfffffa80041a0060 winlogon.exe            576    520      3      115      1
  0 2016-11-19 17:03:19 UTC+0000
0xfffffa80041c2060 services.exe            624    528     11      285      0
  0 2016-11-19 17:03:19 UTC+0000
0xfffffa80041dab10 lsass.exe               632    528      9      845      0
```

Encryption Keys Example

- Hashdump – see hash passwords

```
C:\Users\jomuniz\Desktop\ForesicsTools\Dumpit>volatility-2.5.standalone.exe -f J
OMUNIZ-WS01-20161119-173150.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.5
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6ca09fa76c16472feb15e70aed5dc
6bd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Core dumps and hibernation files are also great places to find encrypted keys stored in memory!

- Cmdscan – see all commands used in CMD

```
C:\Users\jomuniz\Desktop\ForesicsTools\Dumpit>volatility-2.5.standalone.exe -f J
OMUNIZ-WS01-20161119-173150.raw --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.5
**************************************************
CommandProcess: conhost.exe Pid: 5880
```

- Iehistory – see all browser history

```
C:\Users\jomuniz\Desktop\ForesicsTools\Dumpit>volatility-2.5.standalone.exe -f J
OMUNIZ-WS01-20161119-173150.raw --profile=Win7SP1x64 iehistory > browser.txt
Volatility Foundation Volatility Framework 2.5
```

Preserving Data Check list

1. Made two bit level copies
2. Validated the copies using hashing
3. Enabled write block to preserve copy

Follow This Practice For Every Investigation

Bit Stream Copies – NOT Original Data!

- Copies everything including hidden and residual data
- Bit Stream copies do not contaminate evidence allowing it to be used for legal
- Not Backups – backups only pay attention to live system data
  - Backups modify the timestamp corrupting data!

Kali - Bit Stream Copies

- **Kali Linux can simply use the DD command.**
  - **dd if=<source> of=<destination> bs=<byte size>**

- Better Option (developed by depart of defense) – **dcfldd** found under forensic tools category
  - **dcfldd if=/dev/sda hash=md5 of=/media/diskimage.dd bs=512 noerror**

```
root@kali:~# dcfldd if=/media/root/SP hash=md5 of=~/Desktop/USB_COPY.dd bs=512
```

Three Rules For Hashes

- You can’t predict the hash value of a file
- No two hash values can be the same
- If anything changes in the file or device, the hash value must change

Secure Hash Algorithm (SHA)

- National Security Agency developed hash functions
- Five algorithms: *SHA-1*, *SHA-224*, *SHA-256*, *SHA-384*, and *SHA-512*.
- SHA-1 produces a message digest that is 160 bits long;
- SHA-224 produces a 224-bit hash.

Example commandline = sha1sum {file}

Hash Validation

Calculate the Hash value and match to original evidence

- Evidence must maintain the same value as copies
- Hash value tools can validate disk images to original

- **HashCalc**
- **MD5 Calculator**
- **HashMyFiles**
- **Md5sum**
- **Chaosmd5**
- **Autospy**
- **dc3dd**
- **Etc. etc. etc. etc.**

=

79054025
255fb1a2
6e4bc422
aef54eb4

Common Hash Algorithms

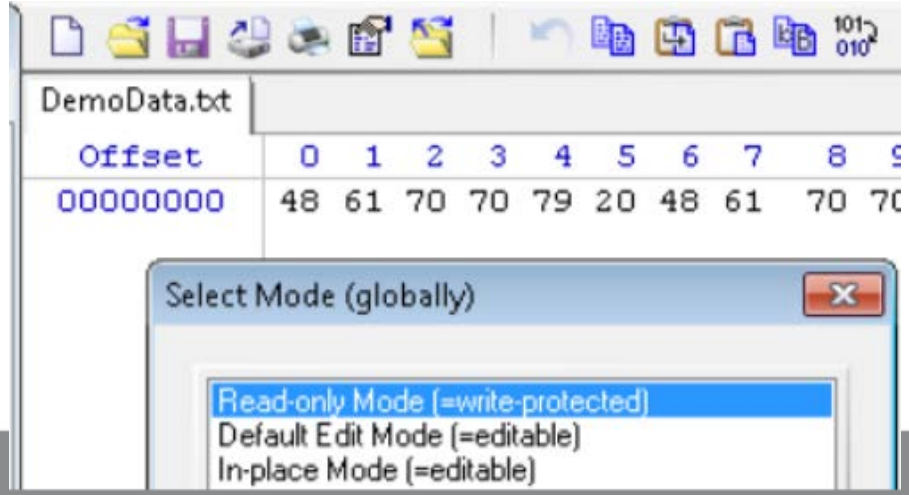
- MD5 – 128 bit hash value
- SHA-1 - produces a 160 bit hash value
- SHA-256 (bit) – 32 bit words (SHA 2 family)
- SHA-512 (bit) – 64 bit words (SHA 2 family)

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Operations	Collisions found?
SHA-0		160	160	512	$2^{64} - 1$	32	80	add, and, or, xor, rotate	Yes
SHA-1									Theoretical attack (2^{51})
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64} - 1$	32	64	add, and, or, xor, shift, rotate	No
	SHA-512/384	512/384	512	1024	$2^{128} - 1$	64	80		

Write Block

Ensure your investigation doesn't contaminate evidence by blocking Write so access is Read Only. (Hardware or software)

Windows - Show me - WinHex Example (www.winhex.com)



All Files Matter

- Forensic images contain all files including slack space and unallocated space
- Slack space and unallocated space is essentially seen as wasted space by the OS
- **Slack space** – space between file clusters
- **Unallocated space** – space where files are not written to according to the operating system

Artifacts such as deleted files, fragments and hidden data could be identified in slack space and unallocated space!

Lost Clusters

- Operating Systems could mark parts of a drive as bad or lost

- Lost clusters are marked used, but not allocated to any files

Example: File not closed properly or process is interrupted before saved correctly.

Bad Clusters

- Bad clusters marked as unusable space.
- Special software may be required to recover data depending on the cause of the bad data segment.
- Formatting a hard drive may have sectors labeled as bad during the process.

Secure Disposal

- **Deleting Data Spinning Disk** – Space allocated for replacement
- **Deleting Data Flash** – TRIM and Wear-Leveling algorithms may auto delete data
- **Forensic Delete** – Replacing data with 1's and 0's
- **Destroying Drives** – Recommend drilling, but magnets and other tools are available

Example: Foremost

- Run command **Fdisk –l**
- Identify device under “devices”
- Example USB stick

```
root@kali:~# fdisk -l
Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xaaea4a6f

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 60262399 60260352 28.8G 83 Linux
/dev/sda2       60264446 62912511  2648066  1.3G  5 Extended
/dev/sda5       60264448 62912511  2648064  1.3G 82 Linux swap / Solaris


Disk /dev/sdb: 1.9 GiB, 1992294400 bytes, 3891200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: C8330CA1-00D6-4C78-9E8E-3136D5F8ABB4

Device     Start     End Sectors  Size Type
/dev/sdb1   2048 3889151 3887104  1.9G Microsoft basic data
root@kali:~#
```

- Create a folder to store your data. Run the following command:
  - **Formost –t all –t –i <location to scan> -o <where to send what is found>**
- Example

```
foremost -t all -v -i /dev/sdb1 -o /root/Desktop/recover/
```

- Results will be organized in folder

Meta Data

- Data about data (i.e. who created it, when, etc.)

Kali - exiftool

- Download ***apt-get install exiftool***
- Run using the command ***exiftool <file>***

```
root@kali:/# exiftool /media/root/SP/joeymuniz.docx
ExifTool Version Number         : 10.31
File Name                       : joeymuniz.docx
Directory                       : /media/root/SP
File Size                       : 74 kB
File Modification Date/Time     : 2016:11:12 16:06:2
File Access Date/Time           : 2016:11:19 22:03:2
File Inode Change Date/Time     : 2015:01:24 16:55:0
File Permissions                : rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
```

Remediation: Eradication Techniques

- **Sanitization** – Returning the system to the corporate trusted state
  Golden Image | Data
- **Reconstruction / Reimage** – Reinstall corporate golden image

CSA+ speaks about this, however this step may destroy evidence about the attack!!!!

Collecting Windows Data with System Access

Process Memory

- Pmdump.exe
- Pd.exe
- Userdump.exe
- Adplus.vbs

Open Files

- PsLoggedOn
- Net Sessions
- LogonSession

Logged-In Users

- Net file command
- PsFile utility
- OpenFiles command

System Restore Points

- Rp.log
- Change.log.x files

Process Information

Pslist / Pslist –x

Tasklist

Fport

Listdlls

Registry Settings

- Reg.exe
- Win Registry Editor
- Regedit.exe
- Rededit32.exe

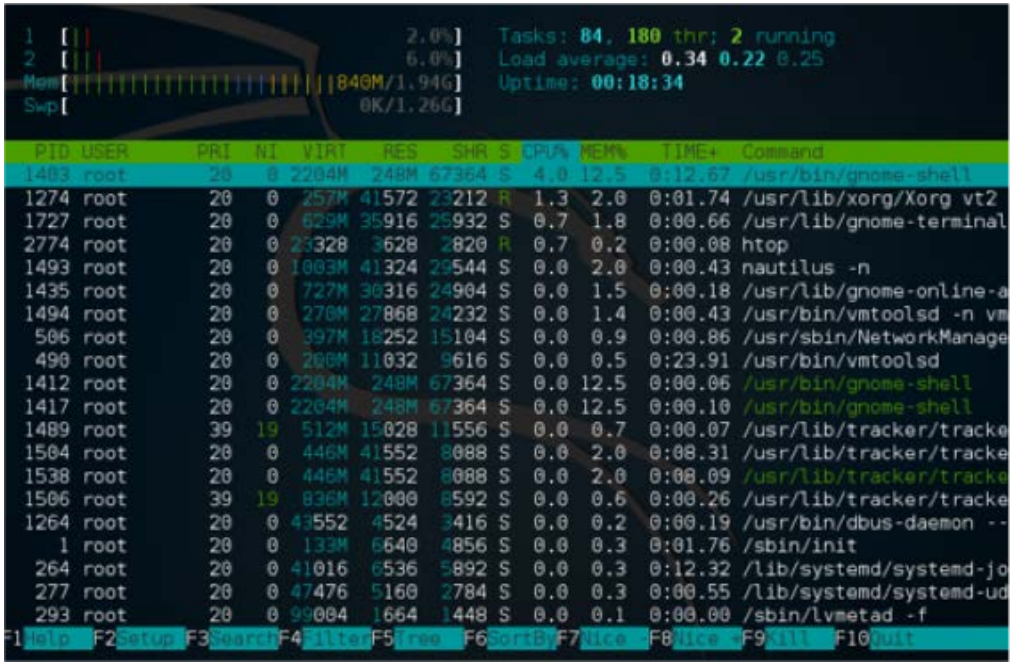
Other Common Things to Collect

- **Temporary Applications –** Windows stores user temp files at C:\Windows\(user name)\AppData\Local\Temp
- **Password Files** – Shadow / SAM
- **Coredumps and hibernation files** - Encryption keys typically stored in memory

Collecting Linux / MacOS Data with

System Resources

- top
- atop (apt-get this)
- htop (apt-get this)
- ps
- Df – available disk space
- Pstree
- Pgrep



Indications of a Compromised System

- Unusual Outbound Network Traffic
- Anomalies in Privilege User Account Activity
- Geographical Irregularities
- Unknown Logins
- Large Number of Request from Same File
- Mismatched Port-Application Traffic
- Suspicious Registry or System File Changes
- Unidentified Open Connections

Secure Development

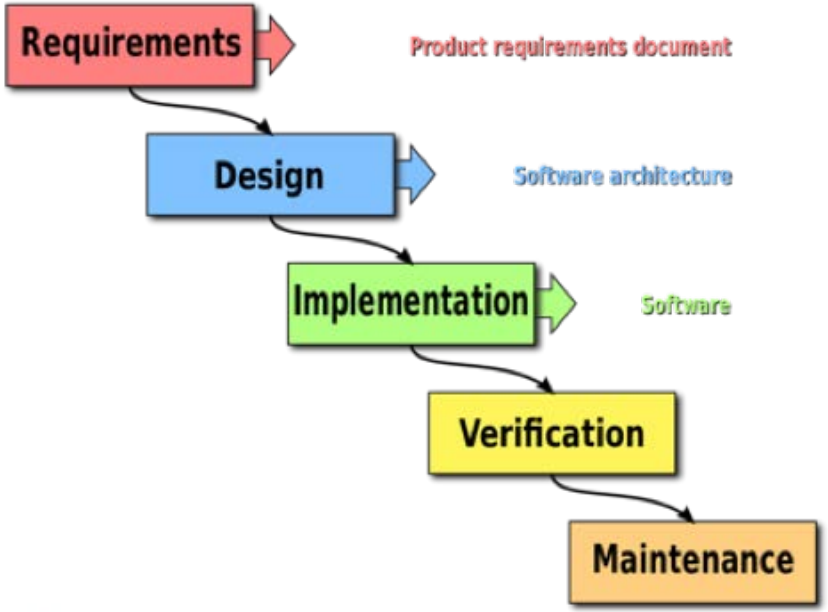
Pearson

Secure Software Development Life Cycle (SDLC)

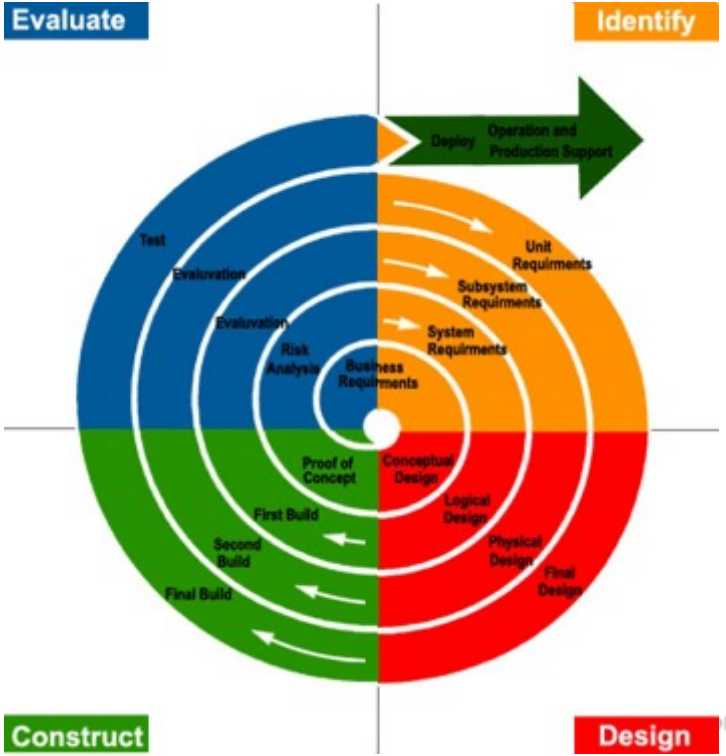
- Core Security Training
- Establish Security Requirements
- Establish Design Requirements
- Create Quality Gates / Bug Bars
- Perform Security and Privacy Risk Assessments
- Use Threat Modeling
- Perform Static Analysis
- Conduct Final Review
- Beta Testing

Design Model Examples

Waterfall

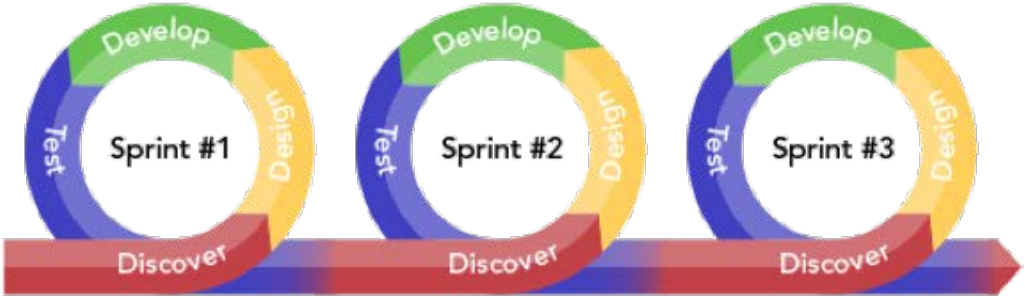


Spiral



More Examples

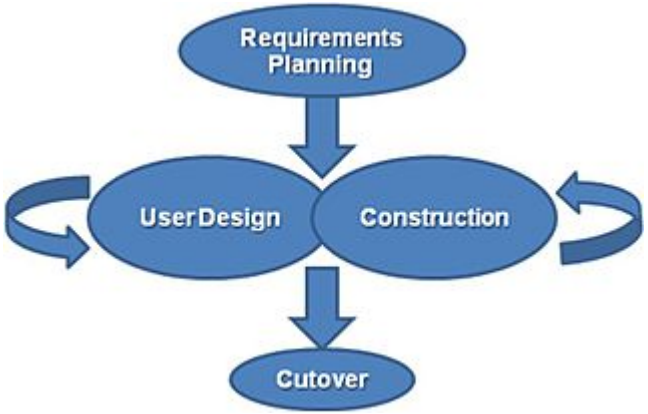
Agile Sprints



Agile Method

Note: Based on user stories
IE “Discovery”

Rapid Development



Quality Gates / Bug Bars

- Define minimum acceptable level of security and privacy quality
- Helps understand risks associated with security issues, identify and fix security bugs
- Improves overall quality of products produced

Security Testing Phases

- Static Code Analysis
- Web App Vulnerability Scanning
- Fuzzing
- Interception proxy to crawl application
- Many others ….

Part of the SDLC Process

Secure Coding Best Practices

- Enforce coding policy
- Perform risk assessments
- User input validation
- Web application firewalls
- Error message management
- Database security
- Secure network traffic

- Secure sensitive information
- Ensure availability
- Monitor and logging
- Manufacture authentication
- Secure sessions
- Cookie management

Static Code Analysis

- Part of the code review process (white box testing)
- Security Development Lifecycle using static (**non-running**) source code

Note: Dynamic code analysis uses running code and typically done with automated tools

Different Types Static Code Analysis

- **Data Flow Analysis** – Collect run-time information about data while in a static state
- **Taint Analysis** – Identify variables that are tainted with user controllable input

Fuzzing

- Fuzz testing is a blackbox software testing technique **(SENDING LOTS OF DATA) with attempt crash system**

- Finding and implementation bugs using malformed / semi-malformed data injection in an automated fashion

Fuzzing Examples

- Numbers (signed/unsigned integers/float...)
- Chars (URLs, command-line inputs)
- Metadata: user-input text (id3 tag)
- Pure binary sequences

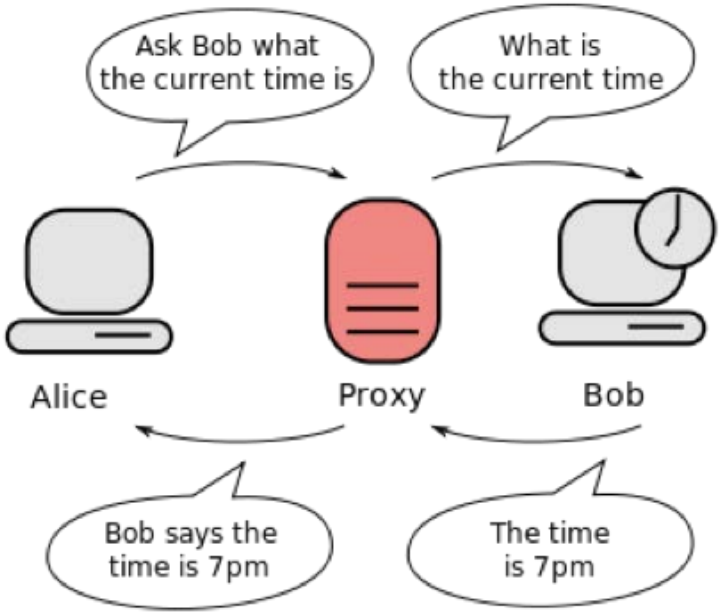
Fault Injection

- Similar to fuzzing but directly inserting faults into error handling paths.

- Inject at compile-time
- Abuse protocol flaws
- Inject during runtime

Interception Proxy

- Intermediary for requests from clients



Crawl and scan

- XXS
- SQL Injection
- Insertion points (cookies, HTTP headers, parameter names)
- Static code analysis
- View, edit, or drop individual messages

Manual Peer Review Best Practices

- Produce code review checklists for consistency
- Don’t single out developers for positive culture
- Review meaningful changes in code
- Mix human and tools
- Continuously monitor and track patterns of insecure code

User Acceptance Testing (Beta)

- Tested in real world with intended audience
- Option examples – In-house, paid group, beta release
- Record feedback for developers to make final changes

Stress Test Application

- Performance testing determining robustness, availability, and reliability under extreme conditions
- Sometimes called **Load Testing**

Post Test Symptoms

- Data loss or corruption
- Resource utilization unacceptable post stress
- Application fails to respond
- Unhandled exceptions

Regression Testing

- Testing changes to make sure older programming still works with new changes
- Run old test cases against new version
- **Example: New version has bugs from older version since Regression Testing wasn't used**

Input Validation

- Correct testing for any input that is supplied by something else

Example - Validating U.S. State Selection from Drop-Down Menu
Great against attacks like SQL injection!

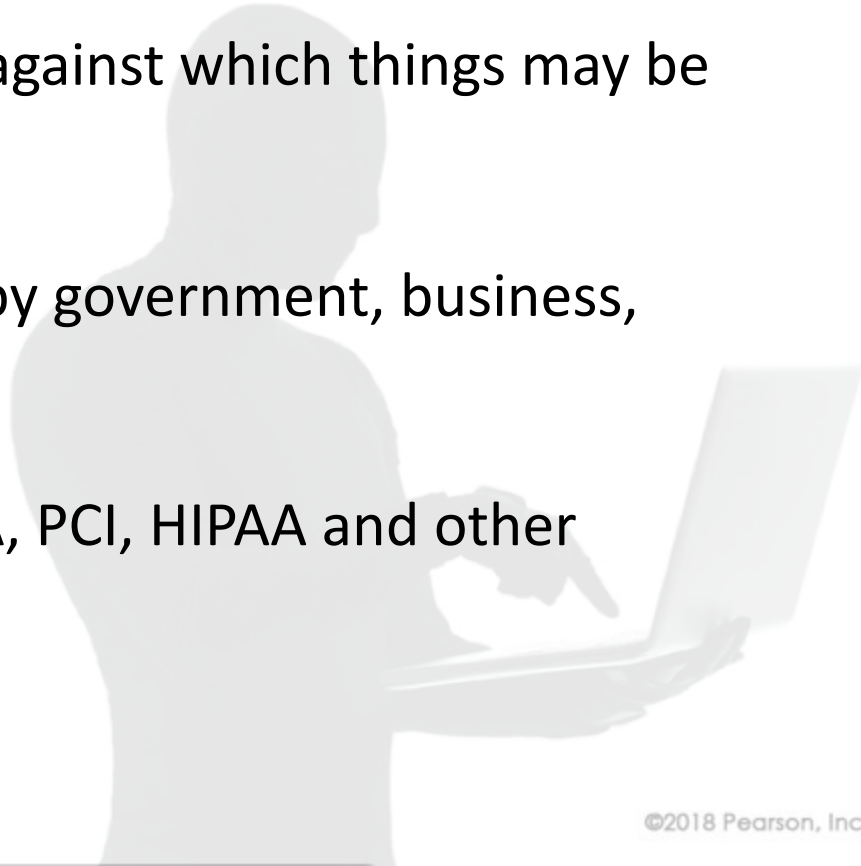
```
^(AA|AE|AP|AL|AK|AS|AZ|AR|CA|CO|CT|DE|DC|FM|FL|GA|GU|
HI|ID|IL|IN|IA|KS|KY|LA|ME|MH|MD|MA|MI|MN|MS|MO|MT|NE|
NV|NH|NJ|NM|NY|NC|ND|MP|OH|OK|OR|PW|PA|PR|RI|SC|SD|TN|
TX|UT|VT|VI|VA|WA|WV|WI|WY)$
```

Parameterized Queries

- Use pre-developed SQL statements verses variables.
- Targets preventing SQL attacks
- Different from input validation since input is already developed and you are selected existing statements

Benchmarks

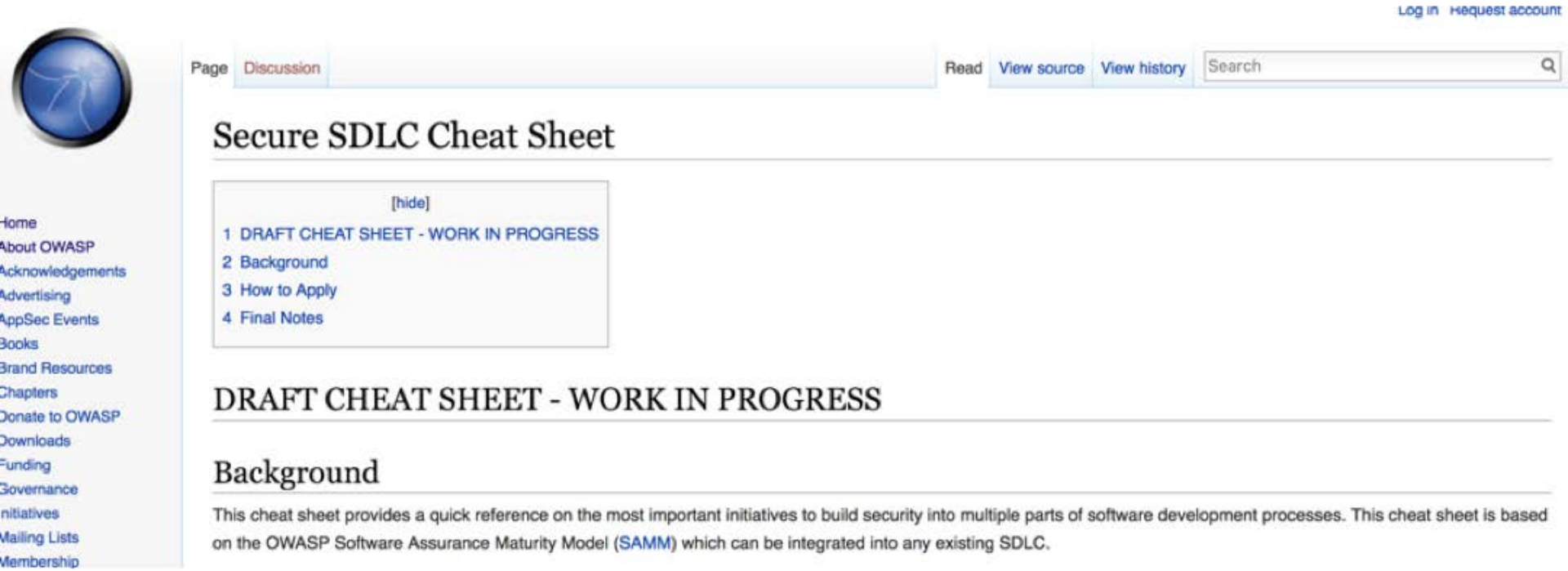
- Standard or point of reference against which things may be compared or assessed
- CIS benchmarks are respected by government, business, industry, and academia
- Can be used to help with FISMA, PCI, HIPAA and other security requirements



Open Web Application Security Project (OWASP)

- Worldwide non-profit focused on improving security of software
- All material is free and open software license
- LOTS OF MATERIAL
  - OWASP Testing guide
  - OWASP Guide to building secure web applications and Web Services
  - OWASP Code review guide

Models Exist (Example OWASP)



Log in Request account

Page Discussion Read View source View history Search

Secure SDLC Cheat Sheet

[hide]

1 DRAFT CHEAT SHEET - WORK IN PROGRESS
2 Background
3 How to Apply
4 Final Notes

DRAFT CHEAT SHEET - WORK IN PROGRESS

Background

This cheat sheet provides a quick reference on the most important initiatives to build security into multiple parts of software development processes. This cheat sheet is based on the OWASP Software Assurance Maturity Model (SAMM) which can be integrated into any existing SDLC.

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership

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**

- Research and education organization targeting cyber security topics
- Offers information security training and security certifications (more than 400 multi-day courses in 90 cities around the world)
- Maintains a collection of research documents covering various aspects of security topics

System Design Recommendations

- Also called CIS Controls designed to combat cyber attacks
- Concise, prioritized set of cyber practices
- Five critical tenets of an effective defense system
  - ***Offense Informs Defense***
  - ***Prioritization***
  - ***Metrics***
  - ***Continuous Diagnostics and Mitigation***
  - ***Automation***

Know What These Mean

- **Preventive Security** – Designed to block attacks and reduce vulnerability exposure
- **Collective Security** – Centralized data collection and correlation
- **Analytical Security** – Proactively identify vulnerabilities to enforce better security practices

Concept Review

Pearson

Concept Review

- Deploy vulnerability scanner across the network but afraid sensitive data will be seen. What do you do?

Encrypt between systems. Host agents

- What will Chmod 777 –Rv do?

Removes security – read, write view everything

- What does it mean when you send a ton of random data at something to test it for crashing?

Fuzzing

Concept Review

- What protocols can be used to profile a system?

Slides 80 – Netflow, DHCP, DNS, SNMP

- IPS Logs show different attacks. You are required to look at the logs and recommend remediation technology

Practice reading IPS logs

- Server is extremely vulnerable but can't be fixed for a few months. What can you do?

Secure around it … IE the networ

Concept Review

- Where is data found that is data fragments between files? (unallocated space, slack space, deleted space, formatted space)

  Slack Space

- What is a tool you can't use to create a forensic copy? (DD, FTK, RW, Encase) RW

- What is the first step for forensics after you collect a system?

  Slide 157 – Make a forensic copy

Concept Review

- How would you start a response to a incident?

Slide 46 – Preparation / Identification

- Which tool is best to prevent a rootkit? 1) IPS 2) AntiVirus 3) File integrity / Breach detection 4) Content filter?

File Integrity / Breach Detection

- All laptops must have the current security configuration template is a (policy, standard, procedure or guideline)?

Standard

Concept Review

- What if a user logs into a server and gets root. What can you do to reduce this risk?

  Remove Host privilege levels | Remove system from network (not isolation or segmentation at this point)

- What is a data source that is made up of multiple customer data that you can use to enhance your security?

  Threat Intelligence

- Which comes first for the SDLC?

  Slide 191 – Requirement Gathering

Concept Review

- What is a WAF?

  Web Application Firewall

- Which provides a single point of failure? Consolidation, Load Balancing, Process power, HA?

  Consolidation

- Why have a lessons learned report?

  Slide 145 – To improve from the breach

Concept Review

- Which would not be in a security policy? (Statement about cyber security, requirements for AES-256, delegation of authority, Designation of responsible executive)

AES-256 requirements

- What is it called when one person explains a concept while the other documents it?

Over the should review

- You find out a patch broke services. What practice can prevent this? (Vulnerability scanning, Regressive testing, secure code development, over the should review)

Regressive testing

Concept Review

- What type of control is a fire extinguisher (Logical, Physical, Administrative, Operational)? Physical
- Which authentication protocol is best for untrusted networks? (LDAP, TACACS+, RADIUS, Kerberos?) Kerberos
- Which software development module uses a four phase linear development? (Waterfall, Agile, RAD, Spiral) Sprial

Concept Review

- What type of firewall should be deployed to protect against SQL injection, XSS and other similar attacks? (Packet filter, Stateful firewall, NGFW, WAF)? WAF

- Which threat analysis detection is best for unknown threats (Trend, Signature, Heuristic, Regression) Heuristic

- Which tactic blocks software not permitted on host desktops? (Blacklisting, Whitelisting, Antimalware, Signature detection?

White-listing

Concept Review

- What is the file format of dd? RAW
- Which is a step of the recovery stage? (Rebuild a compromised system, Scanning, Destroy a hardd drive, Reporting) Scanning
- Which NIST publication covers cybersecurity incident handling (SP 800-53, SP 800-88, SP 800-69, SP 800-61) SP 800-61
- Which is not a purging activity? (factory reset, overwriting, block erase, crypto erase) Factory reset

Concept Review

- Which ISO standard covers security management controls? (27001, 9001, 82101, 1400) 27001

- What would a background check policy be considered? (physical, technical, logical, administrative)? Administrative

- Which model would you recommend describing 5 activities associated with IT service management ? (ISO 27001, TOGAF, ITL, COBIT)? ITL

Concept Review

- Which policy would cover how to destroy records? (Data deletion policy, password policy, data ownership policy, data retention policy) Data retention policy
- What tier of the NIST Cybersecurity framework is policy adaptive? (T1, T2, T3, T4?) T4
- Joey is writing a document listing acceptable rules for VPN access. What is this? (Policy, Procedure, Guideline, Standard) Standard

Concept Review

- Joey quotes a bill of materials as a contractor and later is asked to select which BOM to go with. What policy would prevent Joey from choosing his own BOM? (Dual controls, succession planning, management, separation of duties)

Separation of duties **(Dual control is when two people access one thing)

- Joey identified Julie fell for a phishing attack and lost her password. What technology would not help in the future? (user training, SIEM monitoring logins, NGFW, multifactor authentication? NGFW

Concept Review

- Joey first pushed the same security controls to all systems. Later, he decided to isolate systems based on functionality. What two design models are being covered? (Protective enclaves, threat based, Uniform protection design, information base, threat analysis based)

Uniform protection design / Protected enclaves

- Which is best for avoiding vulnerabilities in software updates? (AV, centralized patch management, OS patching standards, scanning)

Centralized patch management

Download The CTR Comic

https://tinyurl.com/ycwt2moz

https://tinyurl.com/y6uurzuu

jomuniz@cisco.com

Pearson