JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Intro to Threat Management

THREAT MANAGEMENT

What does this section cover?

- Identification of threats to your cybersecurity posture
- Methods to secure your networks
- Understanding of response and countermeasures
- Threats, Vulnerabilities, and Risk
- Footprinting and Reconnaissance

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Overview of Threat Management

- Threats to Confidentiality, Integrity, and Availability of your organization
- Coverage of the controls used to secure our networks and endpoints
- Evaluation of the security of controls
- Information gathering (passive and active reconnaissance and footprinting)

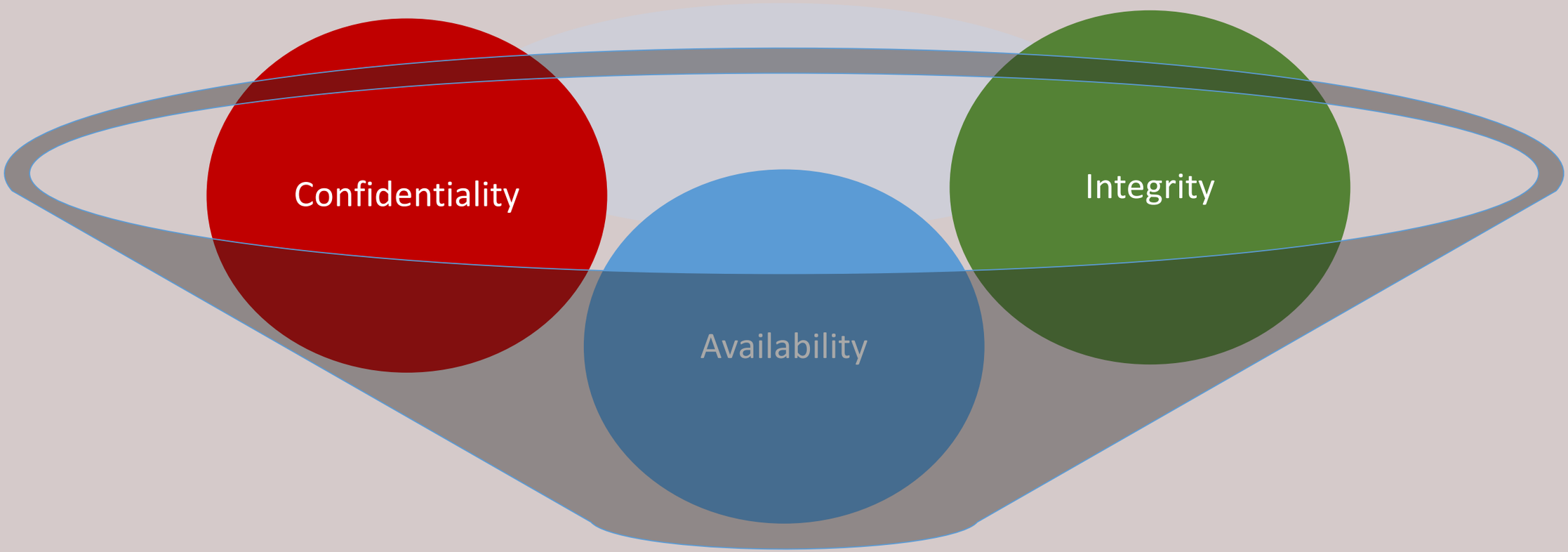
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Security Triad (CIA)

THREAT MANAGEMENT

COMPONENTS OF SECURITY (CIA)



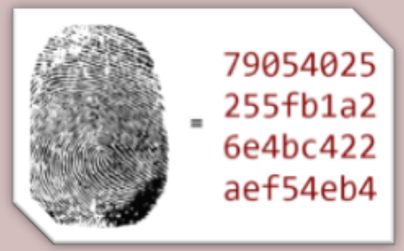
Information Systems Security,
Data Security, and Services

CONFIDENTIALITY

- How secure is the information?
- How secure does the data need to be?
- Best methods
  - Physical Protections
    - Locked doors, fences, security guards, security cameras, safes, …
  - Electronic Protections
    - Encryption (storage and in transit), passwords, firewalls, two-factor authentication, …
- Failure of confidentiality occurs if someone can obtain and view the data

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

INTEGRITY



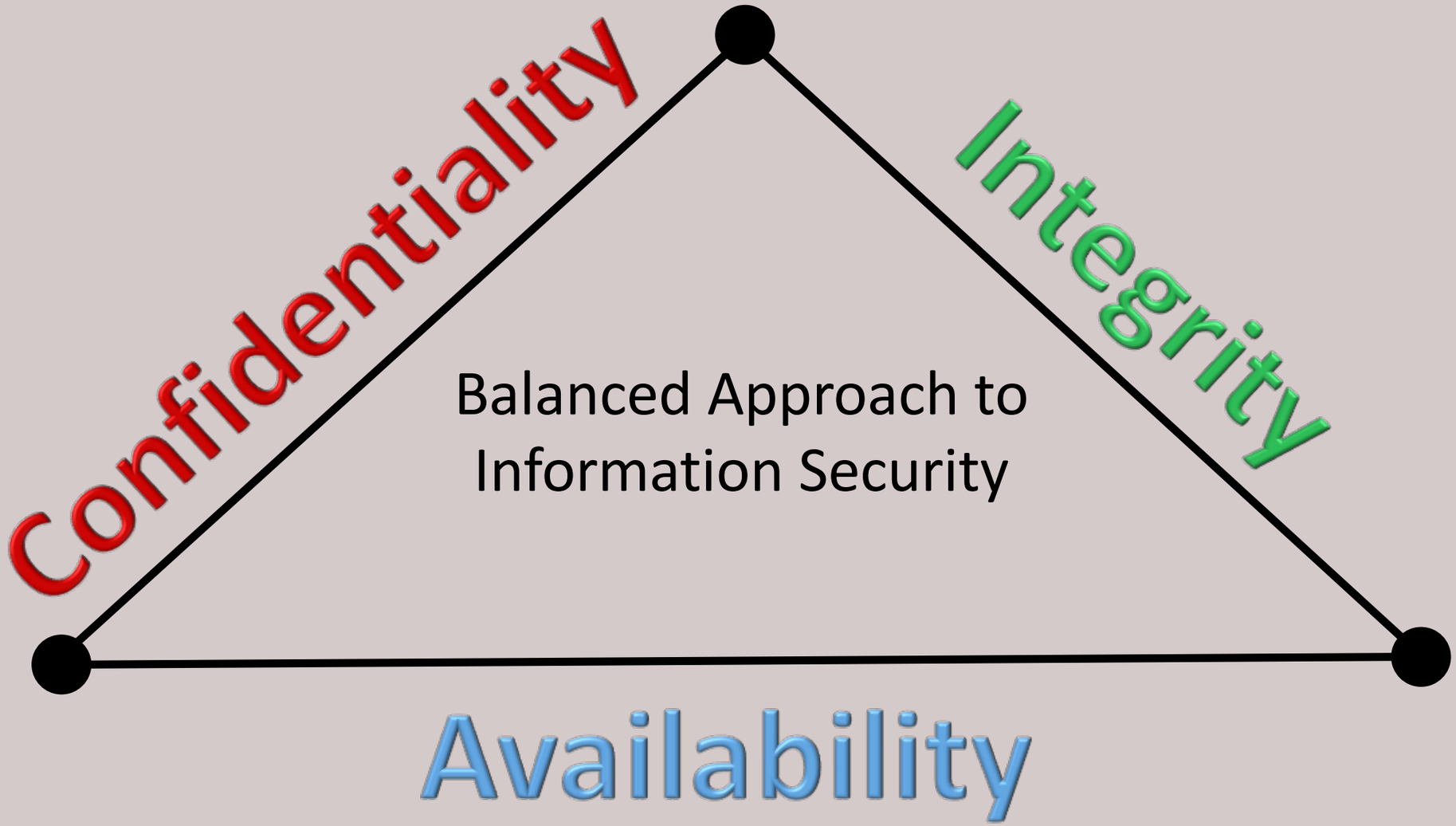
- How correct is the information?
- Has the data been modified during retrieval, in transit, or in storage?
- Best methods
  - Hashing of files and information
  - Checksums during data transmission
- Failure of integrity occurs if someone modifies the data being stored or when it is in transit

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

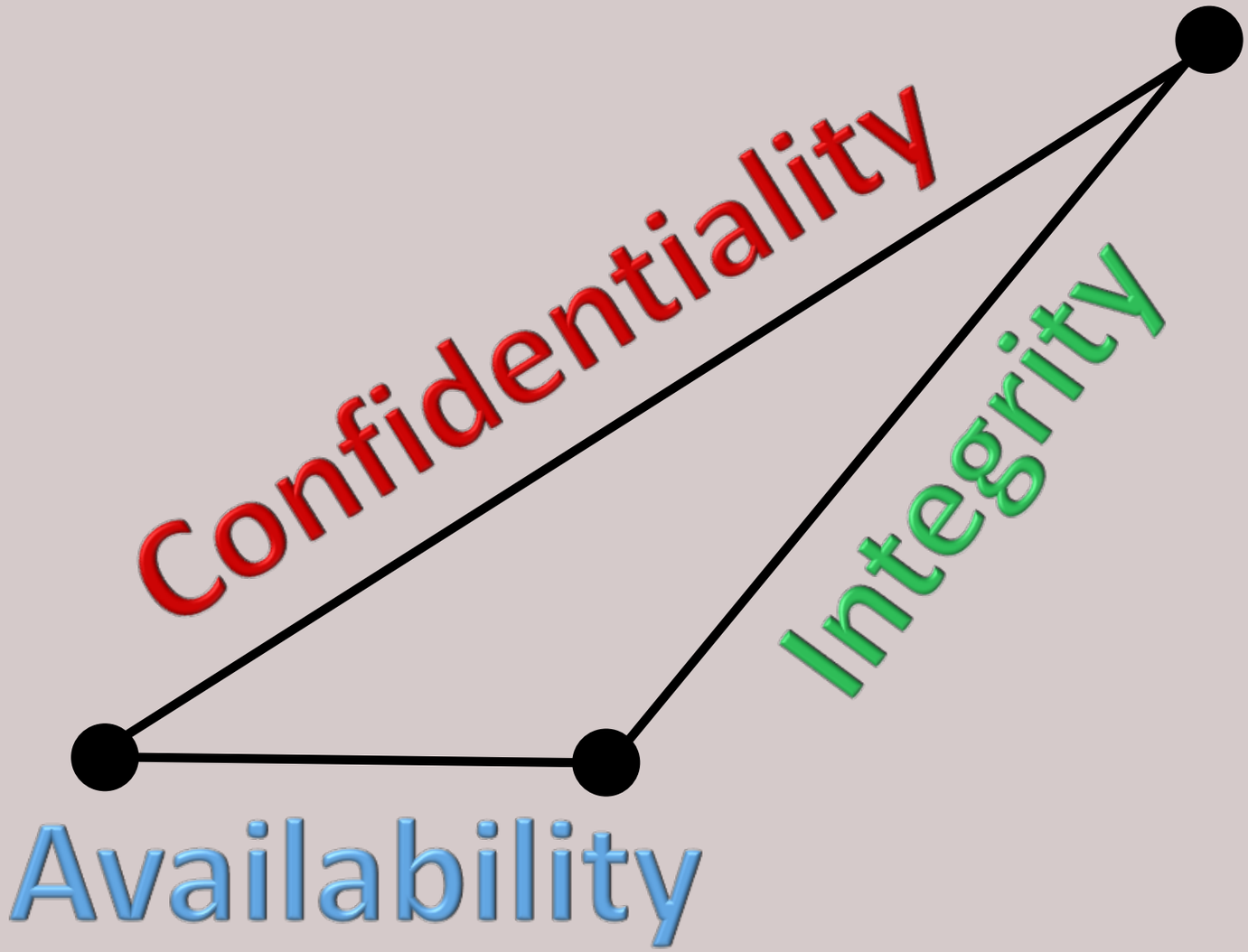
AVAILABILITY

- How much uptime is the system providing?
- Is the data accessible by users at all times?
- Best methods
  - Redundancy in the system design, including components and data paths
  - Backup strategies and disaster recovery plan
- Failure of availability occurs if the data cannot be accessed by the end user

APPROACHES TO THE SECURITY



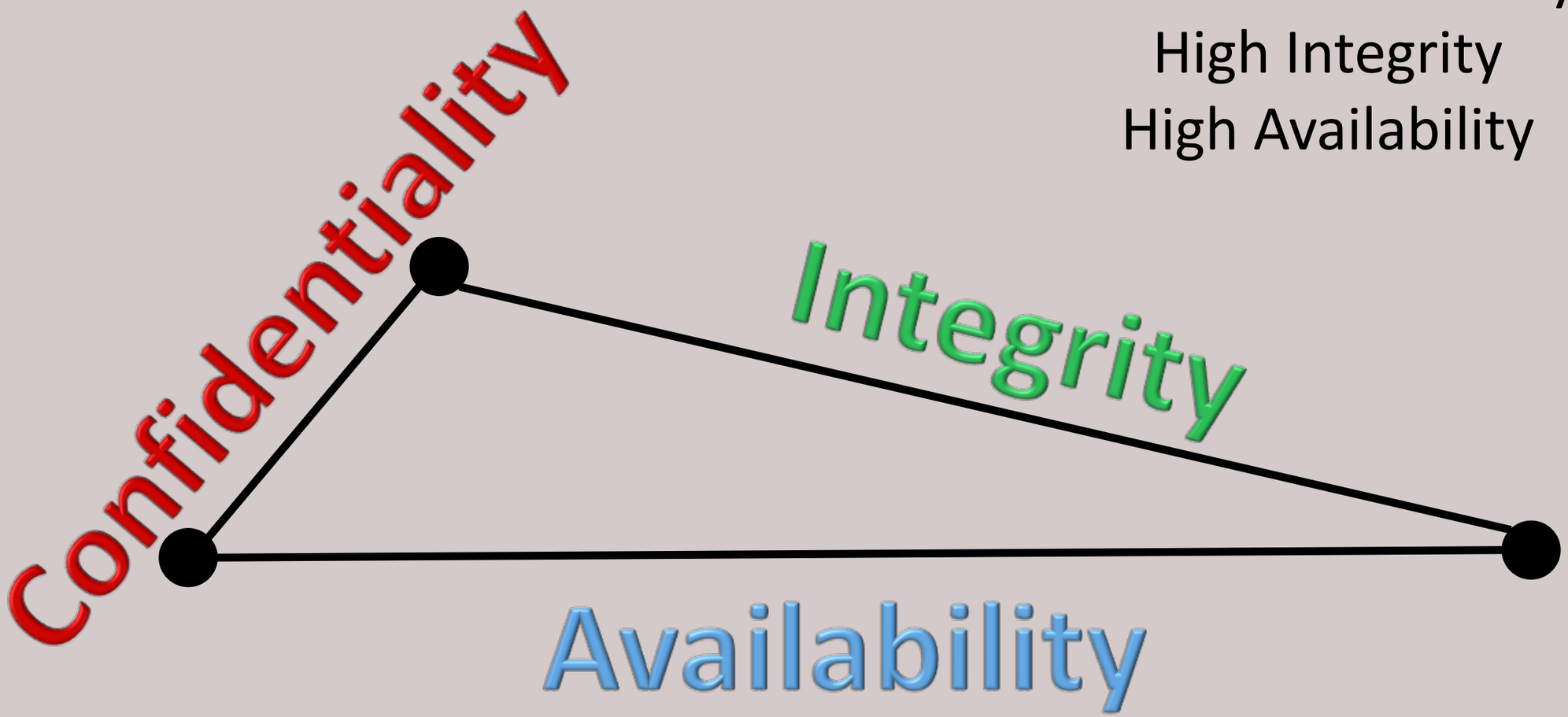
APPROACHES TO THE SECURITY



High Confidentiality
High Integrity
Low Availability

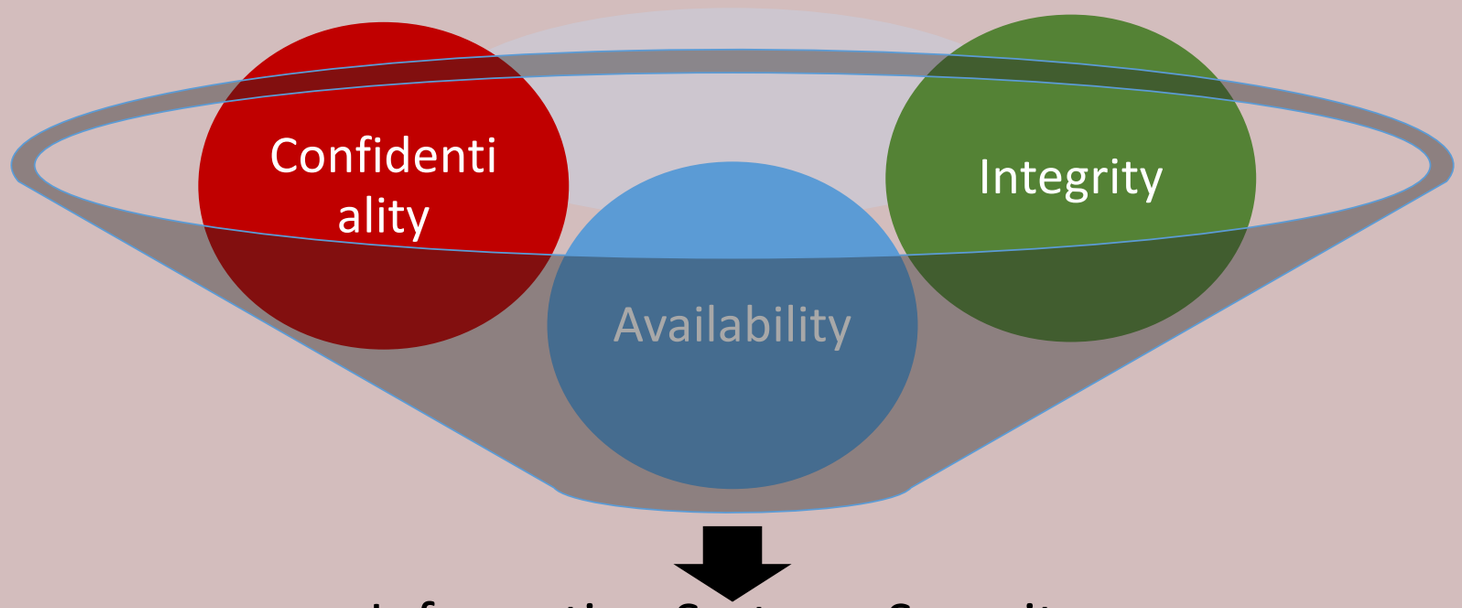
APPROACHES TO THE SECURITY

Low Confidentiality
High Integrity
High Availability



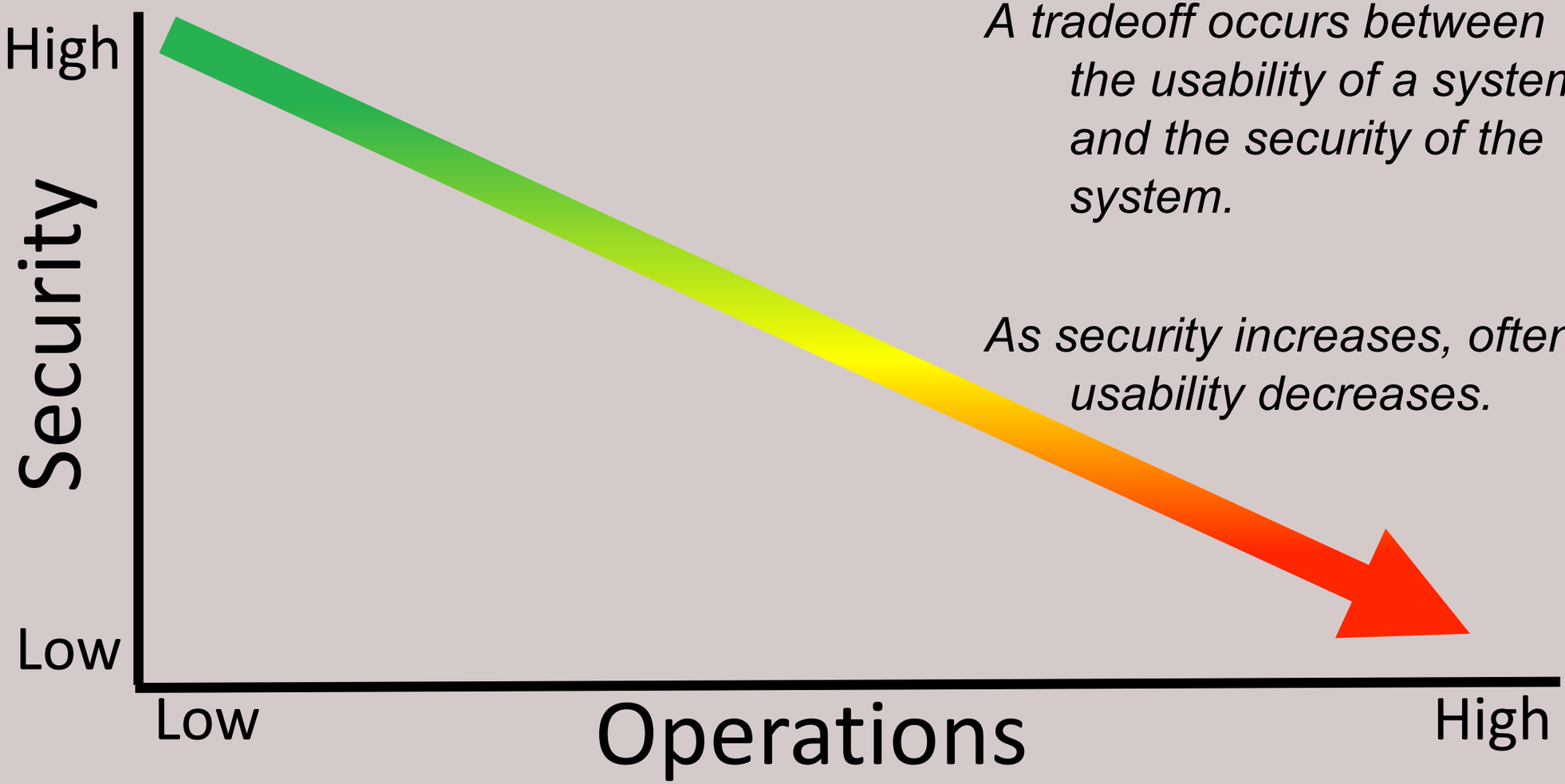
IMPORTANCE OF CIA TRIAD

- Cybersecurity analysts characterize risks, attacks, and security controls by assigning them to one or more of the CIA goals



Information Systems Security,
Data Security, and Services

SECURITY VS OPERATIONS



A tradeoff occurs between the usability of a system and the security of the system.

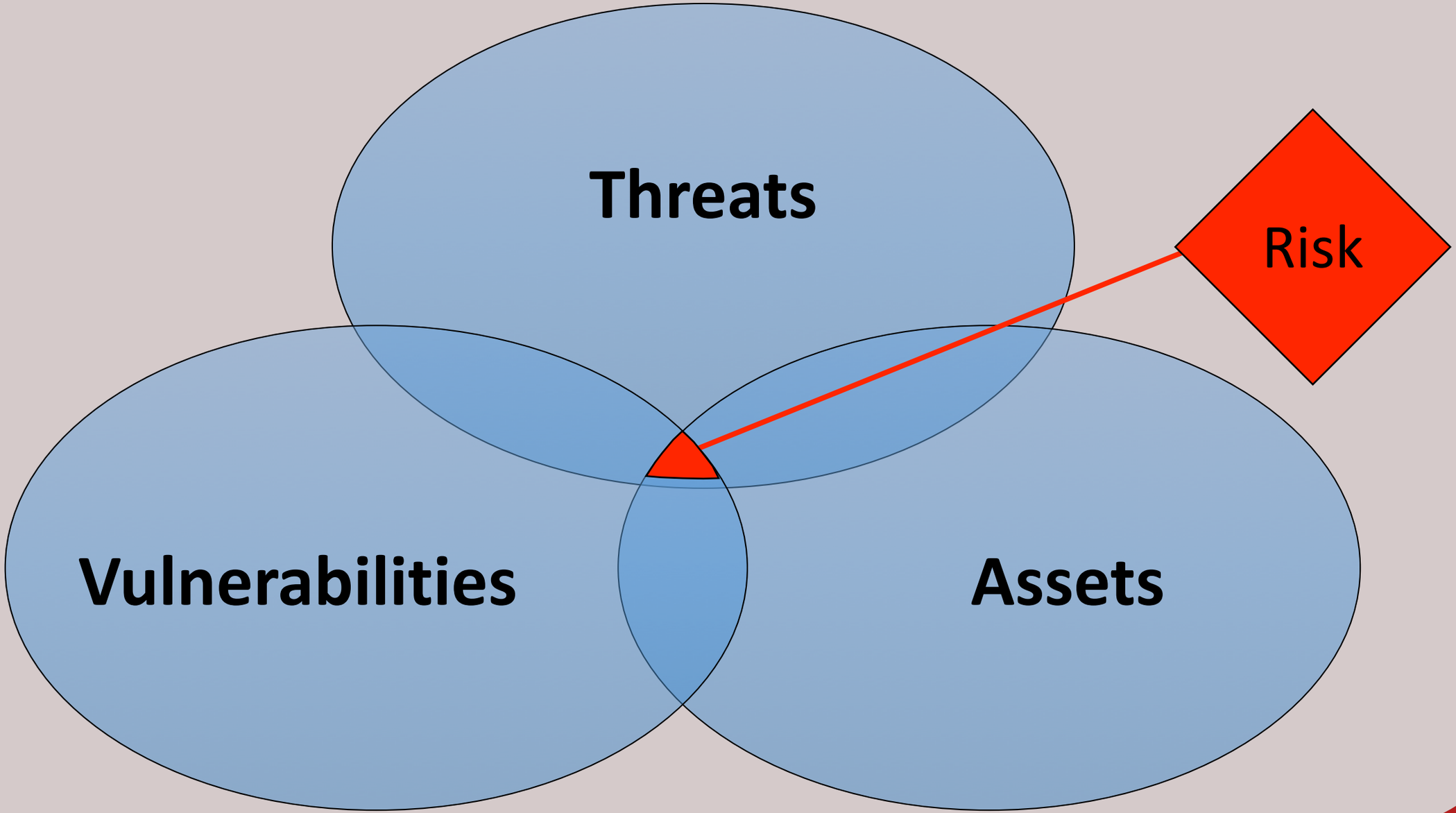
As security increases, often usability decreases.

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Risk Considerations

THREAT MANAGEMENT

WHERE RISK EXISTS...



ASSETS

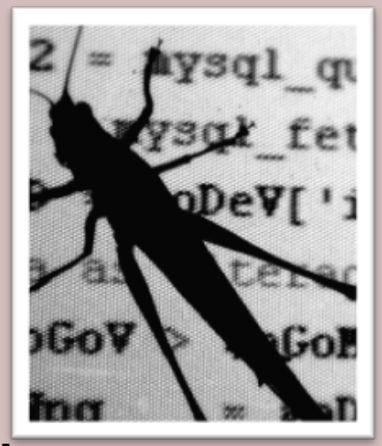
Any item that has a value to the organization

Examples:

- Information or Data
- Network Equipment
- Servers/Computers
- Software
- Personnel
- Processes

VULNERABILITY

Any weakness in the system design, implementation, software code, or lack of preventative mechanisms



Examples:

- Software bugs
- Misconfigured software
- Misconfigured network devices
- Improper physical security

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

VULNERABILITIES

- Cybersecurity professionals control vulnerabilities

- Vulnerabilities are internal factors

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

THREAT

Any condition that can cause harm, loss, damage, or compromise of an asset

Examples:

- Natural Disasters
- Cyber Attacks
- Breach of integrity of data
- Disclosure of confidential data
- Malware

THREATS

- Cybersecurity professionals cannot control threats, but they can be mitigated

- Threats are external factors

RISK

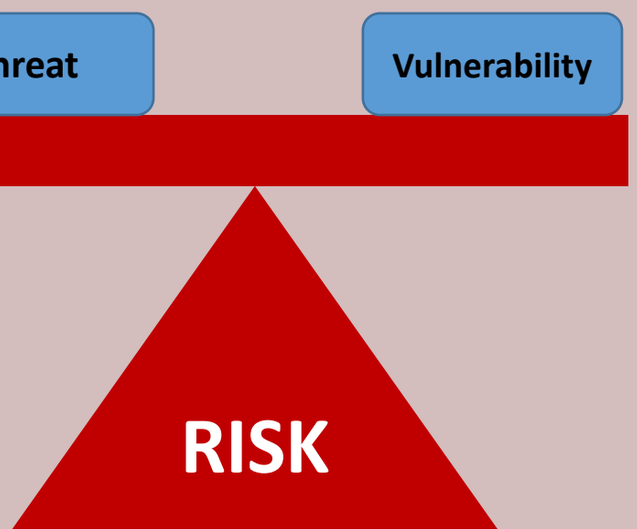
- Probability (or likelihood) of the realization of a threat

- Vulnerability without a threat equates to no risk…

RISK =

Vulnerability

X Threat



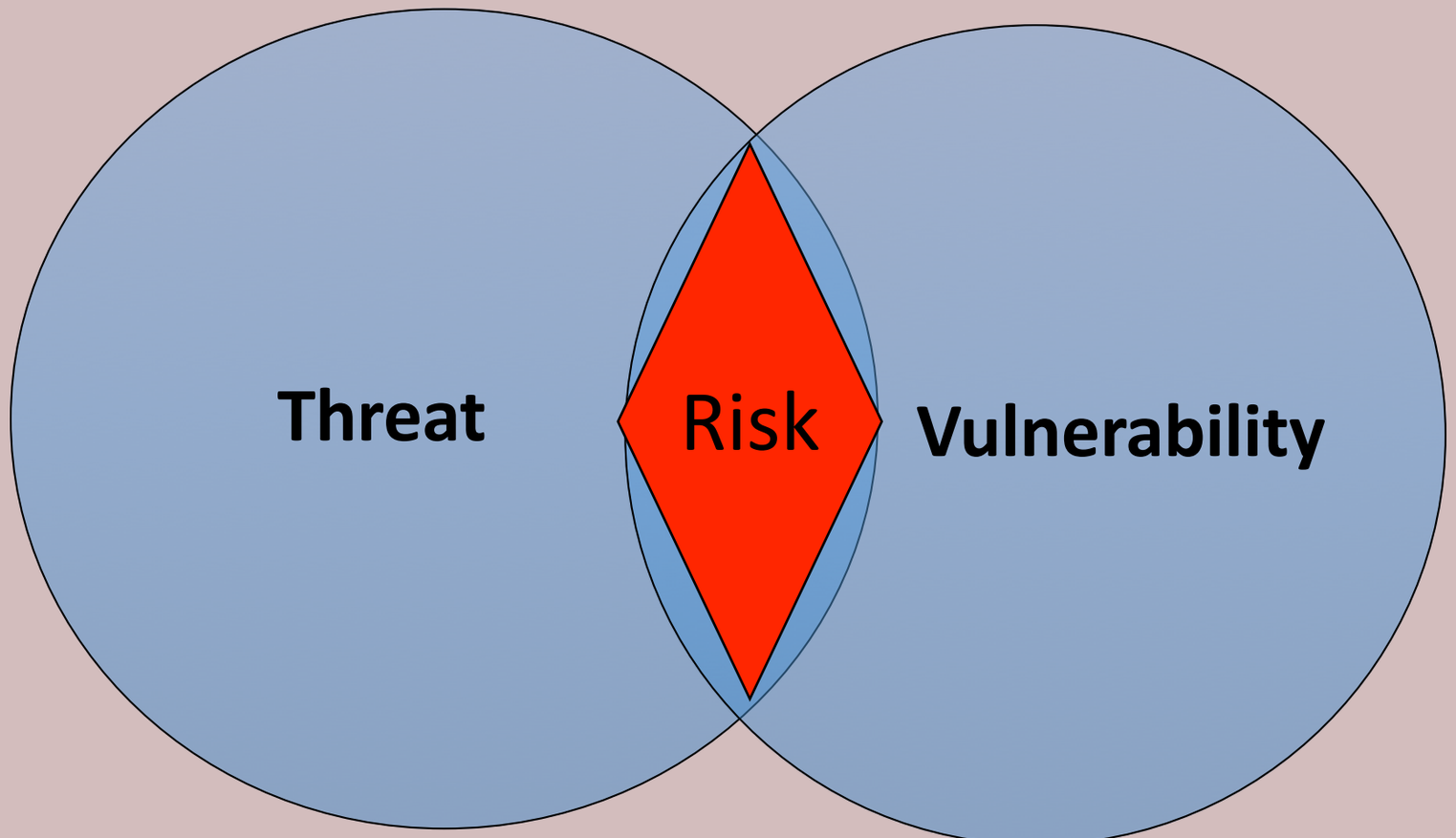
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Risk Assessment

THREAT MANAGEMENT

WHERE RISK EXISTS...



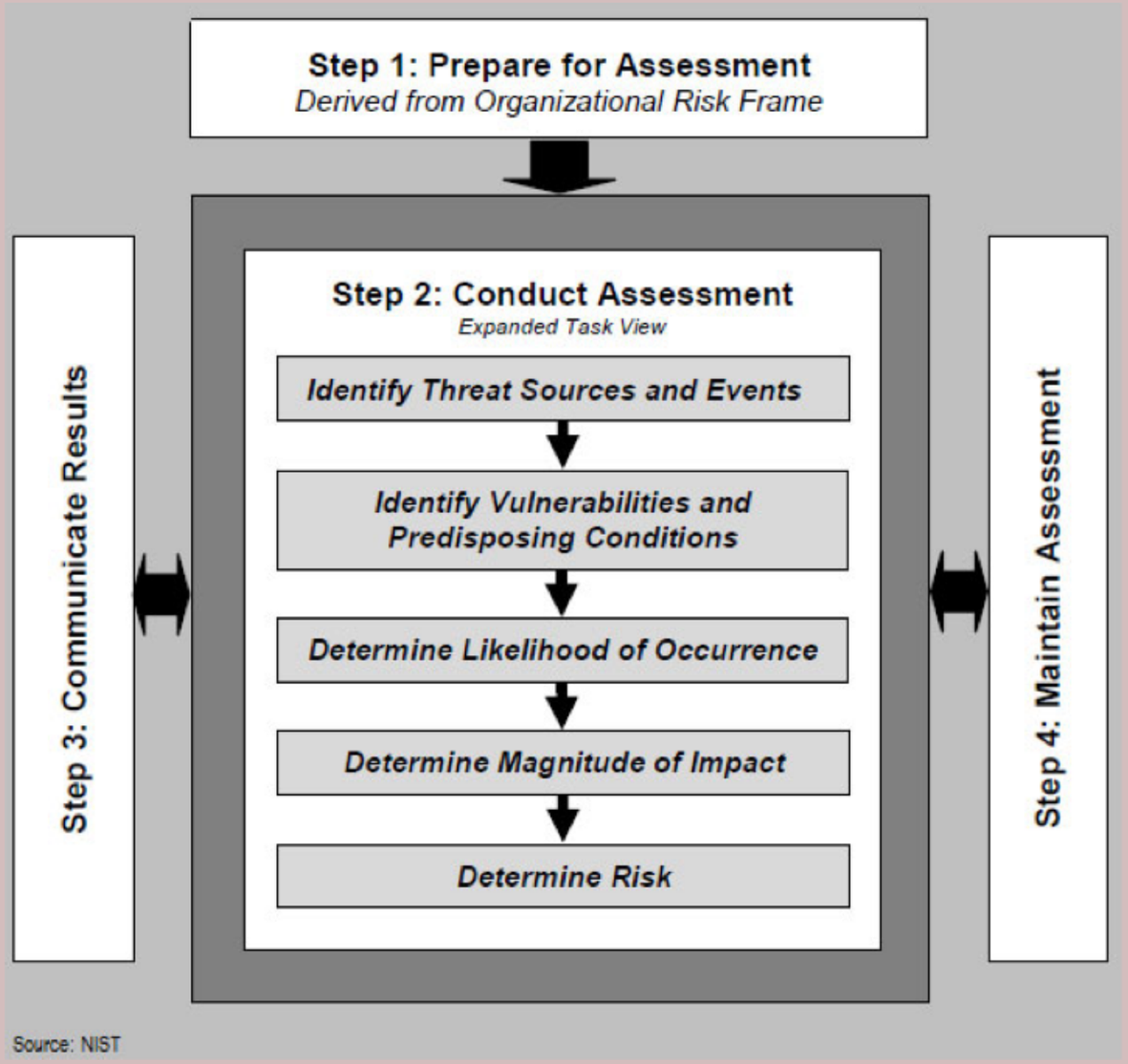
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

RISK ASSESSMENTS

- Organizations should conduct routine risk assessments
- Risk assessments measure your current level of risk based on threats, vulnerabilities, and mitigations in place
- National Institute of Standards and Technology (NIST) publishes NIST Special Publication 800-30 as a foundation for risk assessments

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

NIST SP 800-30



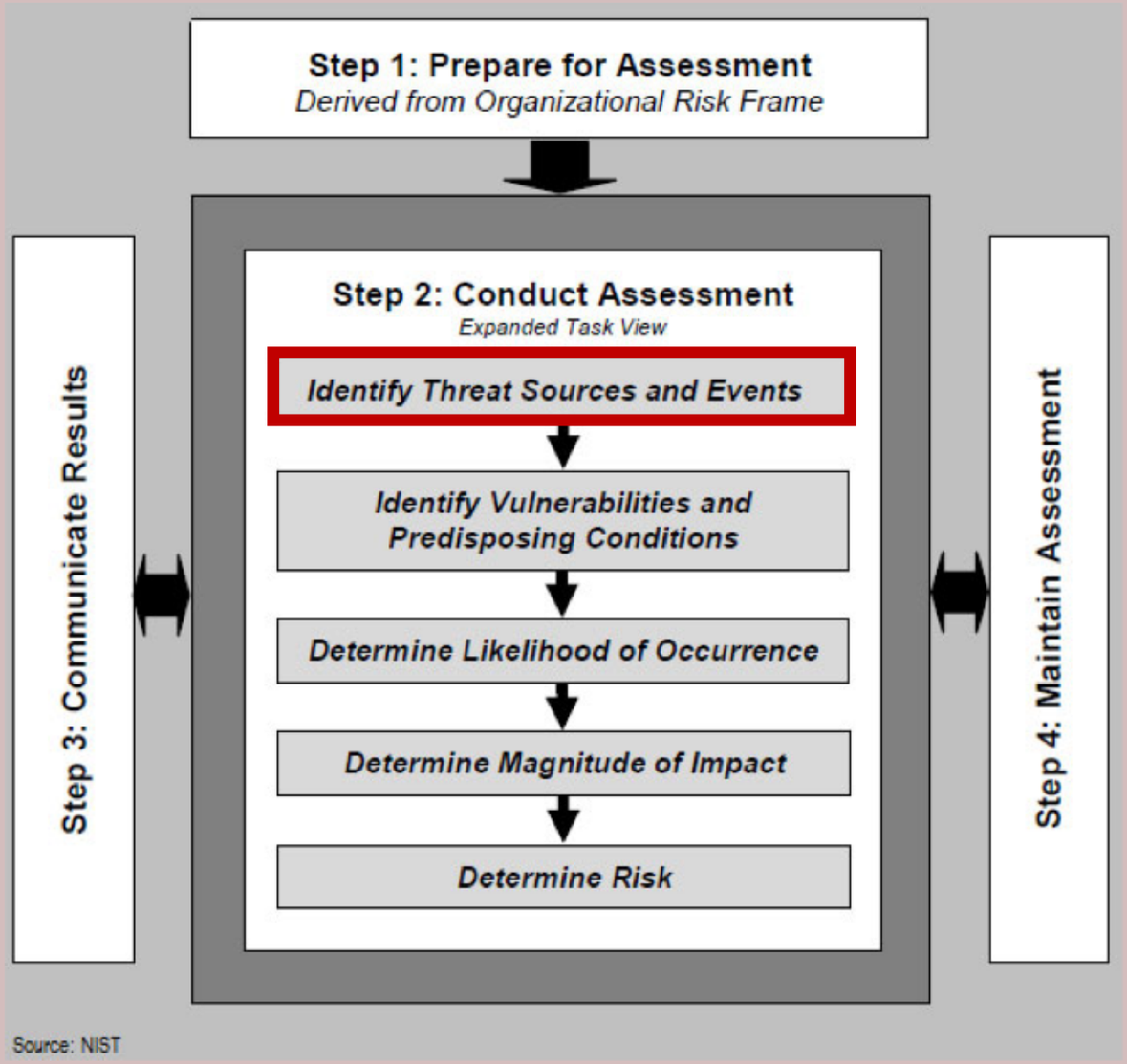
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identify Threats

THREAT MANAGEMENT

NIST SP 800-30



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identify Threats

- Adversarial Threats
- Accidental Threats
- Structural Threats
- Environmental Threats

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Adversarial Threats

- Consider their capability, intent, and likelihood

- Examples:
  - Trusted insiders
  - Competitors
  - Suppliers
  - Customers
  - Business partners
  - Nation states

Accidental Threats

- Occurs when someone makes a mistake that hurts the security of the system

- Example:
  - System administrator accidently takes servers offline causing loss of availability
  - Amazon Web Services (Feb 2017)
    - Technician utilized a SOP to take a small number of servers offline, but input the command incorrectly
    - Caused a large number of servers to go offline
    - It took down the entire US-EAST-1 region!
    - https://aws.amazon.com/message/41926/

Structural Threats

- Occurs when equipment, software, or environmental controls fail

- Example:
  - IT server fails due to hard drive failure
  - Servers fail due to overheating (HVAC fail)
  - Software failure (OS bug or crash)

Environmental Threats

- Occurs when natural or man-made disasters occur

- Example:
  - Fires
  - Flooding
  - Severe storms
  - Loss of power from the city power grid
  - Fiber or telecommunication lines cut

Always Remember…

- Threats come from both external and internal sources, but most risk assessors think of internal sources first…
- We aren't just worried about hackers, but also the trusted insider…
- As you design security controls, don't forget to think about disgruntled employees, inept administrators, or the insider threat!

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Best Practices

- It can be helpful to get copies of a similar organization's risk assessment to use as a baseline for your own organization

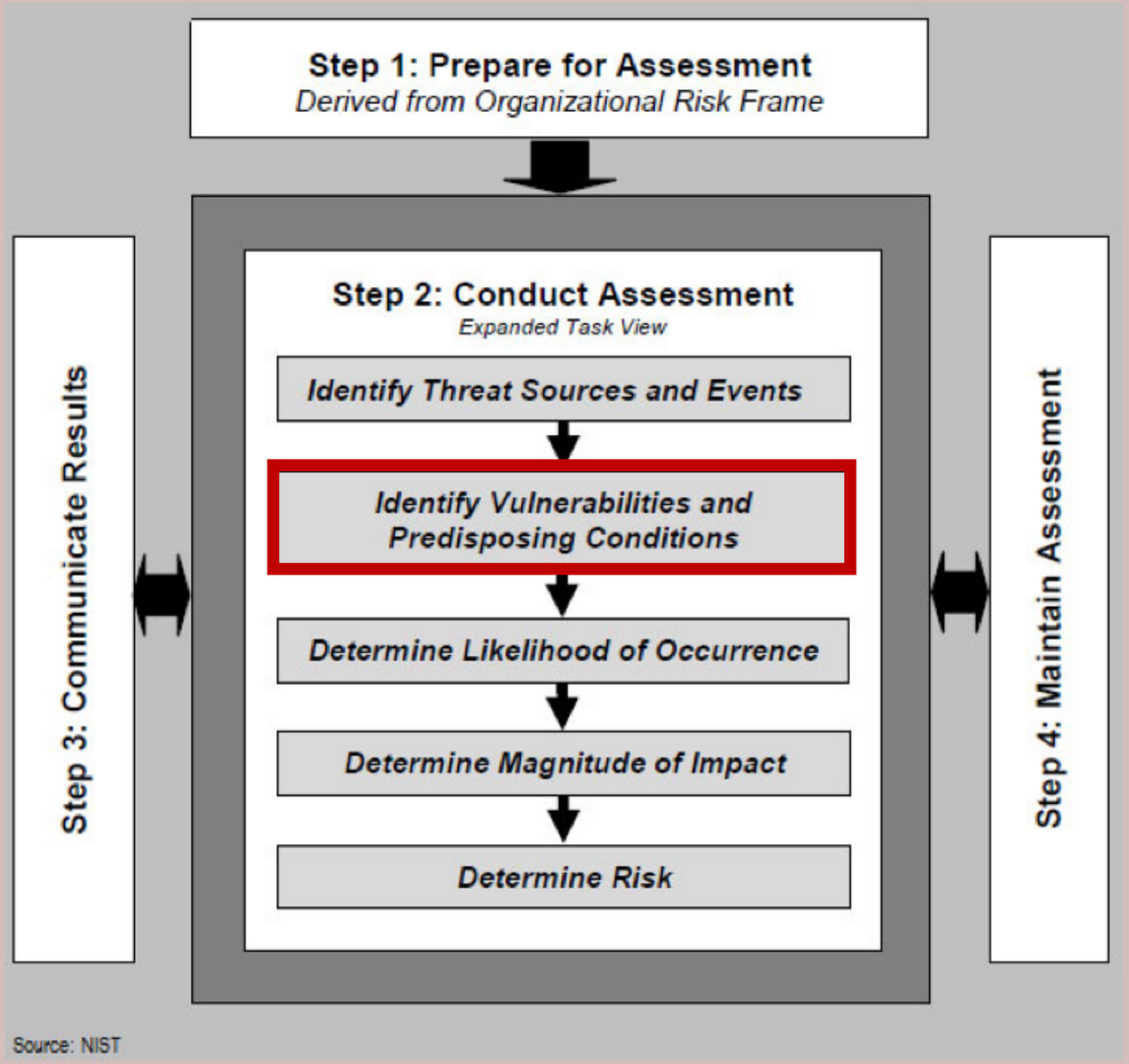
- Conduct quality assessment checks throughout the process to ensure you stay on track

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identify Vulnerabilities

THREAT MANAGEMENT

NIST SP 800-30



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identify Vulnerabilities

- During the identification of threats, we generally look external to the organization, but...
- Identifying vulnerabilities focuses on internal factors
- Our focus it to match up vulnerabilities to the threats identified

Always Remember…

- If you have a threat without a vulnerability, it isn't a risk.
  - Threat
    - Hackers are using a zero-day exploit against Windows XP systems
  - Vulnerability
    - We don't use Windows XP systems
  - Risk
    - NONE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Always Remember…

- If you have a vulnerability without a threat, it isn't a risk.
  - Threat
    - Hackers haven't found any exploitable coding errors
  - Vulnerability
    - Unpatched operating system software
  - Risk
    - NONE

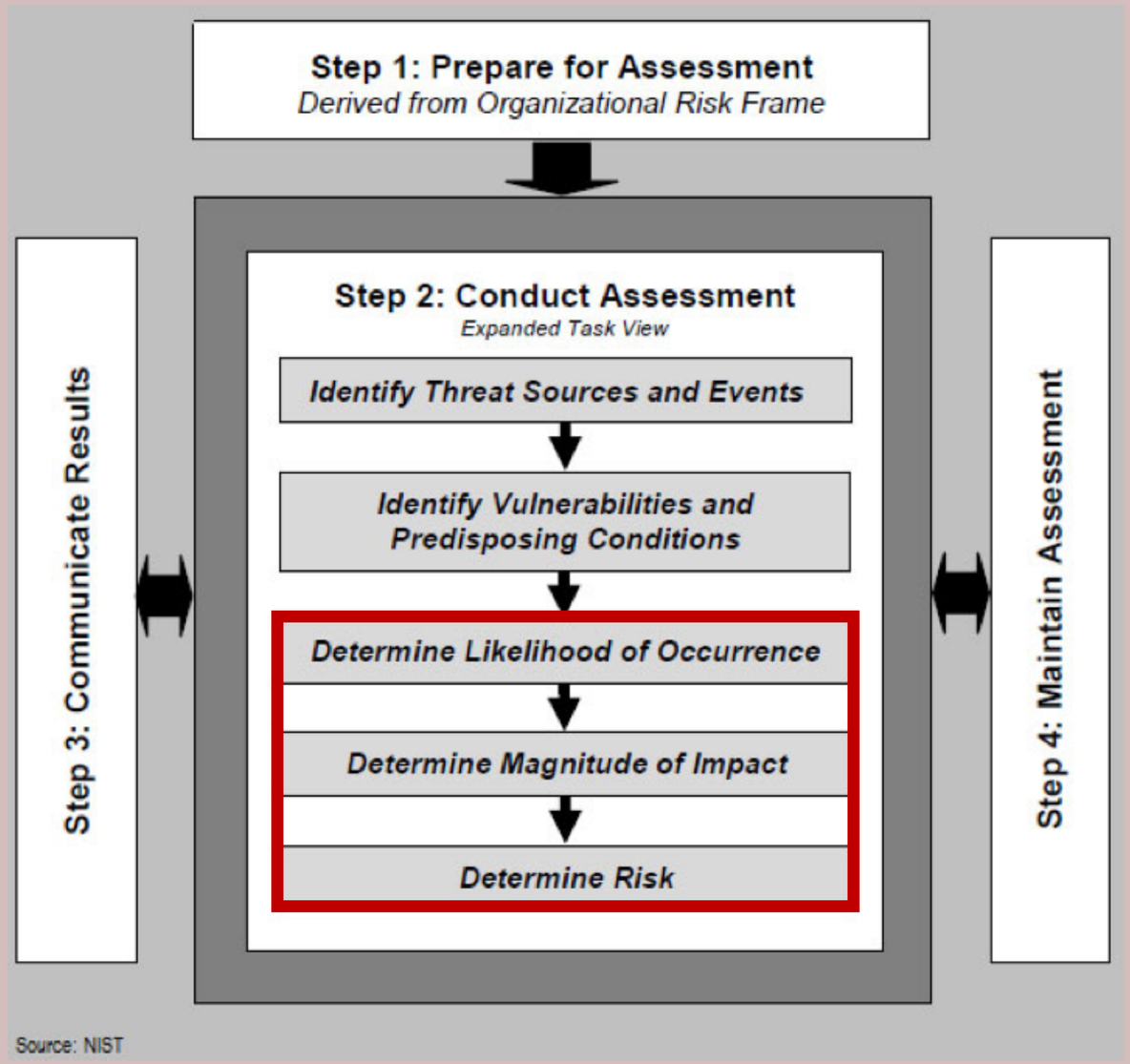
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Likelihood, Impact, and Risk

THREAT MANAGEMENT

NIST SP 800-30



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Likelihood and Impact

- Measurement of the risk that the combined threat and vulnerability pose is based on the likelihood and impact
- Likelihood is the chance that the risk will be realized
- Impact is the severity of damage that occurs if the risk is realized

Likelihood Factors

- What is the likelihood that the threat will initiate the risk?
  - Example: How likely is it that the hacker attack us?
- What is the likelihood that if the risk occurs it will have a bad impact for us?
  - Example: If the organization has proper security controls, the threat may be mitigated with no adverse affects to the organization.
- Likelihood is qualitative
  - Low, Medium, High

Impact

- Always assume the threat takes place and the risk is realized when measuring
- Identify the severity of the impact
- Consider each of the pieces of CIA triad: confidentiality, integrity, and availability
- Impact is qualitative
  - Low, Medium, High

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Qualitative and Quantitative Assessments

THREAT MANAGEMENT

Qualitative vs Quantitative

- Qualitative measurement is subjective
- Quantitative is based on numbers
- For the CompTIA CSA+ exam, you do not need to understand quantitative assessments, but they are covered on exams like CASP and CISSP.

Qualitative Example

LIKELIHOOD	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

IMPACT

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Qualitative Example

LIKELIHOOD	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

IMPACT

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Qualitative Example

LIKELIHOOD \ IMPACT	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

ANNUAL LOSS EXPECTANCY (ALE)

- Common calculation to determine the cost associated with risk

- Aids in determining when to accept, avoid, transfer, or mitigate the risk

ALE = Cost X Occurrences

If a risk would be actualized 3 times a year, then Occurrences equals 3.0.

If a risk would be actualized once ever 3 years, then Occurrences equals 0.33.

ANNUAL LOSS EXPECTANCY (ALE)

ALE = Cost X Occurrences

ALE = $1 million X 5.0

ALE = $5,000,000

Assume a theft of customer information costs a company $1 million per occurrence, and risk is large and expected to occur 5 times per year…
…Then, it makes sense to spend up to $5 million to mitigate this risk!

ANNUAL LOSS EXPECTANCY (ALE)

ALE = Cost X Occurrences

ALE = $1 million X 0.2

ALE = $200,000

But, if a theft of customer information costs a company $1 million per occurrence, and the risk that it occurs is only once every 5 years…
...Then, it would make sense to only spend up to $200,000 to mitigate this risk!

**** If it costs >$200,000 to mitigate, just accept the risk and pay $200k each time ****

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Risk Controls and Mitigations

THREAT MANAGEMENT

Risk Controls

- Cybersecurity professionals work to minimize risk to the organization through risk management and controls

- Four ways to handle risk:
  - Risk Acceptance
  - Risk Avoidance
  - Risk Mitigation
  - Risk Transference

RISK ACCEPTANCE

- Organization accepts the risk associated with a system's vulnerabilities and their associated risks

- Risk acceptance is common when the risk is low enough to not apply countermeasures, or adequate countermeasures have already been applied

RISK AVOIDANCE

- Risk is too high to accept, so the system configuration or design is changed to avoid the risk associated with a specific vulnerability

Example:

- Utilizing Windows XP is too dangerous, so we install Windows 10 instead to avoid the risk of an unsupported operating system

RISK MITIGATION

- Main goal of security is to minimize risk to a level acceptable to the organization
- Our goal is not necessarily to eliminate all risks…
- By adding risk controls, we can mitigate the risk down to an acceptable level

RISK TRANSFERENCE

- If the organization cannot afford to accept, avoid, or mitigate the risk, they can transfer the risk to another business

Example:

- If the organization is concerned that it would be too costly to recover from a flood, they can purchase flood insurance

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

RISK CONTROLS

- Technical controls
  - Systems, devices, software, and settings used to enforce CIA requirements
  - Examples
    - Using firewalls, IDS, and IPS
    - Installing antivirus and endpoint security

- Operational controls
  - Practices and procedures to increase security
  - Examples
    - Conducting penetration tests
    - Utilizing standard operating procedures

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

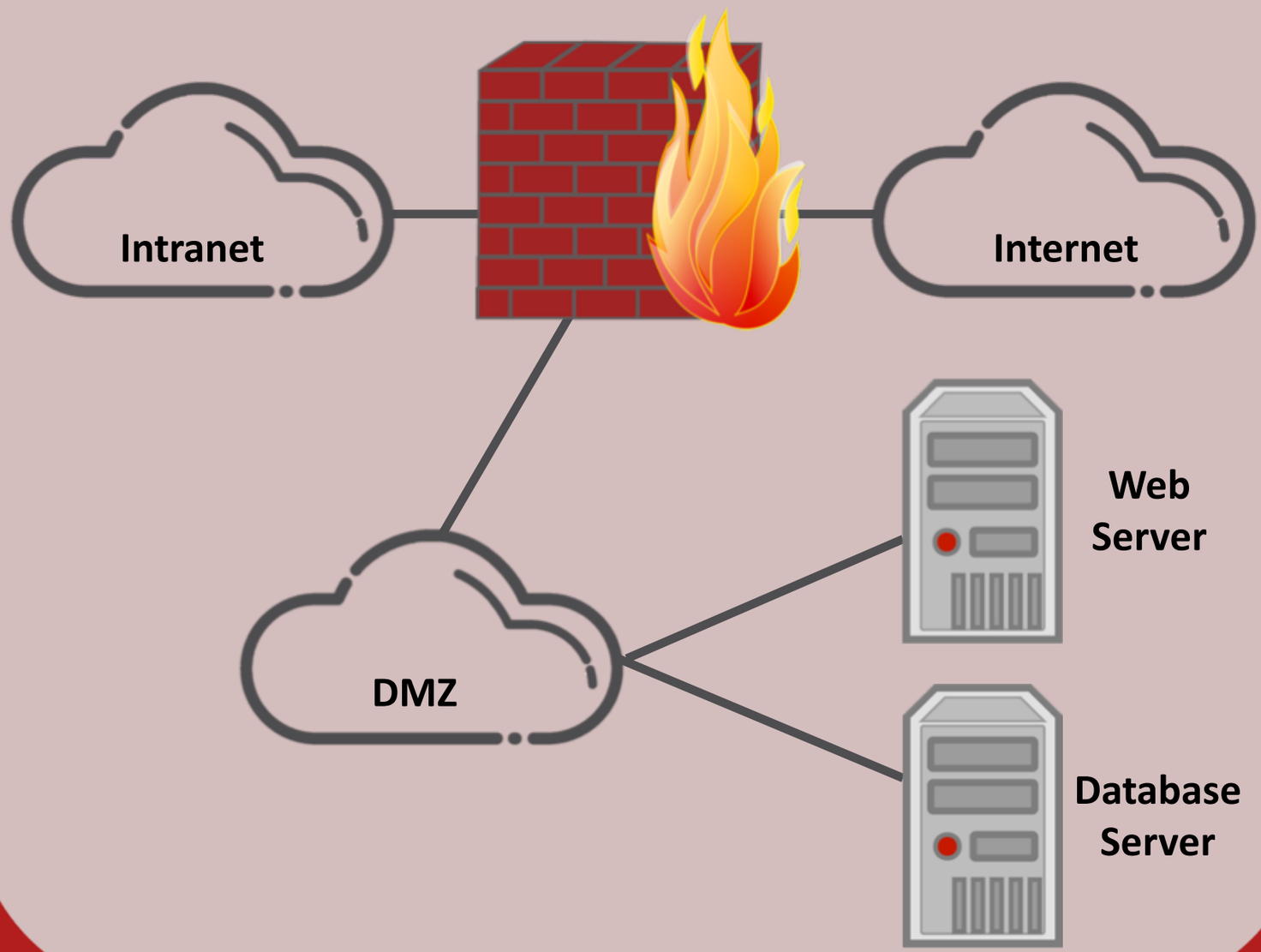
Network Perimeter Security

THREAT MANAGEMENT

Firewalls

- Most common network perimeter security
- Firewalls are at network boundaries
- Generally setup as triple-homed devices
  - Internet, DMZ, and intranet

Triple-Homed Firewalls

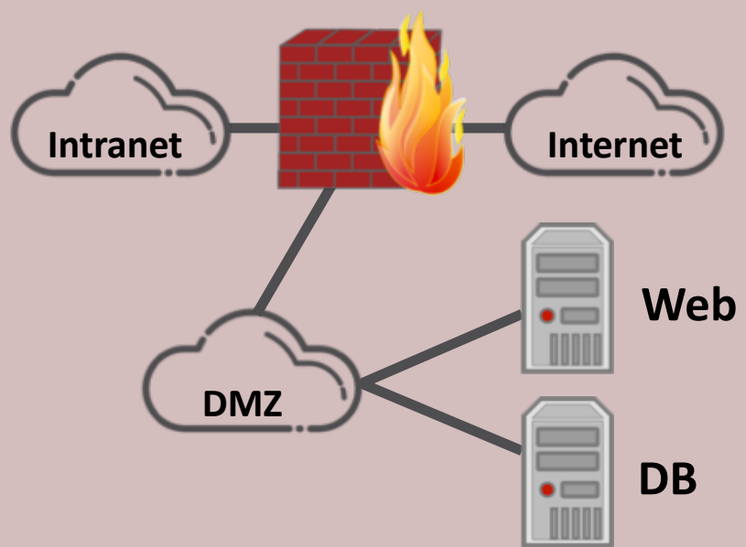


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Demilitarized Zone (DMZ)

- Special network zone hosting servers that gets traffic from the internet

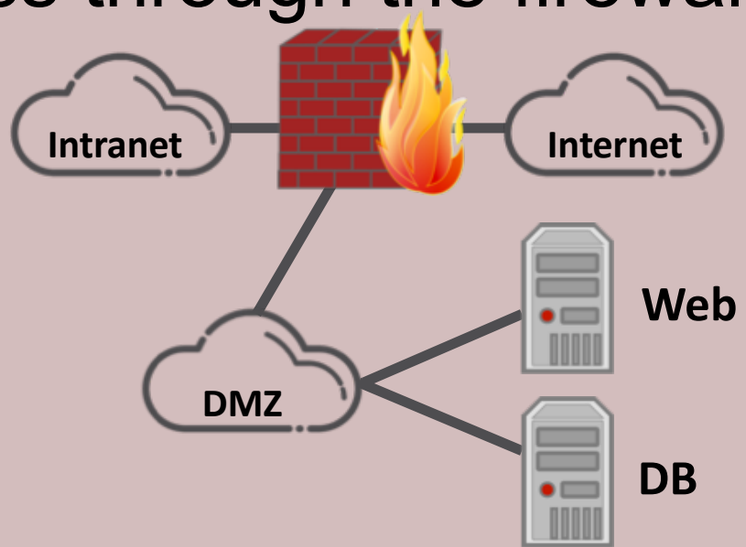
- Acts as an semi-trusted zone



Access Control List (ACL)

- All traffic passing through the firewall is checked against the ACL

- ACL contains rules to define what traffic can pass through the firewall



Access Control List (ACL)

- Firewall should be deny by default
  - If no rule says allowed, traffic is denied

Rule	SourceIP	Source port	DestIP	Dest port	Action
1	any	any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	any	any	any	Deny
3	any	any	192.168.120.1	any	Deny
4	192.168.120.0	any	any	any	Allow
5	any	any	192.168.120.2	25	Allow
6	any	any	192.168.120.3	80	Allow
7	any	any	any	any	deny

Firewall Types

- Packet Filtering
  - Check each packet against rules for IP and port
- Stateful Inspection
  - Maintains information about the state of each connection (basic firewalls sold today)
- Next-Generation (NGFWs)
  - Uses contextual information about users, apps, and processes to make decisions
- Web Application (WAFs)
  - Protects against web application attacks like SQL injection and Cross-site Scripting (SQL/XSS)

Common TCP Ports

Port	Service
20, 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
69	TFTP
80	HTTP
110	POP3
123	NTP

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Common TCP Ports

Port	Service
143	IMAP
161	SNMP
389	LDAP
443	HTTPS
1433	SQL Server
1521	Oracle
1720	H.323
1723	PPTP
3389	RDP

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

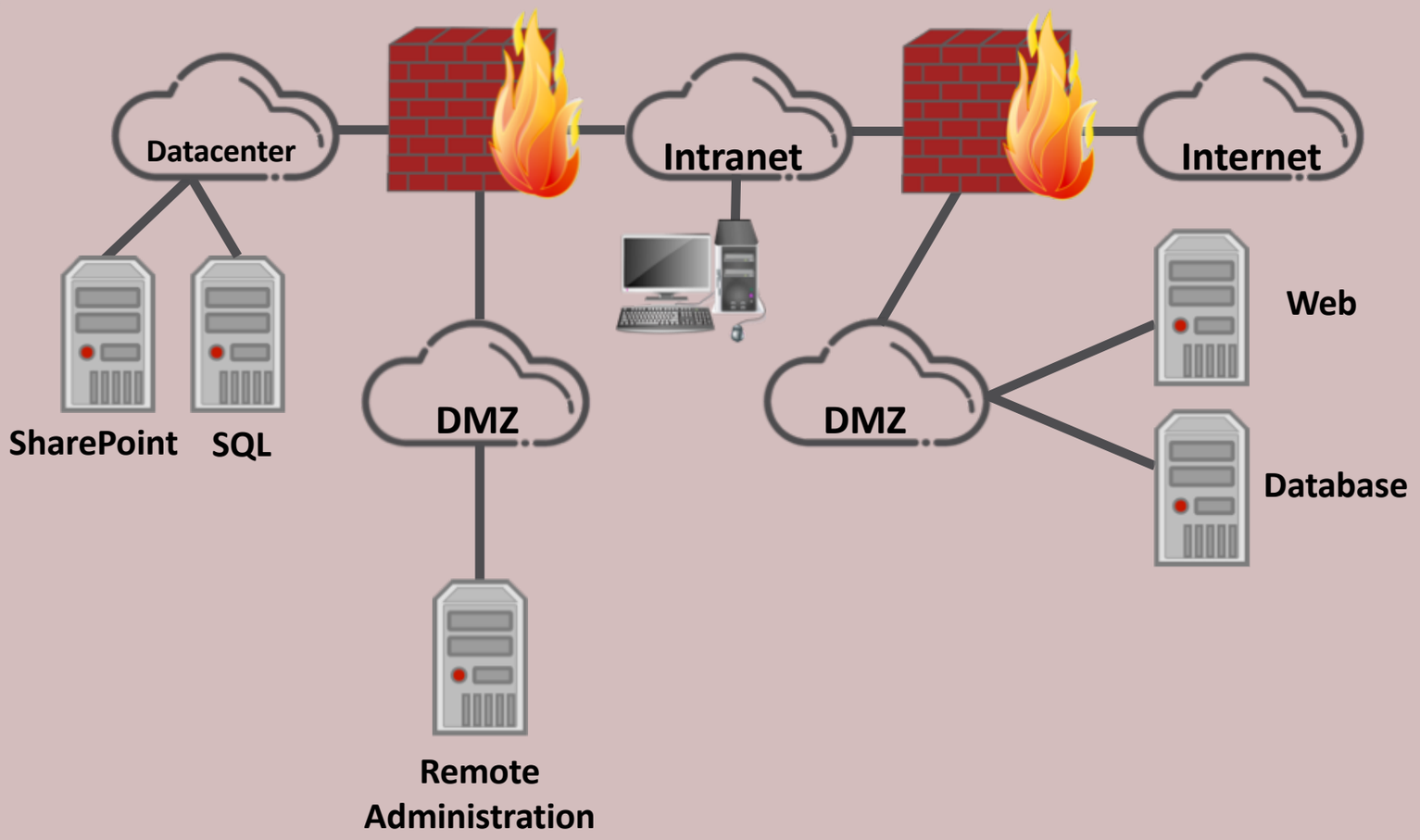
Network Segmentation

THREAT MANAGEMENT

Network Segmentation

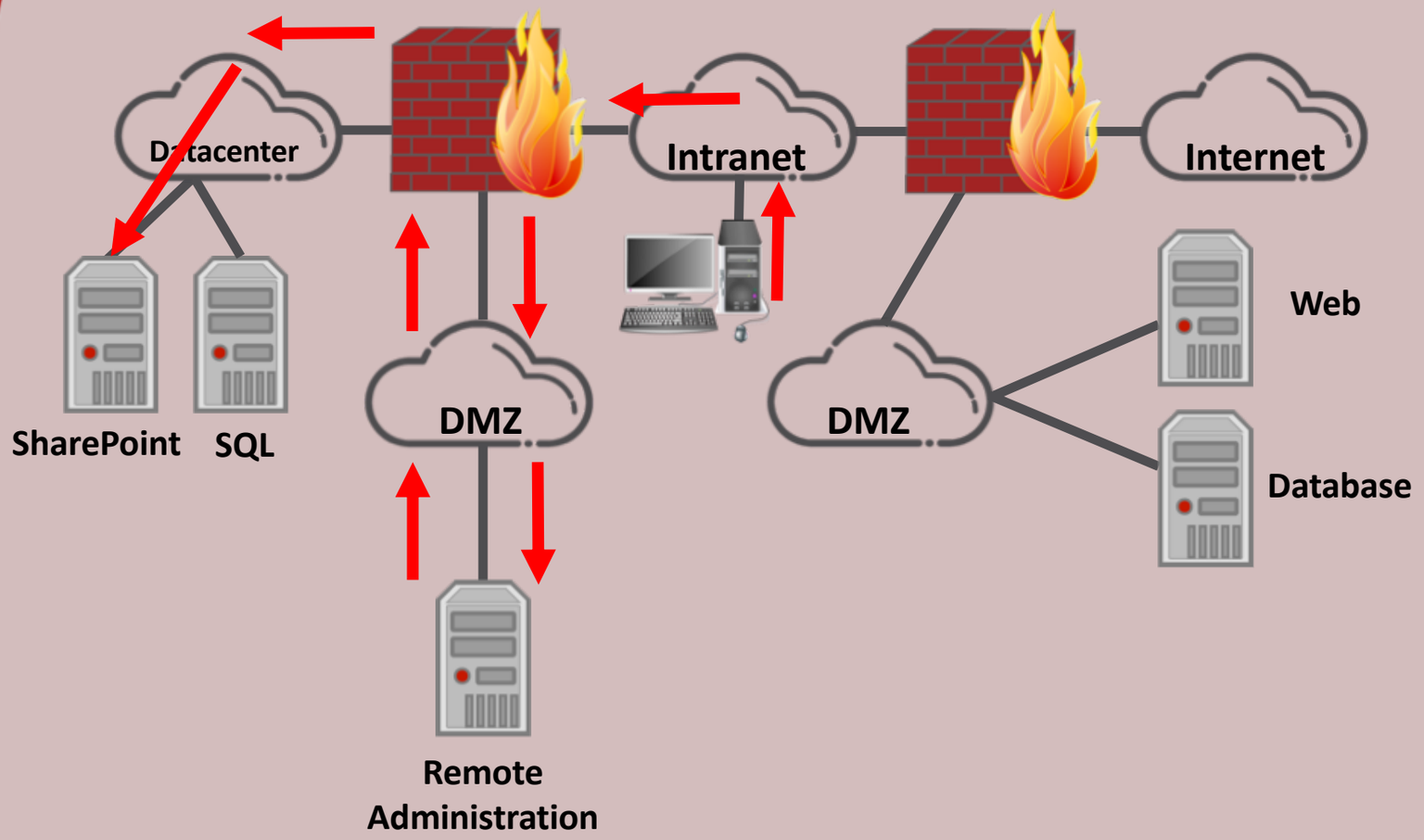
- Separates networks of different security levels from each other
- Much like we did intranet, internet, and DMZ
- We apply this same principles to break apart our large networks into more secure enclaves

Network Segmentation



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Segmentation



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Access Control

THREAT MANAGEMENT

Network Access Control (NAC)

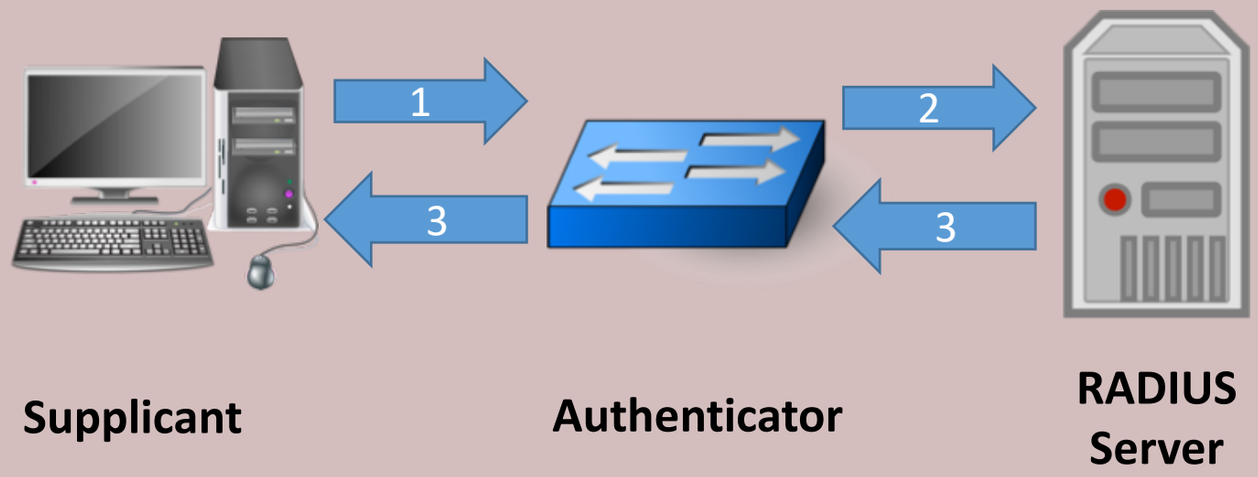
- Limits network access to only authorized individuals and systems

- Ensures the systems connecting to the network meet basic security requirements

802.1x

- 802.1x protocol is most common standard utilized for NAC

- Works for wired and wireless networks



Agent-based and Agentless

- Agent-based
  - Requires the device requesting access to have special software to communicate with NAC service (such as 802.1x)
- Agentless
  - NAC authentication is conducted in a web browser and doesn't need special software (such as Wireless at a hotel)

In-Band and Out-of-Band

- In-Band
  - Uses dedicated appliances placed between the devices and the services they are requesting
    - Example: Hotel networks that require you to enter your name and room number before gaining access

- Out-of-Band
  - Relies on existing network and has device communicate to authentication servers (like 802.1x)

NAC Approval Criteria

- Time of Day
- Role of the user
  - Admins can access datacenter only when inside datacenter
- Location of the user
  - User must be in datacenter to access
- System health status
  - Anti-virus up to date, security patches installed, host firewall enabled, etc.

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Defense Deception Methods

THREAT MANAGEMENT

Defense Deception Methods

- Cybersecurity professionals may want to go beyond just standard defense and attempt to lure an attacker to specific targets

- Examples:
  - Honeypots
  - DNS Sinkholes

Honeypot

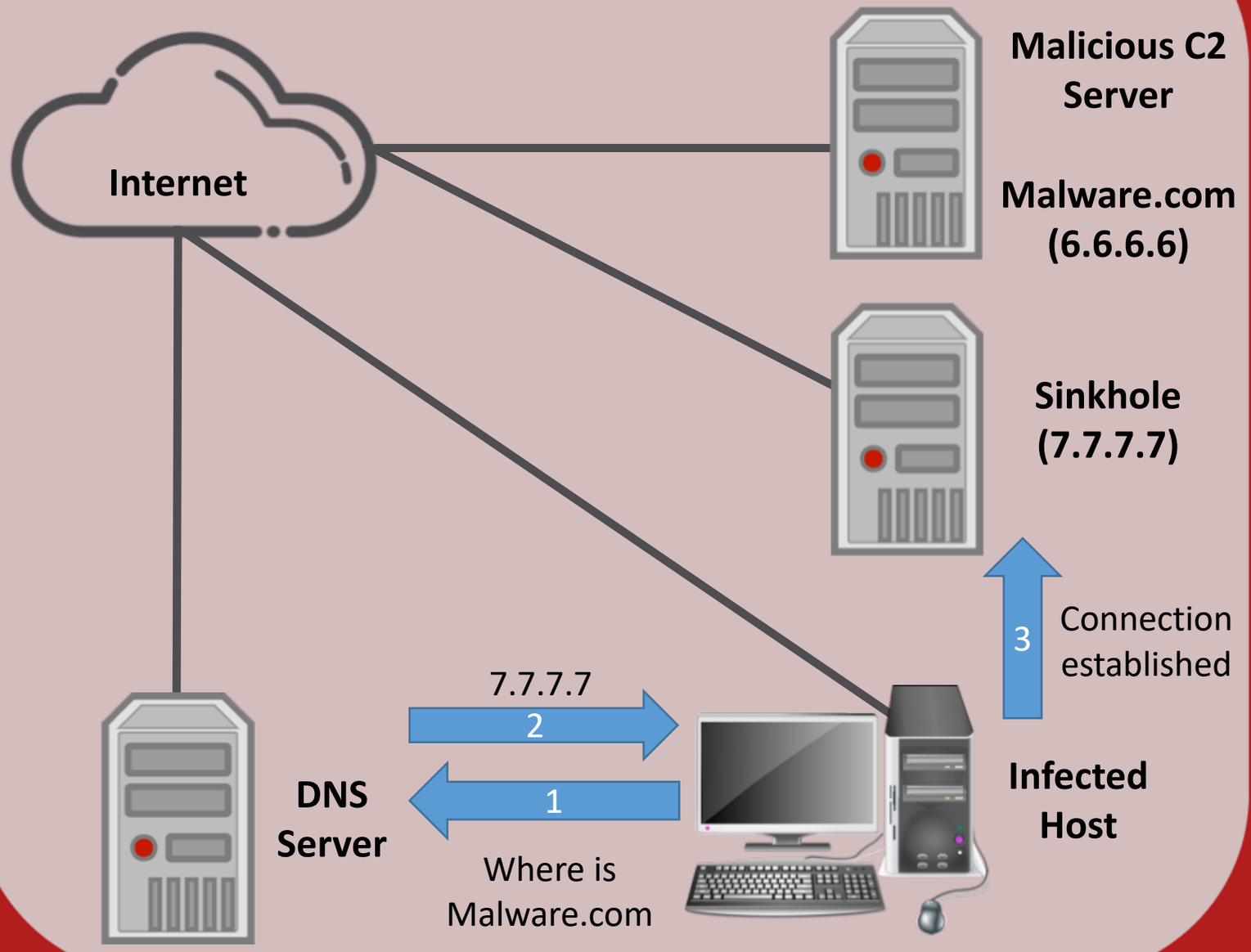
- System designed to look like a lucrative target due to the types of services being run or vulnerabilities contained
- In reality, honeypots are designed to falsely appear vulnerable and to fool malicious attackers to waste time going after them
- They simulate successful attacks and allow us to monitor attacker techniques

DNS Sinkhole

- Provide false DNS information to malicious software

- Compromised system requests DNS information from the server, but the server detects the suspicious request and gives the IP address of the sinkhole instead of the real Command and Control server

DNS Sinkhole



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Secure Endpoint Management

THREAT MANAGEMENT

Secure Endpoint Management

- Hardening System Configurations
- Patch Management
- Compensating Controls
- Group Policies
- Endpoint Security Software

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Hardening System Configurations

- Hardening a system makes it as resistant to attack as possible

- Examples:
  - Disabling unnecessary services
  - Disabling unnecessary ports
  - Verifying secure configurations
  - Centrally controlling device security settings

Patch Management

- Once a patch is released by the vendor, attackers begin to reverse engineer it
- Organizations must ensure proper patch management to prevent attacks
- Examples:
  - Microsoft System Center Configuration Manager (SCCM)

Compensating Controls

- If you can't implement a security control, you can compensate for it
- Provides a similar level of security by using an alternate means
- Examples:
  - WannaCry outbreak required disabling SMBv1, but this could break an file share
  - Point-of-Sale or embedded systems can't be updated without possibility of breaking

Group Policy Objects (GPO)

- Provides admins an efficient way to manage system and security configuration settings across many devices in a network

- Examples:
  - Require the use a firewall on all hosts
  - Mapping to a share drive on login
  - Run scripts at login to verify compliance

Endpoint Security Software

- Specialized software to enforce the company's security objectives/policies
- This software should report to a centralized management system for cyber security analysts to view and analyze
- Examples:
  - Antivirus or anti-malware
  - Host-based IDS or IPS

Going the Extra Mile…

- Mandatory Access Control (MAC) sets all security permissions centrally and the users cannot change permissions locally
- Discretionary Access Control (DAC) allows the owners of a file or resource to control the permissions on that resource
- MAC has great security, but is an administration nightmare…only used in very sensitive environments (SE Linux)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Penetration Testing

THREAT MANAGEMENT

Penetration Testing (PenTest)

- Penetration testers simulate a cyber attack against your organization's resources using the same information, tools, and techniques available to an attacker

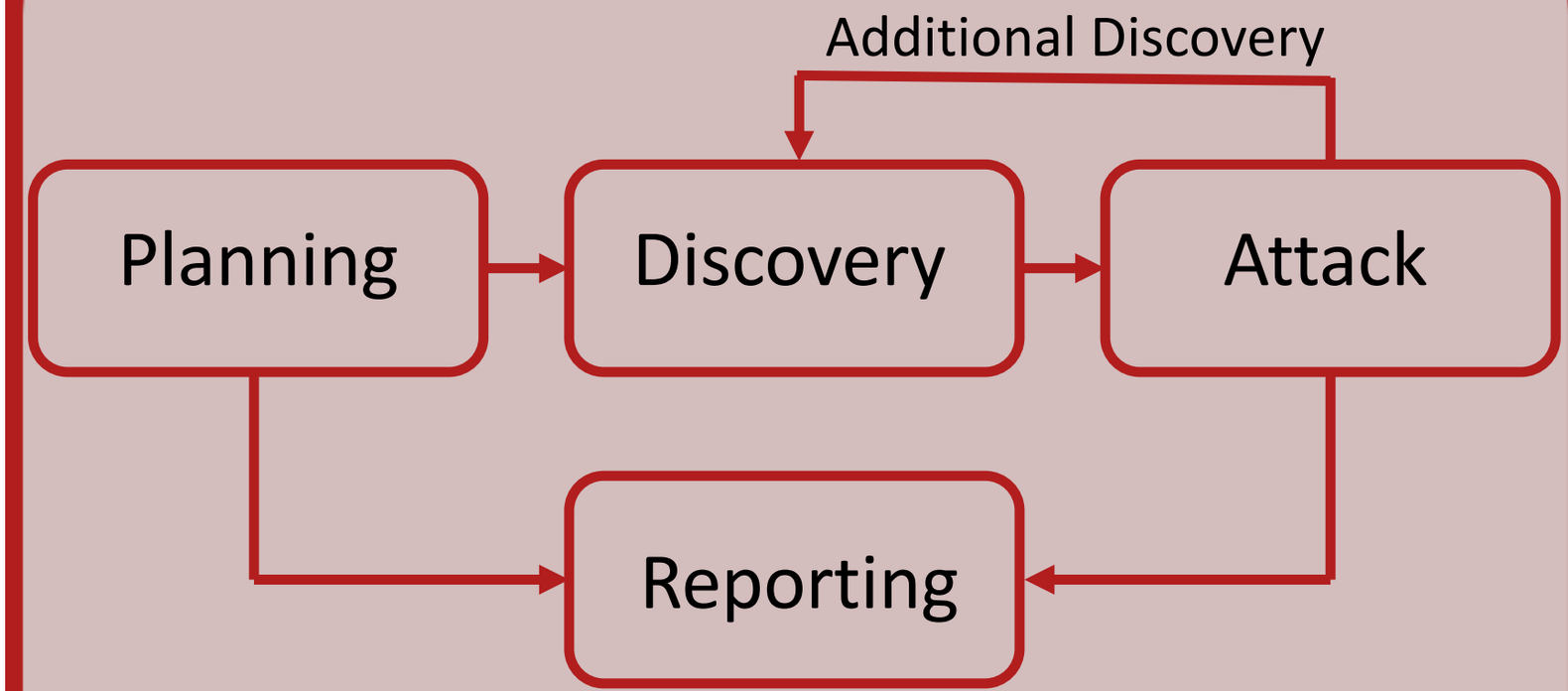
- Goal:
  - To gain access to your systems and report the findings to management

Who can do the PenTest?

- Can be performed by internal staff or external consultants
- Requires highly skilled individuals
- Tests are very time consuming and costly

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Phases of a PenTest



NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) divides PenTests into four phases

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Planning

- An important phase of a PenTest
- No technical work is performed
- Timing, Scope, and Authorization is gained during the Planning Phase
- You should NEVER conduct a PenTest without authorization…it's illegal!

Discovery

- Testers conduct reconnaissance and gather as much information on the network, system, users, and applications

- Examples:
  - Open source research
  - Port scanning
  - Enumeration
  - Vulnerability scanning
  - Web application scanning

Execute the Attack

- Seeks to bypass the security controls and gain access to the system

- Attack Phase (aka Exploitation)
  - Gaining Access
  - Escalating Privileges
  - System Browsing
    - May refer back to discovery phase again
  - Installing Additional Tools

Source: NIST SP 800-115

Reporting

- Testers should prepare a detailed report after the test
- Contains results of the PenTest, describing their successful attacks and suggestions on how to fix them
- Should be prioritized based on the risk posed by each vulnerability exploited

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Security Exercises and Training

THREAT MANAGEMENT

Beyond a PenTest

- Security exercises can put penetration testers and defenders against each other to provide additional training
- Performed in a simulated environment…not production network
- Conducted by three types of teams: Red, Blue, and White

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Red Team

- Participates as the attacker
- Uses reconnaissance and exploitation tools to gain access to the network
- Similar to penetration testers

Blue Team

- Participates as the defender
- Secures the network and attempts to keep red team out through the use of security controls
- Usually made up of system and network administrators

White Team

- Participates as the referee
- Coordinates the exercise and arbitrates disputes
- Maintains the simulated environment and monitors the exercise

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Reverse Engineering

THREAT MANAGEMENT

Reverse Engineering

- Malware authors do not explain how their software works
- Reverse engineering is a technique to take a finished product and understand its inner workings through decomposition
- Conducted through dynamic or static analysis

Dynamic Analysis

- Malware is placed in a sandbox and its behavior observed on the system and the virtual network

- Automated solutions can do this in near real-time, where email attachments are launched and automatically analyzed for malicious activity

Static Analysis: Software

- Analysis of the code of the malware
  - For Ruby and Python, the code is readable because they are interpreted languages
  - For C/C++ and Java, code is compiled into binary
- Static analysis of compiled code requires a decompiler or analysis in binary format

Reverse Engineering Hardware

- Very difficult to perform due to embedded software in firmware
- Most often, dynamic analysis is conducted on hardware
- *Hardware should be purchased from a trusted supplier to minimize the risk of malware being inserted into the firmware of hardware devices during procurement and shipment to your company*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Reconnaissance and Intelligence

THREAT MANAGEMENT

Reconnaissance and Intelligence

- Gathering of information to better understand the security landscape
- Some security standards and laws, such as the PCI-DSS standard, require information gathering from inside and outside your network to ensure compliance through vulnerability scans performed quarterly
- Numerous tools and techniques for conducting this discovery

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Footprinting the Network

THREAT MANAGEMENT

Footprinting the Network

- Creates a map of the network, systems, and other infrastructure of the company
- Created using a mixture of information gathering tools and manual research
- Guidance can be found in the NIST SP 800-115 and the Open Source Security Testing Methodology Manual (OSSTMM)

Active Reconnaissance

- Utilizes host scanning tools to gather information about systems, services, and vulnerabilities in the network
- Does not include exploitation of the vulnerabilities, only identification of them
- Permission should be sought out before conducting active reconnaissance because it could be construed as an attack by mistake

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Mapping

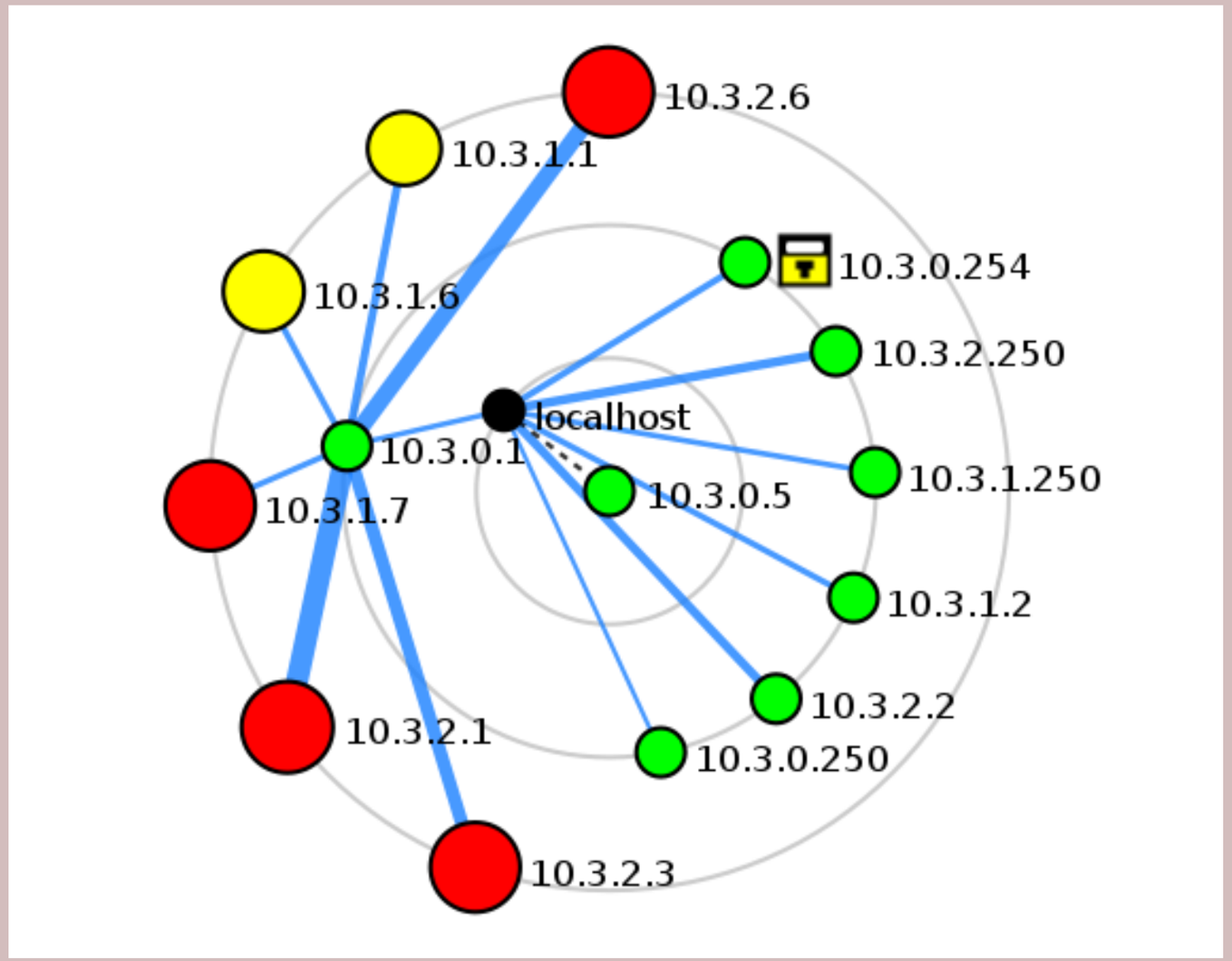
THREAT MANAGEMENT

Network Mapping

- Network mapping tools used during active reconnaissance can approximate the network by using
  - Time to live (TTL)
  - Traceroute information
  - Other responses from the network devices

- Zenmap and nmap are useful for conducting network mapping

Network Mapping (Zenmap)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Mapping Challenges

- Firewalls and Layer 3 Switch ACLs can make it difficult to map a network fully
- Wireless networks are also a challenge
- Virtualized networks and infrastructure
- Cloud services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

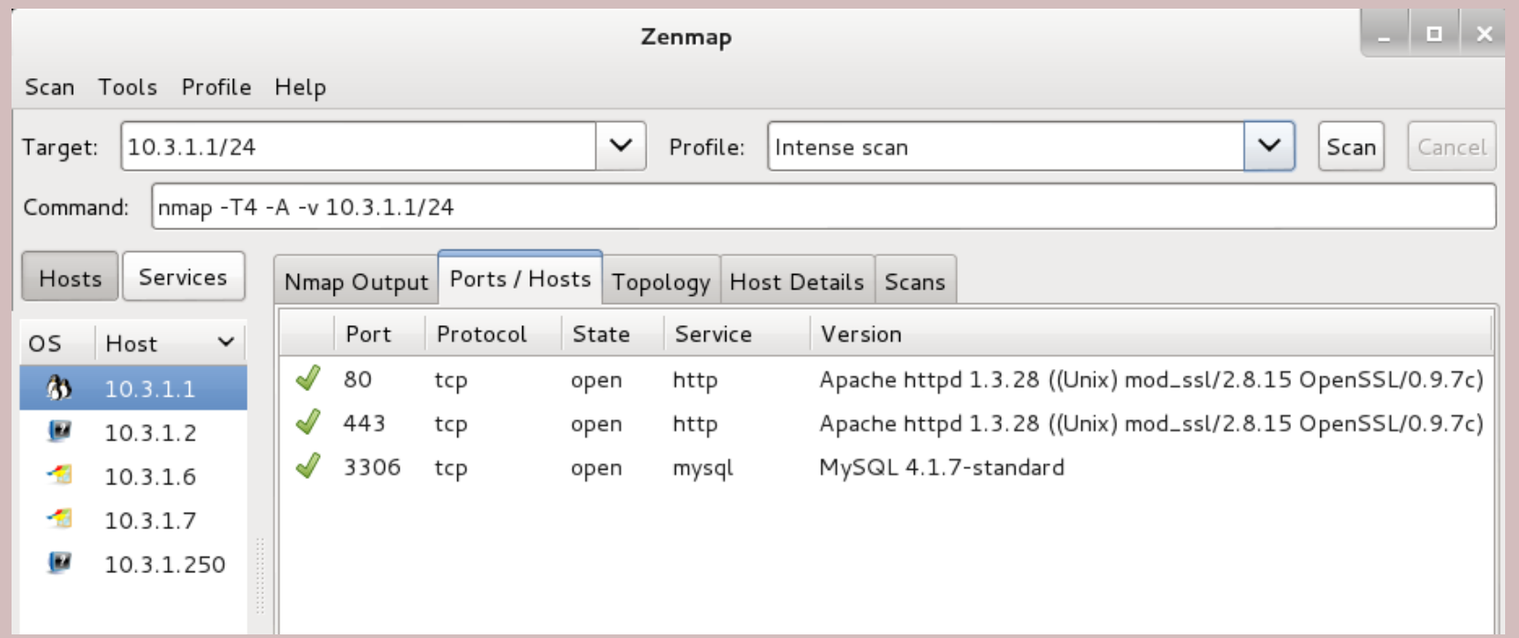
Port Scanning

THREAT MANAGEMENT

Port Scanning

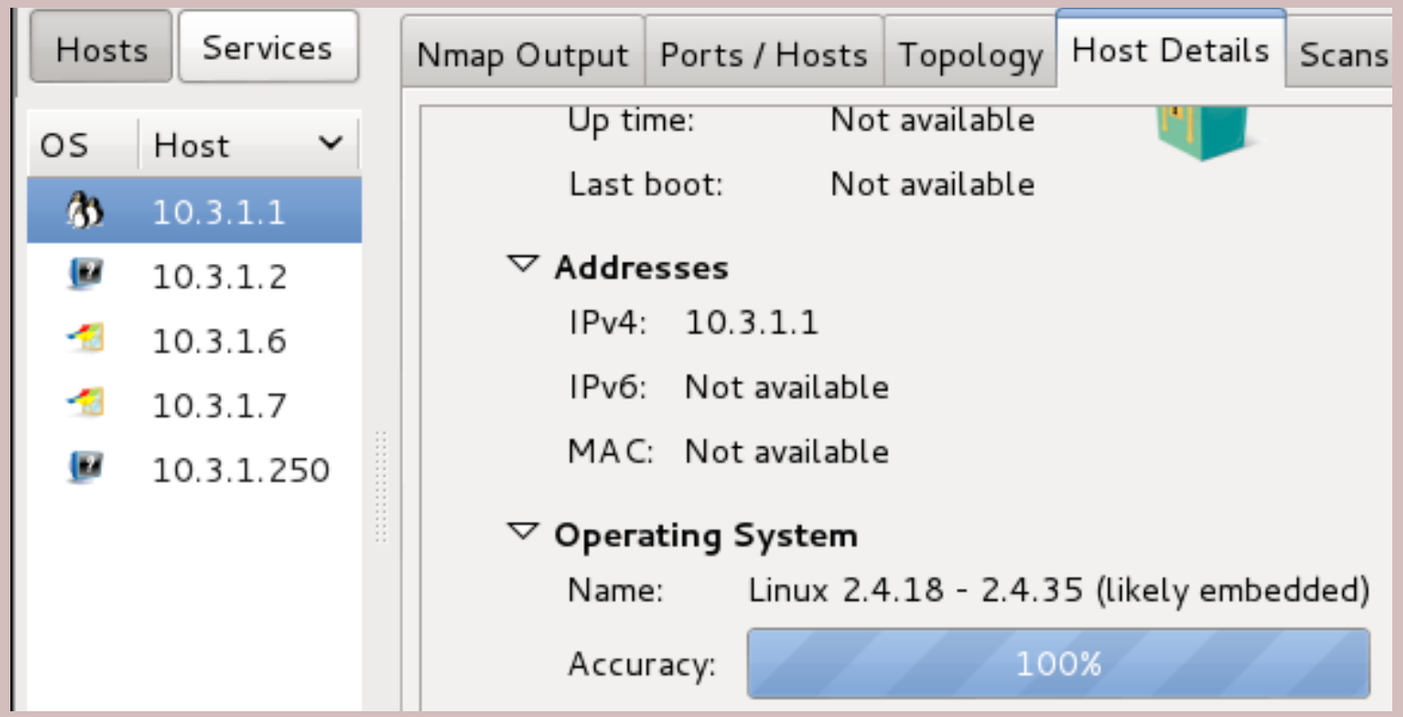
- Most common method to gather information on a network and devices
- Port scanners perform:
  - Host discovery
  - Port scanning and service identification
  - Service Version identification
  - Operating System Identification
- Port scanners also used for network inventory tasks and security audits

Service Scanning (Zenmap)



Service identification attempts to identify the service and its version through banner grabbing or comparing TCP/UDP packet responses to known signatures

OS Scanning (Zenmap)



OS fingerprinting uses TCP/IP stack responses from the TCP and UDP packets sent to identify Windows, Linux, or OSX, and if possible, the version

Importance of Port Numbers

- Well-known ports (0-1023)
- Registered ports (1024-49151)

Where you scan from matters…

- Internal scans will see more information than an external scan

- If you are trying to simulate a cyber attack during a PenTest, you should be scanning from the outside the network to match the attacker's perspective

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Other Port Scanners

THREAT MANAGEMENT

Angry IP Scanner

- Multiplatform (Windows, Linux, MacOS)
- Graphical port scanner
- Doesn’t provide service or OS information by default
  - Must use “fetchers” to get more details
- Well-known, but not as full featured as nmap or Zenmap

Other Port Scanners

- Many other port scanners exist
- Metasploit built-in scanners
- Qualys Vulnerability Management
- Tenable's Nessus Vulnerability Scanner
- You can even write your own in a language like Python!

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Passive Reconnaissance

THREAT MANAGEMENT

Passive Reconnaissance

- More difficult than active reconnaissance
- Relies on logs and other data
- Data you receive may be out of date
- Often used during a cyber incident response

Log and Configuration Analysis

- Local system configuration data and log files can be used to build a network map
- Some tools exist to parse configuration files into a usable topology
- Much of this is done manually, though

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Passive Recon: Network Devices

THREAT MANAGEMENT

Network Devices

- Network devices log many activities, their status, and events
- Includes traffic patterns and utilization
- Logs files, configuration files, and network flows are great for passive recon

Logs Files

- Network devices send their logs to the display console (only logged in user sees them) by default

- You should configure them to send logs to centralized logging server (SYSLOG) or use SNMP to send the information

Levels of Events in Your Logs

Level	Name	Example
0	Emergencies	Failure causing a shutdown
1	Alerts	Temperature exceeded
2	Critical	Software failure
3	Errors	Interface down
4	Warning	Configuration change
5	Notifications	Line protocol up/down
6	Information	ACL violation
7	Debugging	Debugging Messages

An Example from Cisco Devices

Logs File Example

Access list (full timestamp and message id):

Jul 10 16:07:14 cisco2621 636: .Jul 10 15:58:56.590 EDT: %SEC-6-IPACCESSLOGP: list 102 denied tcp 10.0.6.56(3067) -> 172.36.4.7(139), 1 packet

123: May 3 05:15:25.217 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.40.16(3059) -> 10.0.4.101(1060), 2 packets 124: May 3 05:15:27.302 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.16.16(2179) -> 10.0.4.101(1060), 1 packet 125: May 3 05:15:40.362 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.32.16(4206) -> 10.0.4.101(1060), 2 packets 126: May 3 05:15:42.790 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.131.5.17(3737) -> 10.0.4.101(445), 1 packet

127: May 3 05:23:33.404 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1477) -> 10.0.127.20(445), 1 packet 128: May 3 05:23:34.416 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1469) -> 10.0.127.12(445), 1 packet 129: May 3 05:23:35.524 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1473) -> 10.0.127.16(445), 1 packet 130: May 3 05:23:36.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1478) -> 10.0.127.21(445), 1 packet 131: May 3 05:23:37.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1496) -> 10.0.127.39(445), 1 packet 132: May 3 05:23:38.540 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1484) -> 10.0.127.27(445), 1 packet

4872: Dec 11 08:02:53.887 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 200.174.153.126(1028) -> 66.81.85.65(137), 1 packet 4873: Dec 11 08:03:09.583 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 195.23.72.148(1026) -> 66.81.85.65(137), 1 packet

Configuration Files

- Invaluable when mapping a network
- Identifies all routes and devices in detail
- Provides details of SNMP and SYSLOG servers on the network, user & admin accounts, and more

Configuration File Example

```
!
version 12.0
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
service sequence-numbers
!
hostname cisco
!
boot system flash c2600-io3-mz.120-7.T
logging buffered 8192 debugging
no logging console
enable secret 5 $1$dDL8$GDwKRMyUQ5iWZxbq6EAKY.
enable password 7 0519030222455D0A16
!
!
!
!
!
clock timezone MET 1
clock summer-time DST recurring
ip subnet-zero
no ip source-route
no ip domain-lookup
ip domain-name ibm.nl
ip name-server 123.456.321.3
!
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Configuration File Example

```
!
logging 123.456.321.3
access-list 102 deny   ip 123.456.321.0 0.0.0.248 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 permit tcp any host 123.456.321.42 eq ftp
access-list 102 permit tcp any host 123.456.321.42 eq www
access-list 102 permit tcp any host 123.456.321.42 eq 443
access-list 102 permit tcp any host 123.456.321.43 eq ftp
access-list 102 permit tcp any host 123.456.321.43 eq www
access-list 102 permit tcp any host 123.456.321.43 eq 443
access-list 102 permit udp host 123.456.321.3 eq domain any
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any unreachable
access-list 102 permit icmp any any source-quench
access-list 102 deny   udp any any eq netbios-ns
access-list 102 deny   udp any any eq netbios-dgm
access-list 102 deny   ip any any log
access-list 103 permit tcp any host 123.456.321.4 eq smtp
access-list 103 permit udp any host 123.456.321.3 eq domain
access-list 103 permit icmp any any echo-reply
access-list 103 permit icmp any any echo
access-list 103 permit icmp any any packet-too-big
access-list 103 permit icmp any any unreachable
access-list 103 permit icmp any any source-quench
access-list 103 deny   ip any any log
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
```


Netflow Data

- Cisco network protocol
- Captures IP traffic information for traffic monitoring to provide flow and volume
- Contains IP, source port, destination port, and class of service
- Other vendors have “flows”, like Juniper’s Jflow and cflowd, Citrix’s AppFlow, and HP’s NetStream

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Passive Recon: Netstat

THREAT MANAGEMENT

Netstat

- Built-in utility in Windows, Linux, MacOS, and Unix operating systems
- Provides active TCP and UDP connections
- Identify process using a connection
- Provides statistics on sent/received data
- Route table information

netstat -a

- Provides active TCP and UDP connections filtered by TCP, UDP, ICMP, IP, IPv6, and more

```
Last login: Wed Sep 20 20:05:22 on ttys000
[Jasons-MacBook-Pro:~ hacking$ netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  10.40.8.249.54305      hyp01-packet-res.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54304      17.173.65.216.https    ESTABLISHED
tcp4       0      0  10.40.8.249.54302      usdal4-vip-bx-00.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54300      ec2-34-226-108-2.https ESTABLISHED
tcp4       0      0  10.40.8.249.54299      nyc28.ff.avast.c.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54298      mia27.ff.avast.c.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54296      a184-24-97-43.de.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54295      a104-93-80-197.d.https ESTABLISHED
tcp4       0      0  10.40.8.249.54294      adobe.com.ssl.d1.https ESTABLISHED
tcp4       0      0  10.40.8.249.54293      a104-93-68-42.de.https ESTABLISHED
tcp4       0      0  10.40.8.249.54292      ec2-52-35-208-52.https ESTABLISHED
tcp4       0      0  10.40.8.249.54291      17.248.141.48.https    ESTABLISHED
tcp4       0      0  10.40.8.249.54290      ec2-52-35-208-52.https ESTABLISHED
tcp4       0      0  10.40.8.249.54289      adobe.com.ssl.d1.https ESTABLISHED
```


netstat -o

- Identify process using a connection

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49688        DESKTOP-1TI5NVD:49689  ESTABLISHED     1936
  TCP    127.0.0.1:49689        DESKTOP-1TI5NVD:49688  ESTABLISHED     1936
  TCP    192.168.66.129:55899   msnbot-65-52-108-222:https  ESTABLISHED     3684
  TCP    192.168.66.129:55902   msnbot-65-52-108-222:https  ESTABLISHED     1336
  TCP    192.168.66.129:55991   23.102.4.253:https     TIME_WAIT       0
  TCP    192.168.66.129:56000   134.170.58.123:https   ESTABLISHED     1336
```


netstat -e

- Ethernet statistics on sent/received data

```
Interface Statistics

                           Received            Sent

Bytes                    3019189716      2539479229
Unicast packets            22644273        11242559
Non-unicast packets               0               0
Discards                          0               0
Errors                            0               3
Unknown protocols                 0
```


netstat -r

- Displays route table information

```
Jasons-MacBook-Pro:~ hacking$ netstat -r
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            10.40.8.1          UGSc          260       50     en0
10.40.8/21         link#6             UCS             0        0     en0
10.40.8.1/32       link#6             UCS             1        0     en0
10.40.8.1          1c:5e:c:64:e6:89   UHLWIir       274     2098     en0    749
10.40.8.249/32     link#6             UCS             0        0     en0
127                localhost          UCS             0        0     lo0
localhost          localhost          UH             25   902604     lo0
169.254            link#6             UCS             0        0     en0
172.16.145/24      link#16            UC              1        0  vmnet2
192.168.63         link#15            UC              1        0  vmnet1
192.168.66         link#17            UC              2        0  vmnet8
192.168.66.129     0:c:29:74:67:55     UHLWI           0        0  vmnet8    670
```


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DHCP Logs and Configs

THREAT MANAGEMENT

What is DHCP?

- Dynamic Host Configuration Protocol
- Provides an IP address, default gateway, subnet mask, and DNS server to a host
- DHCP server logs and configurations are useful during passive reconnaissance
- Combined with firewall logs, you can determine which hosts use dynamic or static IPs

Example DHCP Configuration

```
#
# DHCP Server Configuration File
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcp.conf(5) man page
#

default-lease-time 600;
max-lease-time 3600;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 8.8.8.8, 4.4.2.2;
subnet 192.168.0.0 netmask 255.255.255.0 {
       Range 192.168.1.50 192.168.1.250;
}

Host courses {
        option host-name “courses.jasondion.com”;
        hardware ethernet 34:15:d2:a5:c6:d1;
        fixed address 192.168.0.10;
}
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Example DHCP Logs

```
Sep 12 04:23:45 fileserver dhcpd[2435]:
reuse_lease: lease age 60 (secs) under 25% threshold,
reply with unaltered, existing lease

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPREQUEST for 192.168.0.56 (192.168.0.67)
from 24:67:d2:e4:a1:17 via enp0s3

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPACK on 192.168.0.56 to 24:67:d2:e4:a1:17 via enp0s3

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPACK on 192.168.0.56 to 24:67:d2:e4:a1:17 via enp0s3
```


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Firewall Logs and Configs

THREAT MANAGEMENT

Firewall Logs and Configs

- Both firewall and router logs and configurations indicate accepted and blocked connections
- It is a good way to passively understand your network design
- Reading configurations is quicker than “reverse engineering” the log files

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Firewall Logs

- Often use log levels to categorize information and debug messages
- Cisco, Palo Alto, and Check Point all log things a little different, but have common items
  - Date/Time Stamp
  - Details of the event
- Logs are designed to be human readable
- Access logs on Cisco using “show logging” command

Example Firewall Logs

Feb 2 12:15:04 192.168.0.1 %ASA-5-710003: User 'ASAadmin' executed the 'enable' command

https://www.cisco.com/c/en/us/about/security-center/identify-incidents-via-syslog.html

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Example Firewall Config

```
ip access-list extended inb-lan
    permit tcp 192.168.0.0 0.255.255.255 any eq 22
    permit tcp 172.16.0.0 0.15.255.255 any eq 22
    permit tcp 10.10.0.0 0.255.255.255 any eq 22
    deny tcp 192.168.1.0 0.255.255.255 any eq 22
```

It can help to read these to yourself like this:

“Allow tcp traffic from 192.168.0.0 to any destination IP on port 22”

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

System and Host Log Files

THREAT MANAGEMENT

Host/Server Log Files

- System logs are collected by the system
- Useful for troubleshooting and reconstructed a cyber attack
- Log files provide information on system configuration, applications, and user accounts
- You have to have system access to get these logs, though

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Windows System Log Types

- Application logs
  - Logged by programs/applications
- Security logs
  - Records login events, resource usage, files created/open/deleted, etc.
- Setup logs
  - Records application setup actions
- System logs
  - Events from Windows components
- ForwardedEvents logs
  - -Event subscriptions from remote computers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Linux System Logs

- /var/log directory
- Other applications may store their own log files elsewhere

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DNS Harvesting

THREAT MANAGEMENT

Why Use DNS?

- Often our first step in information gathering
- DNS information is publically available
- A quick Whois search can give you many details to use
- Hostnames can tell you about the server (DC1.jasondion.com might be a domain controller…)

nslookup

```
Command Prompt
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Benny>nslookup
Default Server:  cns3.tm.net.my
Address:  202.188.0.133

> www.cisco.com
Server:  cns3.tm.net
Address:  202.188.0.133

Non-authoritative answer:
Name:    www.cisco.com
Address:  198.133.219.25

> www.dlink.com
Server:  cns3.tm.net
Address:  202.188.0.133

Non-authoritative answer:
Name:    www.dlink.com
Address:  64.7.210.132

> exit

C:\Documents and Settings\Benny>
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DNS Records

- MX (mail server records)
- A (address records)
- C (canonical records)
- PTR (pointer records)

tracert

```
Command Prompt

C:\>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list.
    -w timeout         Wait timeout milliseconds for each reply.

C:\>tracert 209.85.135.99

Tracing route to mu-in-f99.google.com [209.85.135.99]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    15 ms    14 ms    14 ms  172.29.64.217
  4    19 ms    19 ms    19 ms  gdr01-gdr11.ip.t-con.hr [195.29.240.74]
  5    32 ms    30 ms    31 ms  193.159.225.61
  6    38 ms    38 ms    37 ms  217.5.66.42
  7    41 ms    40 ms    41 ms  74.125.50.149
  8    42 ms    42 ms    43 ms  66.249.94.86
  9    42 ms    45 ms    41 ms  209.85.130.15
 10    43 ms    49 ms    54 ms  72.14.239.58
 11    42 ms    42 ms    43 ms  mu-in-f99.google.com [209.85.135.99]

Trace complete.

C:\>tracert www.google.com

Tracing route to www.l.google.com [209.85.135.99]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    15 ms    14 ms    14 ms  172.29.64.217
  4    20 ms    18 ms    18 ms  gdr01-gdr11.ip.t-con.hr [195.29.240.74]
  5    32 ms    31 ms    31 ms  193.159.225.61
  6    37 ms    76 ms   109 ms  217.5.66.42
  7    42 ms    41 ms    40 ms  72.14.198.117
  8    43 ms    46 ms    43 ms  66.249.94.86
  9    67 ms    41 ms    40 ms  209.85.130.21
 10    48 ms    53 ms    51 ms  209.85.253.22
 11    42 ms    43 ms    46 ms  mu-in-f99.google.com [209.85.135.99]

Trace complete.

C:\>
```

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Domain Names and IP Ranges

THREAT MANAGEMENT

Domain Names

- The human readable names we use to locate servers, like jasondion.com
- Managed by registrars
- Generic top-level domains
  - .com, .net, .org, .edu, .mil, .gov
- Country code top-level domain (ccTLD)
  - .com.uk, .edu.it

IP Ranges

- Five regional authorities
  - AFRINIC (Africa)
  - ARIN (USA, Canada, Antarctica, and Caribbean)
  - APNIC (Asia, Australia, New Zealand, etc)
  - LACNIC (Latin America, Caribbean)
  - RIPE (Europe, Russia, Middle East)
- Each authority provides Whois services for their IP space

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DNS Zone Transfers

THREAT MANAGEMENT

DNS Zone Transfers

- Design to replicate DNS databases between two DNS servers
- This is a vulnerability if zone transfers are allowed, so most prevent zone transfers to servers that aren't trusted
- You can use dig to perform the transfer:

  # dig axfr @dns-server domain.name

Try Performing a Zone Transfer

- DigiNinja provides a couple DNS servers that ALLOW zone transfers for you to practice this technique

- Open up your Linux terminal and try it against nsztm1.digi.ninja and nsztm2.digi.ninja

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DNS Brute Forcing

- Used when you can't perform a DNS zone transfer
- Simply sends manual or scripted DNS queries for each IP of the organization
- Organizations can protect against this by sending responses slowly or with IDS/IPS rules to prevent this

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Whois and Host Commands

THREAT MANAGEMENT

Whois

- Allows search of databases for domain and IP blocks
- Provides detailed registration information used when claiming the domain name
- Names, Addresses, IPs, Phone numbers, and more can be gained

Whois Example

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-09-07T08:50:36-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited
(https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited
(https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited
(https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: DNS Admin
Registrant Organization: Google Inc.
Registrant Street: 1600 Amphitheatre Parkway,
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6502530001
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
Registry Admin ID:
```

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Host

- Provides information about a systems IPv4 and IPv6 addresses and servers

```
Jasons-MacBook-Pro:~ [redacted]$ host google.com
google.com has address 74.125.136.101
google.com has address 74.125.136.113
google.com has address 74.125.136.139
google.com has address 74.125.136.138
google.com has address 74.125.136.102
google.com has address 74.125.136.100
google.com has IPv6 address 2607:f8b0:4002:c00::66
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
```


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Info Gathering and Aggregation

THREAT MANAGEMENT

Information Gathering

- Can be done using packet captures
- Requires an intruder to breach a company's network to gather this info
- Treasure trove of information
  - What hosts are on the network
  - What operating systems are the running
  - What shares are available
- This is done using tools like Wireshark
  - Beyond the scope of this lesson…

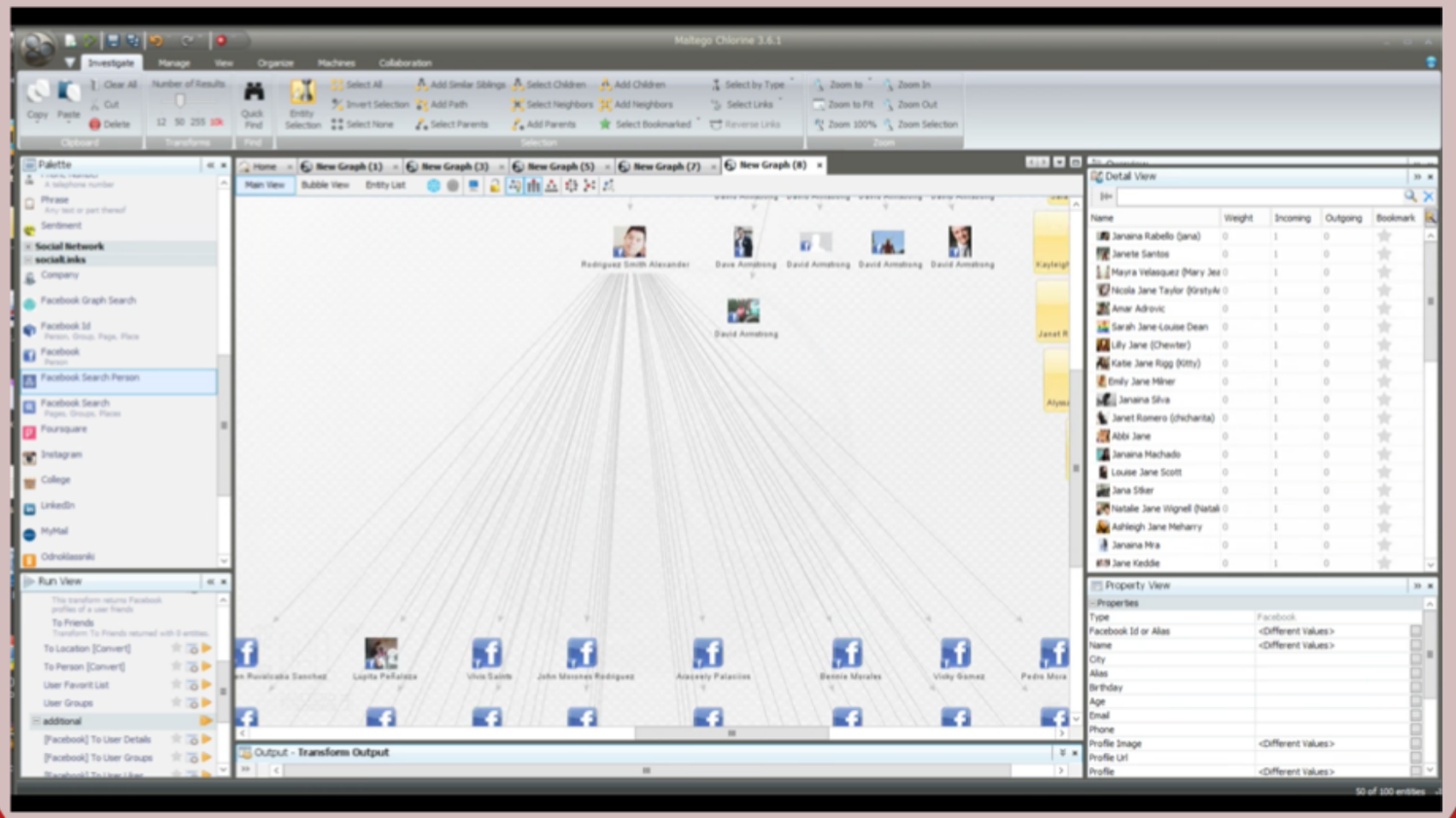
Information Aggregation

- Gathering information from various platforms for analysis with a single tool

- theHarvester
  - Gathers emails, domains, hostnames, employee names, open ports, banners, etc.
  - Text-based tool installed in Kali

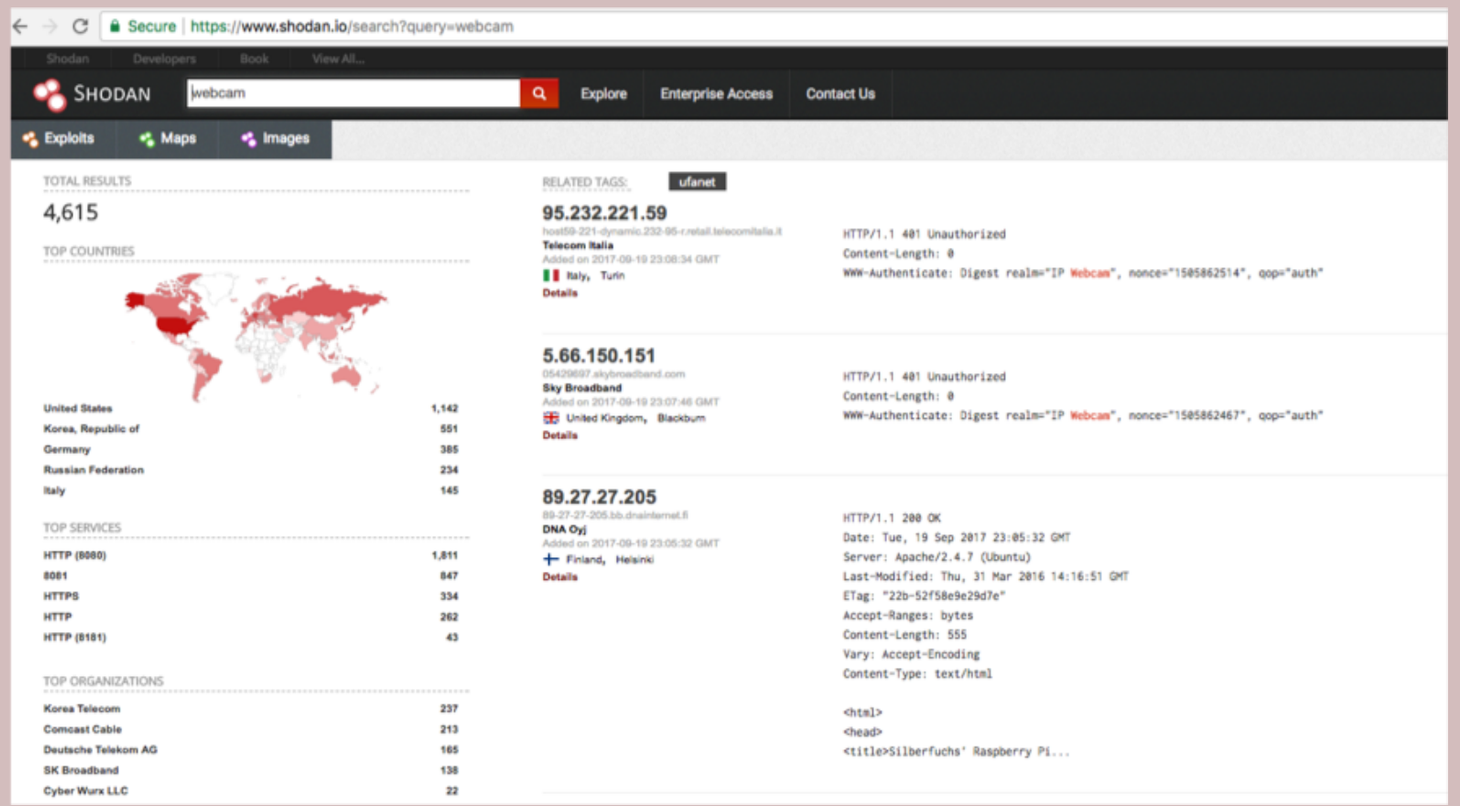
Maltego

- Builds relationship maps between people and resources



Shodan

- Search engine for internet-connected devices and their vulnerabilities



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Organizational Intelligence

THREAT MANAGEMENT

Organizational Intelligence

- Your organization has an online profile, whether you know it or not…
- This can be used by an attacker against you…
- In a penetration test, we act as the attacker, so we must use this information too!

Organizational Data

- Locations (of facilities and buildings)
  - Your physical security posture
  - Business hours
- Work routine of the organization
- Organizational charts
  - Relationships between departments and people
- Documents (contains metadata)
- Financial data
- Personal information of your employees

* Useful during social engineering *

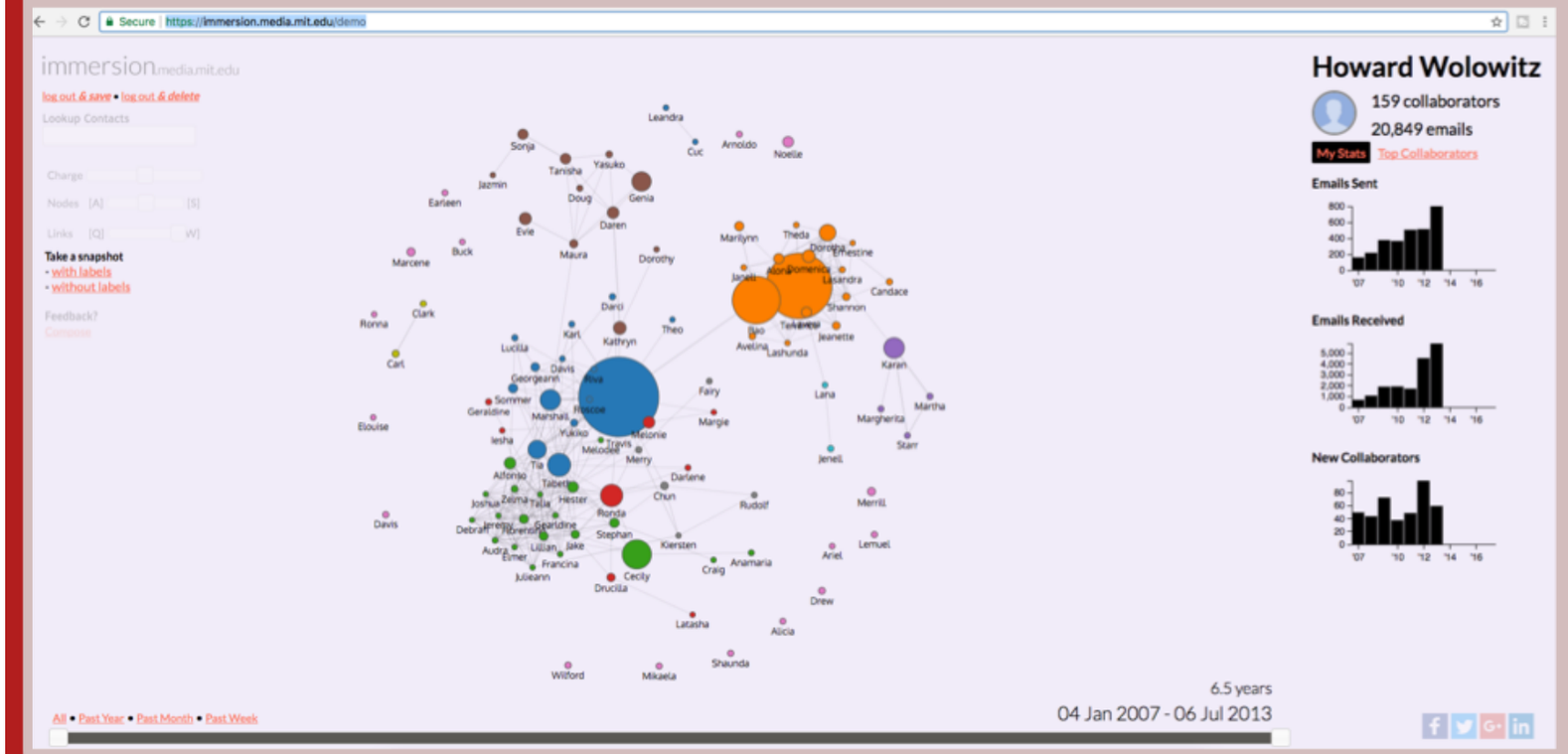
Document Harvesting

- Metadata
  - Contains author's name and software version used
- EXIF data
  - Photos could contain geolocation coordinates
- It is important to scrub metadata and EXIF data from documents posted on the web
- Emails
  - Can you be used to perform contact chaining and conduct social engineering campaigns

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Immersion

https://immersion.media.mit.edu/demo



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Where Can I Get Documents?

- Organizations are getting smarter and posted less sensitive information online

…on the Internet nothing is ever gone!

- The Internet Archive
  - archive.org
- Time Travel Service
  - timetravel.mementoweb.org
- Google Cache View
- Cachedview.com

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Where Can I Get More?

- Social media is great to find details about the organization's employees
- Many people post what companies they work for and don't set their privacy settings up properly
- Paid public record searches, like Zaba Search, NETR Online, etc.

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

The Threat: Social Engineering

- Exploits the human element of security
- Occurs via phone, email, social media, or even in person
- Social Engineering Toolkit (SET)
- Creepy (geolocation tool)
- Metasploit (phishing and other tools)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Detecting, Preventing, and Responding to Reconnaissance

THREAT MANAGEMENT

Detecting, Preventing, and Responding to Reconnaissance

- Successful reconnaissance doesn't always mean a successful attack, but we want to limit the damage that could occur as much as possible

- We utilize the same technique to limit both casual and directed reconnaissance

Detecting Recon: Overview

- Monitoring must occur at connection points between two network zones

- Perform data collection so you can analyze the data at a later time

Detecting Recon: Data Sources

- Network traffic analysis using IDS, IPS, HIDS, NIDS, firewalls, and other security devices
- Packet analysis
- Protocol analysis
- Traffic and flow analysis
- Device and system logs
- Port and vulnerability scans
- Security Information and Event Management Logs

- If you outsource your services, you might have to relay on your SaaS or PaaS provider to detect it for you…

Detecting Recon: Data Analysis

- Anomaly Analysis
  - What is different about this? What's not normal?
- Trend Analysis
  - Helps to identify future problems based on past
  - Example: Traffic congestion
- Signature Analysis
  - Fingerprint or hash used to detect threats
- Heuristic or Behavioral Analysis
  - Detects threats based on behavior
  - Useful to detect unknown threats
- Manual Analysis
  - Human expertise is used to analyze the data

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Preventing Passive Recon

- Control the information your release
- Blacklist system that are abusing your services
- Use CAPTCHAs to prevent scripts and bots
- Utilize third-party registration for domains/Ips
- Set rate limits for lookups and searches
- Avoid publishing zone files, if possible
- Educate your users about social media risks

Preventing Active Recon

- Employ network defenses
- Limit external exposure of services and know your forward facing footprint
- Utilize an IPS to limit or stop probes/scans
- Utilize monitoring and alert systems based on signature, behavior, or anomaly