Fence Barriers

- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- Fences are combined with entry/exit gates of varying strength
  - Barricade gates
  - Tire shredders

Types of Gates

I

Class I: Residential gate operation

II

Class II: Commercial, such as parking lot or garage

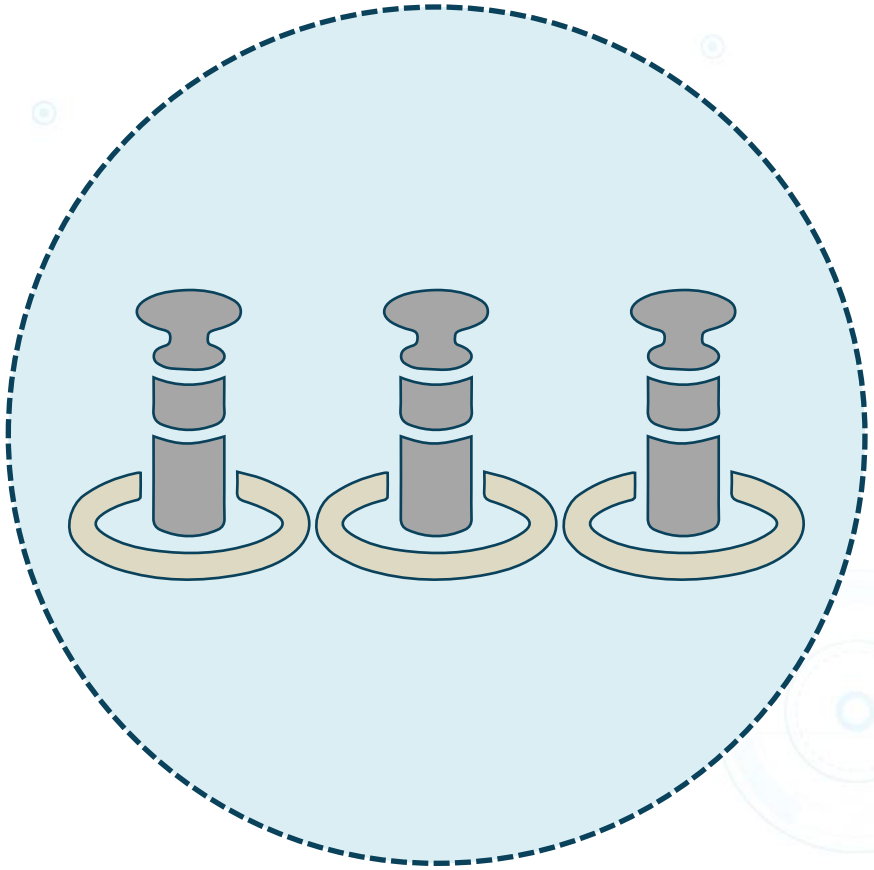
III

Class III: Industrial/limited access (warehouse, factory, docks)

IV

Class IV: Restricted access operation requiring supervisory control

Bollards



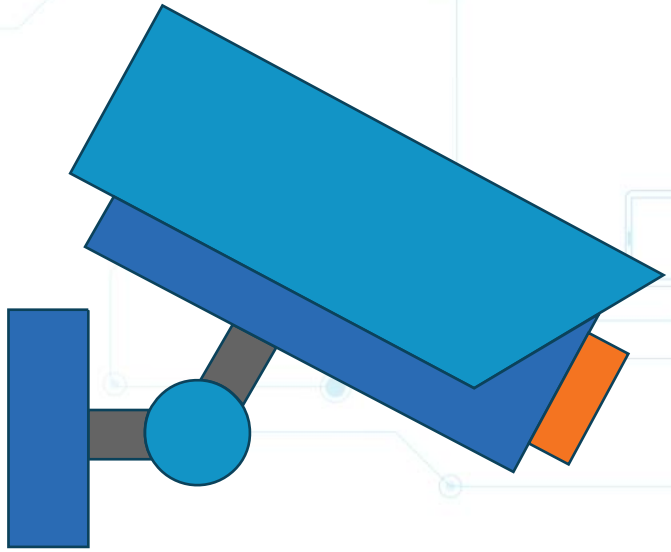
- Bollards are strategically placed pylons meant to prohibit vehicles from entering certain areas
- Typically concrete or strong metal
- High-tech bollards can be mechanical and include cameras and sensors

Signage

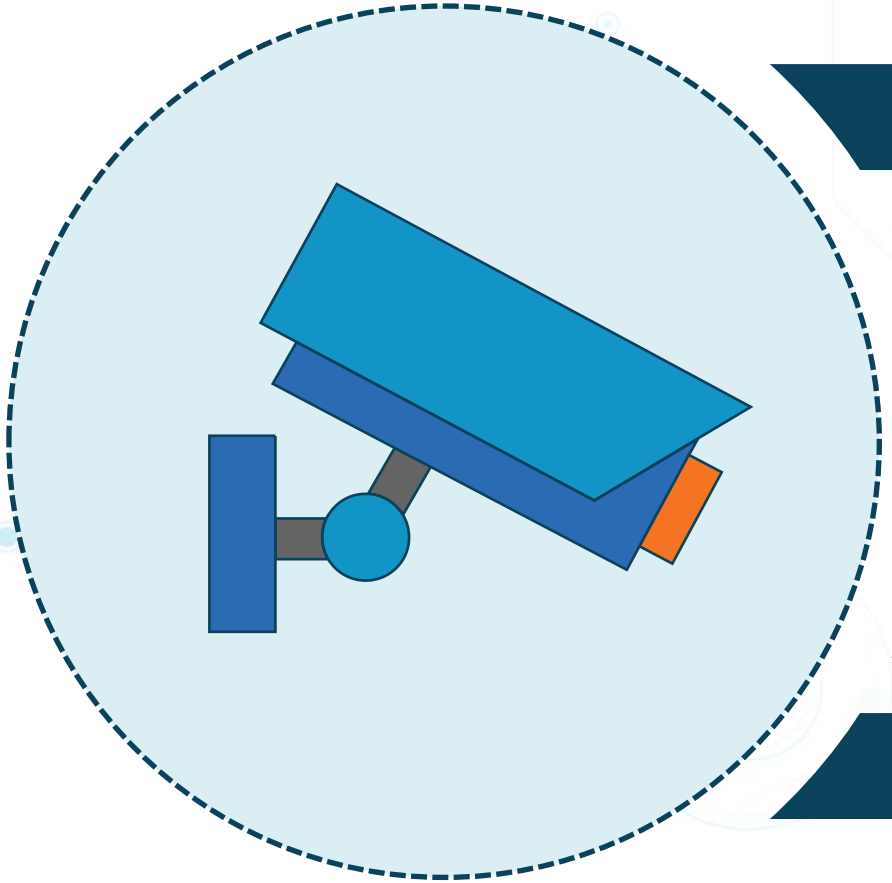
- Signs and window stickers are a deterrent control designed to deter individuals from doing something unauthorized
  - Authorized Personnel Only
  - Do Not Enter
  - No Trespassing
  - Beware of Dog
  - Caution Electric Fence
  - Biohazard Danger

Cameras and Surveillance Methods

- Cameras and surveillance
  - Provide a way to monitor and record the property perimeter for intruders and potential attackers
  - Are considered deterrent and detective physical controls
  - Deliver a way to record intruders in action with recordings
  - Should trigger alerts when a camera is disabled

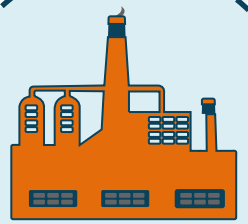


Cameras



- Inside web cams or outside systems
- Closed-circuit to SOC/linked to third-party vendor
- Should be combined with lighting
- Need to locate all dead spots
- Backup video media to safe location

Industrial Camouflage



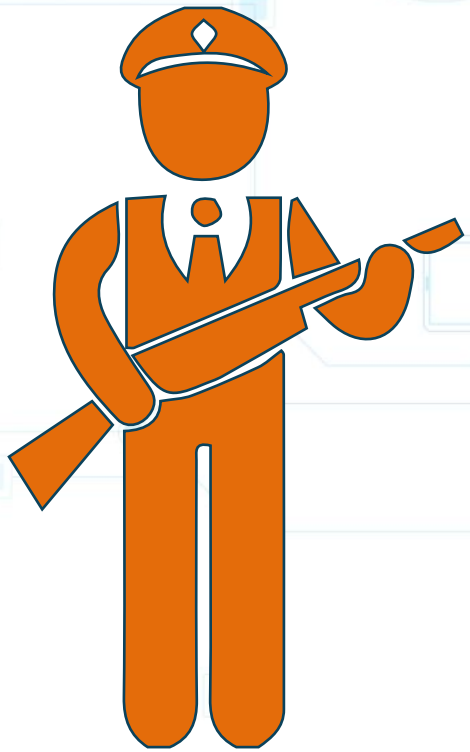
- Cameras and surveillance devices are often camouflaged in landscaping elements, statues, and tall trees
- For example, towers carrying cell phone and other equipment are covered by fake trees
- Certain high-security rooms can be underground and set at distance from main buildings

Personnel Controls

- Many organizations will have all guests register at a reception area security desk
  - Collect and input identification information in visitor log
  - Camera station with picture for temporary badge
  - Distribute temporary access cards or badges
- Guests may need to always be escorted by another employee or security officer to provide two-person integrity and control

Security Guards

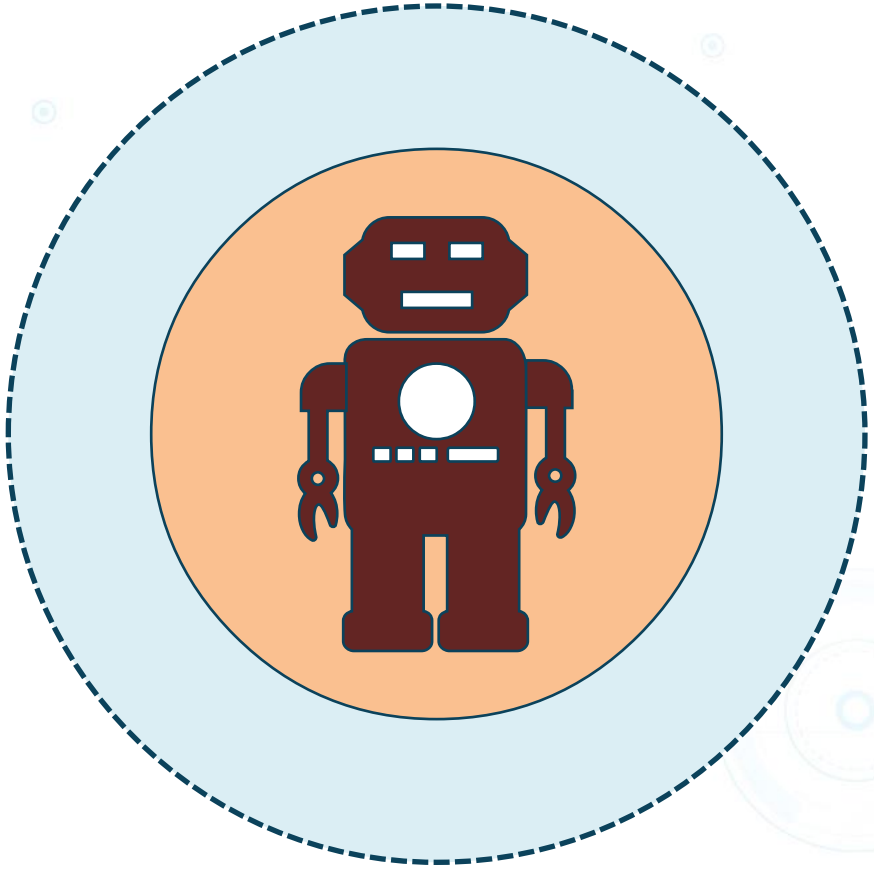
- Guards are typically 24x7 but could be just business hours
- They are a security control of multiple types
  - Detective
  - Deterrent
  - Preventative
- They can provide rapid security response if an intrusion or incident occurs



Security Guard Considerations

- Do you hire or contract, freelance, or certified/licensed?
- Will they be armed or unarmed?
- What is the impact on insurance policies?
- Are you involved with screening and background checks?
- Who provides the ongoing training?

Robot Sentries



- Robot sentries can be used in home or commercial environments as security guards with cameras, sensors, and more
- The Samsung SGR-A1 is a type of sentry gun that was developed jointly with Korea University to support South Korean troops in the Korean Demilitarized Zone

Locking Mechanisms

- Locks are the most common physical security mechanism
- They are considered a preventative control although they technically only delay entry - not prevent it in the long run
- Locks keep honest people out but cannot deter resolute intruders since most locks are easily bypassed and most keys are readily duplicated
- They can be physical, electronic, and/or biometric

Picking Locks

- Picking involves using a tension wrench to rotate the key plug of the lock to find the lock tumblers
- At the same time, the pick is used to move the binding tumblers, one at a time, to the shear line
- When all the tumblers are aligned properly with the shear line, the lock opens

Raking Locks

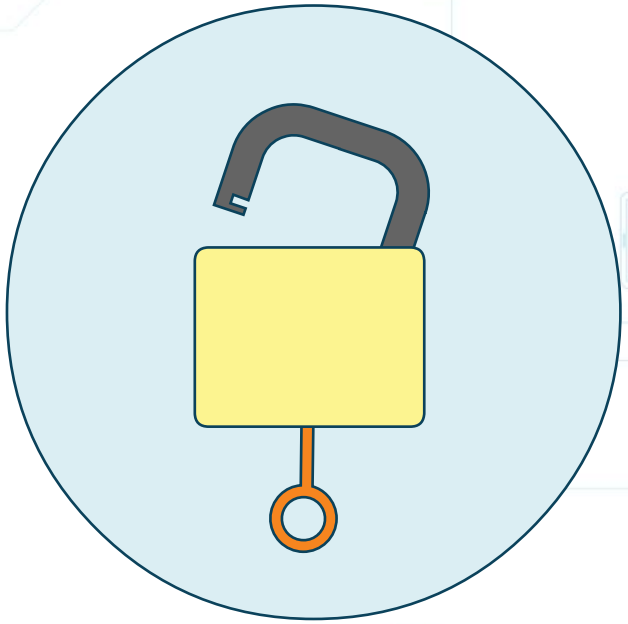
- Raking uses a pick that has a wider tip inserted all the way to the back of the plug.
- The pick is then pulled out quickly, so that all the pins are bounced up.
- As the rake exits, a tension wrench turns the plug.
- Some of the upper pins will fall on the ledge created by the turning pins where the attacker can easily pick the remaining pins

Brute Forcing Locks

- Brute force techniques will always be successful given enough time and effort
- This involves using hammers, tire irons, firearms, and more
- This contributes to locks being a "delay" control

Types of Locks

- Key lock - a lock that requires a key to open
- Warded - wards are obstructions to the keyhole that prevent all but the properly cut key from entering
- Wafer/tumbler - wafers under spring tension are in the core or plug of the lock and protrude outside the diameter of the plug into a shell formed by the lock body

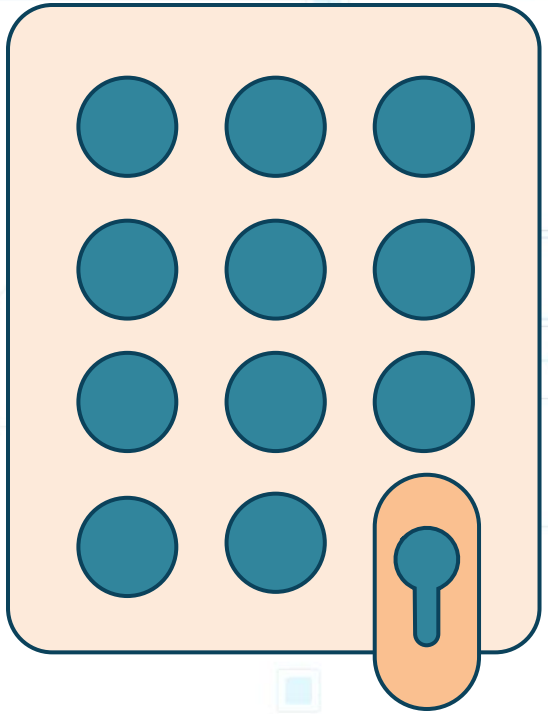


Types of Locks

- Pin tumbler - keys moves pins so that a shear line can be obtained, allowing the key to turn the plug and operate the lock
  - More secure than warded and wafer/tumbler locks
- Deadbolt - a bolt inserted into the frame of the door for additional security when combined with other locks
- Interchangeable core - a lock with a core that can be removed and replaced using a special-change key
- Combination - a sequence of numbers in proper order

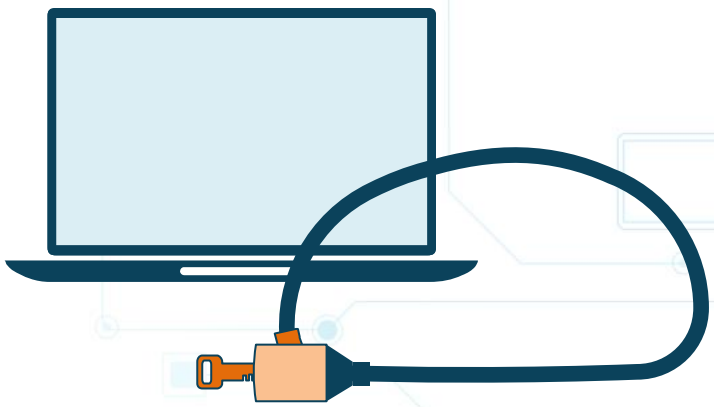
Types of Locks

- Electronic combination
  - Digital readouts obtain power from the energy created when the dials are turned
  - Higher security than combination locks, but more expensive
- Keyless
  - Lock that has buttons that are pushed in sequence to open the door
  - Sometimes called a cipher lock
- Smart lock
  - Inexpensive plastic card that is pre-authenticated to open a door
  - Used in most hotels



Types of Locks

- Cable locks are used to secure devices to a desk or shelf and deter theft of the device
  - Can also be used in combination with laptop docking stations
- USB data blockers are a form of USB locking to prevent infecting your smartphone or tablet with malware
  - They can also prevent attackers from executing or installing malicious code on your device to access your data



Fire Controls

- Prevention
  - Fire-rated construction materials, training, safety
  - Be prepared
- Detection
  - Smoke and fire detectors, sensors
  - Control quickly, minimize damage
- Suppression
  - Contain and extinguish the fire

Fire Controls

- Type A - common combustibles, such as wood products, paper, and laminates
  - Suppressed with water or soda acid
- Type B - combustible liquids, such as petroleum products and coolants
  - Suppressed using halon substitutes, carbon dioxide, dry powders, or soda acids
- Type C - electrical equipment and wires
  - Extinguished using gas, dry powders, or carbon dioxide
- Type D combustible metals
  - Can be suppressed only with dry powder

Types of Sensors

Lighting is the most common

- Good lighting is used in combination with other controls to protect many internal and external areas.
- Potential attackers prefer the cover of darkness. Lighting is a detective and sometimes preventative control.

- Lighting can enhance other security controls such as cameras, security guards, and sensors. They should start at the perimeter and be used in every defense-in-depth mechanism to the "keep"

- Mercury vapor
- Sodium vapor
- Quartz
- LED
- Continuous lighting
- Trip lighting
- Standby lighting
- Emergency lighting

Types of Sensors

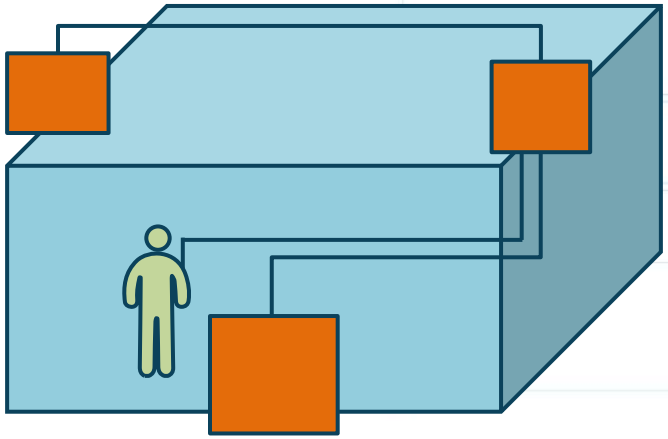
- Photoelectric - a break in a light beam
- Passive infrared - detecting infrared light
- Vibration - a change in the level of vibration
- Acoustical - noise detection of a change in sound waves
- Microwave - a change in high-frequency radio waves
- Electro-mechanical - a break in electrical circuit
- Electrostatic - a change in an electrostatic field
- Moisture and temperature detection - for server rooms and data center environmental controls

Sensors Trigger Alarms

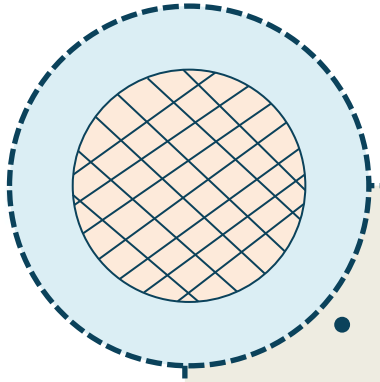
- Static or flashing light on display panel
- Bell rings or horn blares
- SMS or text message sent
- Telephone call or software
- Silent alarms

Mantraps

- Mantraps and cages are often used to control access to a facility or a specific area of a facility
- There is an entry and exit door but only one door can be open at a time
- One person at a time - no piggybacking (tailgating)
- The person can be identified and authenticated
  - Provide credentials and license or passport
  - Can include biometric readers
  - CCTV and intercom systems are often used
  - Security guard behind bullet-proof glass
  - The person is eventually allowed in through strong door with electronic locks



Faraday Cages



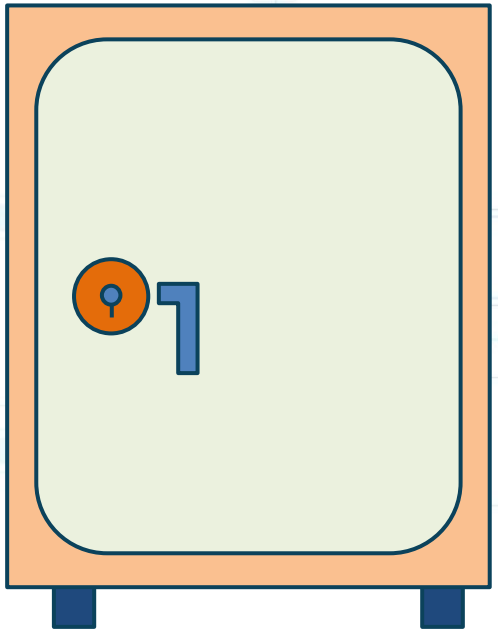
- Faraday cages are rooms, enclosures, or bags that block electromagnetic fields emanating from Electric Magnetic Interference (EMI), Carrington events, solar flares, and Electro-magnetic Pulses (EMP)
- The shield may be fashioned from a continuous covering of conductive material, or in the case of a Faraday cage, a mesh of similar materials
- These can often be found in data centers or other enterprise safe rooms

Cable Runs and Distribution Frames

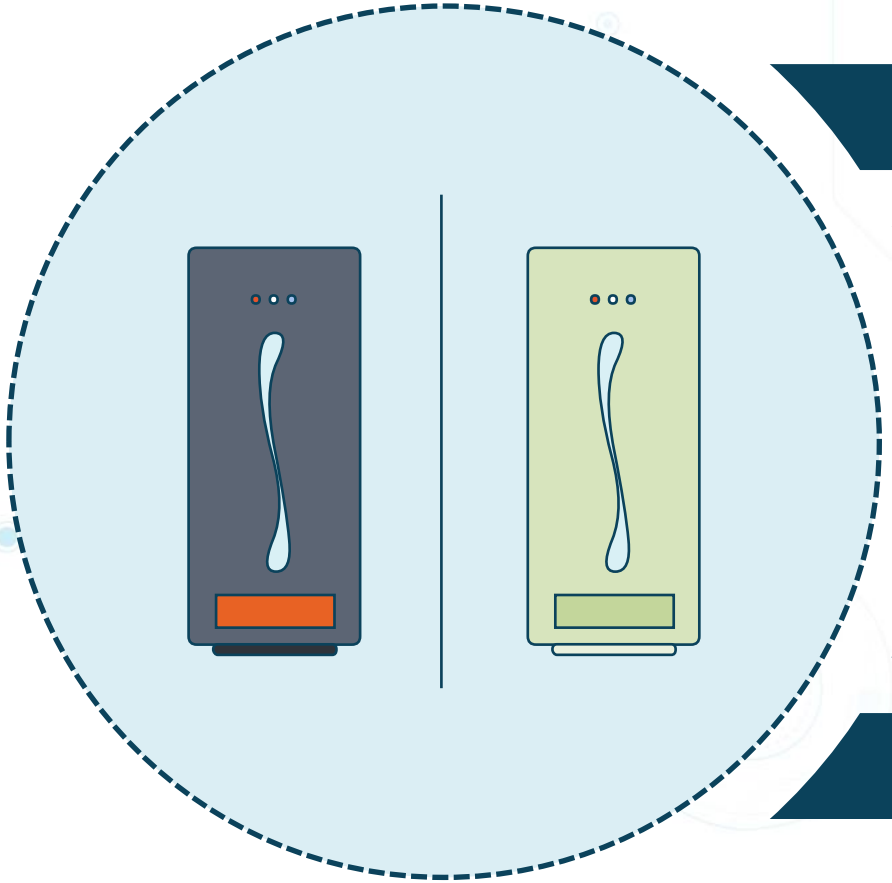
- Remember all cable runs and distribution frame (MDF rooms) rooms and closets
  - Under the floor
  - Above ceiling panels
  - Lock all doors to server rooms
  - Cameras can be used along with other types of sensors

Safes and Vaults

- Safes and vaults may often be where the most valuable corporate physical assets are stored
  - Currency, deeds, licenses, precious metals, diamonds, securities, policies, and failsafe passwords
- They should be attached to the physical infrastructure so it cannot be easily carried away
- Considerations
  - Location
  - Fire and burglar-proof
  - Type of lock (MFA)
  - Material of safe - tensile strength
  - Weight
  - Relocking devices (timers)
  - Sensors and alarms



Air Gap



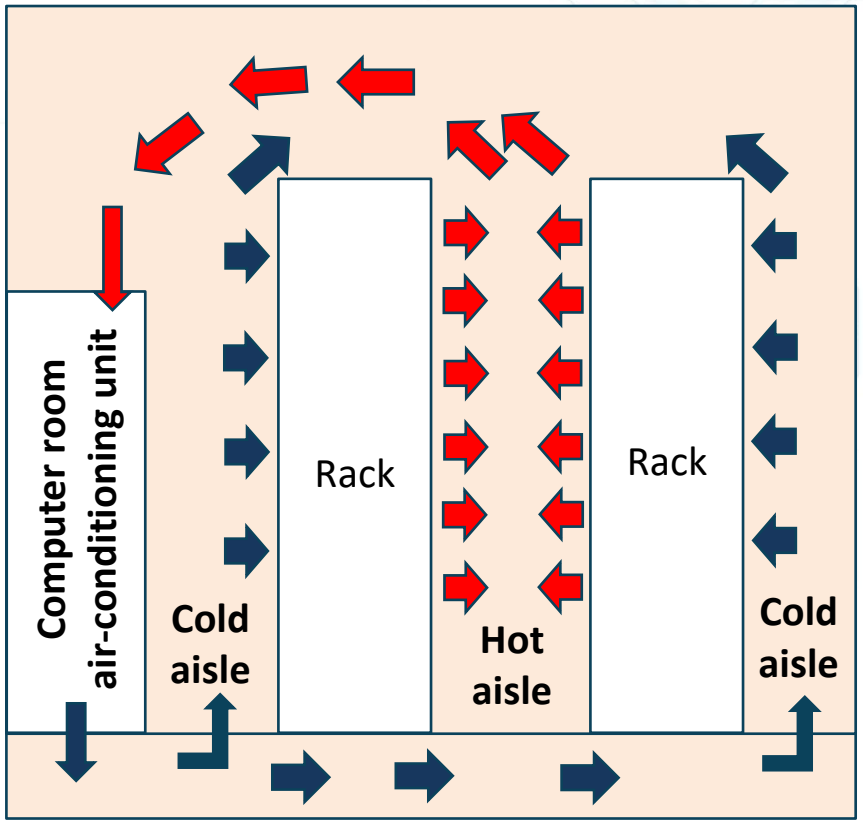
- Secure system has no access to Internet
- Very limited access to LAN, if any
- Can be physical or logical
- Still vulnerable to rogue insider
- Stuxnet was introduced to air-gapped area

Air Gap

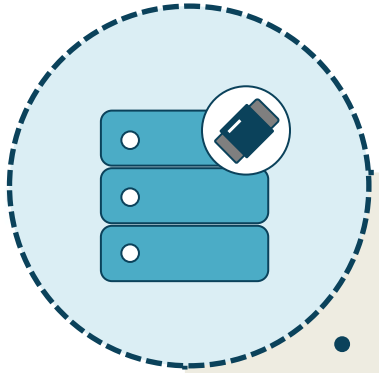
- Military and governmental agency networks and systems
- Financial systems such as stock and cybercurrency exchanges
- Industrial control systems like SCADA in water processing facilities
- Life-critical systems such as nuclear power plants, computers used in aviation, and computerized medical equipment

Hot and Cold Aisles

- Heating, ventilation, and air-conditioning (HVAC) are vital environmental issues
  - Poor HVAC leads to extreme heat, cold, humidity, or dryness
  - Recommended temp: 72 to 76 degrees
  - Recommended humidity: 40 - 60%
- Maintain hot and cold aisles in the server rooms and data center to move hot air from devices into a hot aisle and redirect to an air conditioning unit or room

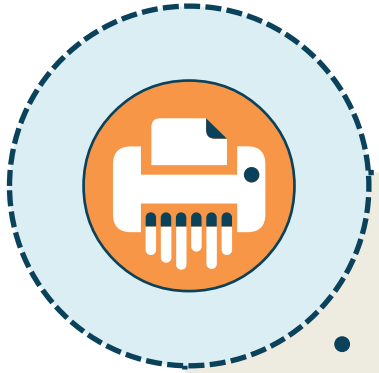


Data Sanitation



- Degaussing - removing the magnetic field of physical drive
- Purging - clearing everything off the media with software programs
- Wiping - overwrite every sector of drive with 1s and 0s
- Encryption - encrypt all files before deletion or disposal of media

Secure Data Destruction



- Burning
- Shredding
- Pulping
- Pulverizing
- Third-party solutions

ping

Command Prompt

```
C:\Users\shankhantoo>ping www.skillsoft.com

Pinging www.skillsoft.com [54.227.113.190] with 32 bytes of data:
Reply from 54.227.113.190: bytes=32 time=66ms TTL=48
Reply from 54.227.113.190: bytes=32 time=73ms TTL=48
Reply from 54.227.113.190: bytes=32 time=67ms TTL=48
Reply from 54.227.113.190: bytes=32 time=73ms TTL=48

Ping statistics for 54.227.113.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 73ms, Average = 69ms

C:\Users\shankhantoo>ping 54.227.113.190

Pinging 54.227.113.190 with 32 bytes of data:
Reply from 54.227.113.190: bytes=32 time=74ms TTL=48
Reply from 54.227.113.190: bytes=32 time=69ms TTL=48
Reply from 54.227.113.190: bytes=32 time=91ms TTL=48
Reply from 54.227.113.190: bytes=32 time=62ms TTL=48

Ping statistics for 54.227.113.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 91ms, Average = 74ms

C:\Users\shankhantoo>
```

tracert/pathping

Command Prompt

```
C:\Users\shankhantoo>tracert www.google.com

Tracing route to www.google.com [172.217.14.164]
over a maximum of 30 hops:

  1     4 ms    17 ms     8 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3   147 ms    36 ms    35 ms  173-219-226-204.suddenlink.net [173.219.226.204]
  4    39 ms    33 ms    24 ms  173-219-233-246.suddenlink.net [173.219.233.246]
  5    37 ms    34 ms    44 ms  72.14.202.216
  6    41 ms    54 ms    44 ms  108.170.252.161
  7   112 ms    40 ms    33 ms  72.14.236.139
  8    42 ms   133 ms    41 ms  dfw28s22-in-f4.1e100.net [172.217.14.164]

Trace complete.

C:\Users\shankhantoo>
```

nslookup

Command Prompt

```
C:\Users\shankhantoo>nslookup www.skillsoft.com
Server:  rdns01.suddenlink.net
Address:  208.180.42.68

Non-authoritative answer:
Name:    www.skillsoft.com
Address:  54.227.113.190


C:\Users\shankhantoo>
```

DNSenum

- DNS enumeration tool
- Locates all DNS servers and entries
- Helps to gather critical information
- Usernames, system names, IPs, etc.

ipconfig

Command Prompt

```
C:\Users\shankhantoo>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : ::cce8:3c9f:1e8b:c27a
   Temporary IPv6 Address. . . . . . : ::6592:e920:b68:8fc7
   Link-local IPv6 Address . . . . . : fe80::cce8:3c9f:1e8b:c27a%4
   IPv4 Address. . . . . . . . . . . : 192.168.0.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : PEROOT.COM

Tunnel adapter isatap.{2293103F-D08C-4C57-8D8D-EFE8435D7B9E}:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\shankhantoo>
```

netstat

Command Prompt - netstat -a

```
C:\Users\shankhantoo>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            cybragnt:0             LISTENING
  TCP    0.0.0.0:445            cybragnt:0             LISTENING
  TCP    0.0.0.0:5012           cybragnt:0             LISTENING
  TCP    0.0.0.0:49152          cybragnt:0             LISTENING
  TCP    0.0.0.0:49153          cybragnt:0             LISTENING
  TCP    0.0.0.0:49154          cybragnt:0             LISTENING
  TCP    0.0.0.0:49155          cybragnt:0             LISTENING
  TCP    0.0.0.0:49156          cybragnt:0             LISTENING
  TCP    0.0.0.0:49160          cybragnt:0             LISTENING
  TCP    0.0.0.0:49213          cybragnt:0             LISTENING
  TCP    127.0.0.1:6543         cybragnt:0             LISTENING
  TCP    127.0.0.1:43227        cybragnt:0             LISTENING
  TCP    127.0.0.1:58284        cybragnt:58285         ESTABLISHED
  TCP    127.0.0.1:58285        cybragnt:58284         ESTABLISHED
  TCP    127.0.0.1:58286        cybragnt:58287         ESTABLISHED
  TCP    127.0.0.1:58287        cybragnt:58286         ESTABLISHED
  TCP    127.0.0.1:58305        cybragnt:58306         ESTABLISHED
  TCP    127.0.0.1:58306        cybragnt:58305         ESTABLISHED
  TCP    127.0.0.1:58308        cybragnt:58309         ESTABLISHED
  TCP    127.0.0.1:58309        cybragnt:58308         ESTABLISHED
  TCP    127.0.0.1:58363        cybragnt:58364         ESTABLISHED
  TCP    127.0.0.1:58364        cybragnt:58363         ESTABLISHED
  TCP    192.168.0.20:139       cybragnt:0             LISTENING
  TCP    192.168.0.20:56212     server-143-204-160-92:https  CLOSE_WAIT
  TCP    192.168.0.20:58271     52.111.227.4:https     ESTABLISHED
  TCP    192.168.0.20:58289     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.20:58290     104.16.248.249:https   ESTABLISHED
  TCP    192.168.0.20:58300     ec2-52-89-235-93:https  ESTABLISHED
  TCP    192.168.0.20:58321     40.126.0.65:https      TIME_WAIT
  TCP    192.168.0.20:58339     64.4.54.254:https      TIME_WAIT
```

arp

Command Prompt

```
C:\Users\shankhantoo>arp -a

Interface: 192.168.0.20 --- 0x4
  Internet Address      Physical Address      Type
  192.168.0.1           3c-7a-8a-7c-aa-57     dynamic
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\shankhantoo>
```

route

Command Prompt

```
C:\Users\shankhantoo>route print
===========================================================================
Interface List
  6...5e b5 7d 4f 59 f4 ......Microsoft Hosted Network Virtual Adapter
  5...1e b5 7d 4f 59 f4 ......Microsoft Wi-Fi Direct Virtual Adapter
  4...ac b5 7d 4f 59 f4 ......Qualcomm Atheros AR956x Wireless Network Adapter
  3...30 65 ec 69 84 af ......Realtek PCIe GBE Family Controller
  1...........................Software Loopback Interface 1
  7...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1     192.168.0.20     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.0.0    255.255.255.0         On-link      192.168.0.20    281
     192.168.0.20  255.255.255.255         On-link      192.168.0.20    281
    192.168.0.255  255.255.255.255         On-link      192.168.0.20    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link      192.168.0.20    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      192.168.0.20    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  4    281 ::/64                   On-link
  1    306 ::1/128                 On-link
  4    281 ::6592:e920:b68:8fc7/128 On-link
  4    281 ::cce8:3c9f:1e8b:c27a/128
```

hping

Command-line TCP/IP packet assembler and network analysis tool that supports TCP, UDP, ICMP, and RAW-IP with an additional traceroute mode

- Auditing TCP/IP stacks
- Discovering path MTU
- Fingerprinting OS's
- Guessing remote uptime
- Performing advanced traceroute
- Scanning ports
- Testing networks and firewalls

netcat

- The swiss army knife of networking tools
- Simple utility that reads and writes data across TCP or UDP network connections
- Feature-rich network debugging and exploration tool, as it can create almost any kind of connection needed, including port binding to accept incoming connections
- Designed to be a reliable back-end tool to use directly
- Often driven by other programs and scripts

curl

- Used in command lines and scripts to facilitate data transfers
- The de facto Internet transfer backbone for thousands of software applications
- Also used in automobiles, televisions, routers, printers, audio equipment, mobile phones, tablets, and media players

theHarvester

- An OSINT tool like Maltego that collects emails, subdomains, hosts, employee names, open ports, and banners from various public sources like search engines, PGP key servers, and the SHODAN computer database
- Intended to assist pen testers in the early stages of a black or gray box test to realize the customer footprint on the Internet

Cuckoo Sandbox

- Open source automated malware analysis system that helps you understand the context, motivations, and goals of an attack or a breach
- Delivers a detailed report that summarizes the activities of inputted files when executed
- Runs inside a realistic but isolated environment known as a sandbox
- Freeware that automates the task of analyzing malicious files in Windows, macOS, Linux, and Android

Nmap

- Open source network mapping utility for discovery and security auditing
- Used for network inventory, managing service upgrade schedules, and monitoring host or service uptime
- Examines raw IP packets to determine what hosts are available on the network, what services those hosts are offering, OS versions running, type of packet filters/firewalls in use, and more
- Designed to rapidly scan large networks and run on all major computer operating systems
- Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping)

Nessus

- One of the most popular and capable vulnerability scanners, particularly for *nix systems
- It recently changed the free version from Home to Essentials, and will scan up to 16 devices for free

Nessus

Nessus | Scans | Settings

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Customized Reports
- Scanners

Scan Templates
‹ Back to Scans

Scanner

Search Library

Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

UPGRADE
MDM Config Audit
Audit the configuration of mobile device managers.

UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration of network devices.

UNOFFICIAL
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

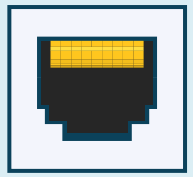
WannaCry Ransomware
Remote and local checks for MS17-010.

Tenable, “Download Nessus Vulnerability Assessment: Tenable®,” Download Nessus Vulnerability Assessment | Tenable®, 2020, https://www.tenable.com/products/nessus.

sn1per

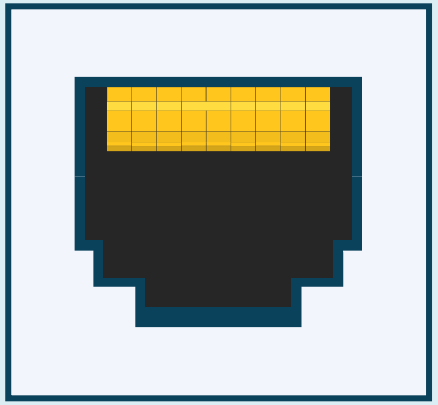
- A cutting-edge vulnerability and penetration scanning utility that automates the functions and processes of collecting data
- It includes a plethora of well-known open-source tools and utilities to leverage during a penetration test to enumerate and scan for vulnerabilities

Tcpreplay



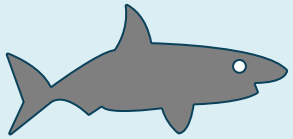
- An assortment of free open source tools for modifying and reiterating already-captured traffic on a network
- Initially created to replay malicious traffic datagrams to IDS and IPS sensor devices and modules
- It also has the ability to replay to web services

Tcpdump



- Outputs an explanation of the contents of IP packets on a network interface that match various regular expressions
- The description is preceded by a timestamp
- Can also run with the -w flag, which will save the packet data to a file for later analysis
- The -r flag causes it to read from a saved packet file rather than to read packets from a network interface
- In all cases, only packets that match expressions will be processed by tcpdump

Wireshark



- Was originally named Ethereal
- A free and open source packet analyzer (sniffer) used for network troubleshooting, analysis, software, and communications protocol development, and education
- Useful to explore sample captures at: https://wiki.wireshark.org/SampleCaptures

Wireshark

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
70	13.032590	fe80::cce8:3c9f:1e8…	ff02::1:3	LLMNR	84	Standard query 0x711d A wpad
71	13.033400	192.168.0.20	224.0.0.252	LLMNR	64	Standard query 0x711d A wpad
72	13.201099	192.168.0.5	224.0.0.251	MDNS	169	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR …
73	13.209603	fe80::1438:f64b:b0b…	ff02::fb	MDNS	189	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR …
74	13.509942	192.168.0.5	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
75	13.618615	fe80::1438:f64b:b0b…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
76	14.210105	192.168.0.5	224.0.0.251	MDNS	169	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR …
77	14.233208	fe80::1438:f64b:b0b…	ff02::fb	MDNS	189	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR …
78	14.327869	192.168.0.14	239.255.255.250	UDP	279	43100 → 1902 Len=237
79	14.335478	fe80::3e7a:8aff:fe7…	ff02::1:ff70:d57	ICMPv6	86	Neighbor Solicitation for ::14b:19ba:6c70:d57 from 3c:7a:8a:7c:aa:57
80	15.666789	fe80::1438:f64b:b0b…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
81	15.872081	fe80::3e7a:8aff:fe7…	ff02::1	ICMPv6	110	Router Advertisement from 3c:7a:8a:7c:aa:57
82	15.973963	MS-NLB-PhysServer-1…	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.12
83	18.841154	fe80::3e7a:8aff:fe7…	ff02::1	ICMPv6	110	Router Advertisement from 3c:7a:8a:7c:aa:57
84	18.943978	MS-NLB-PhysServer-1…	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.12
85	19.335905	192.168.0.14	239.255.255.250	UDP	279	43100 → 1902 Len=237
86	21.810934	fe80::3e7a:8aff:fe7…	ff02::1	ICMPv6	110	Router Advertisement from 3c:7a:8a:7c:aa:57
87	22.015532	MS-NLB-PhysServer-1…	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.12

```
▷ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{2293103F-D08C-4C57-8D8D-EFE8435D7B9E}, id 0
◢ Ethernet II, Src: ARRISGro_7c:aa:57 (3c:7a:8a:7c:aa:57), Dst: IPv6mcast_ff:a4:54:ac (33:33:ff:a4:54:ac)
  ▷ Destination: IPv6mcast_ff:a4:54:ac (33:33:ff:a4:54:ac)
  ▷ Source: ARRISGro_7c:aa:57 (3c:7a:8a:7c:aa:57)
    Type: IPv6 (0x86dd)
```

```
0000  33 33 ff a4 54 ac 3c 7a  8a 7c aa 57 86 dd 60 00   33··T·<z ·|·W··`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 3e 7a   ··· :··· ######>z
0020  8a ff fe 7c aa 57 ff 02  00 00 00 00 00 00 00 00   ···|·W·· ########
0030  00 01 ff a4 54 ac 87 00  ac a7 00 00 00 00 00 00   ····T··· ########
0040  00 00 00 00 00 00 58 74  e7 c4 00 a4 54 ac 01 01   ######Xt ····T···
0050  3c 7a 8a 7c aa 57                                  <z·|·W
```

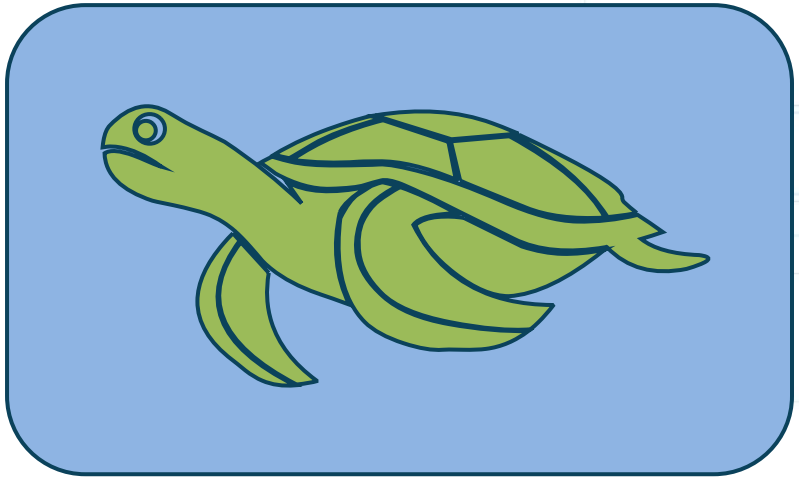
Wi-Fi: <live capture in progress> | Packets: 87 · Displayed: 87 (100.0%) | Profile: Default

Linux File Manipulation Commands

- Head
  - Prints the top number (N) of amount of data from the given input
- Tail
  - Passes the name of a file and it will show you the last ten lines from that file
- Cat
  - Concatenates files and displays the output to the standard output (usually the shell)
- Grep
  - searches for a regular expression that matches text in a file, multiple files, or a stream of input
- Chmod
  - changes the access permissions of files and folders
- Logger
  - Adds log files to /var/log/syslog from the command line, scripts, or other files

Secure Shell

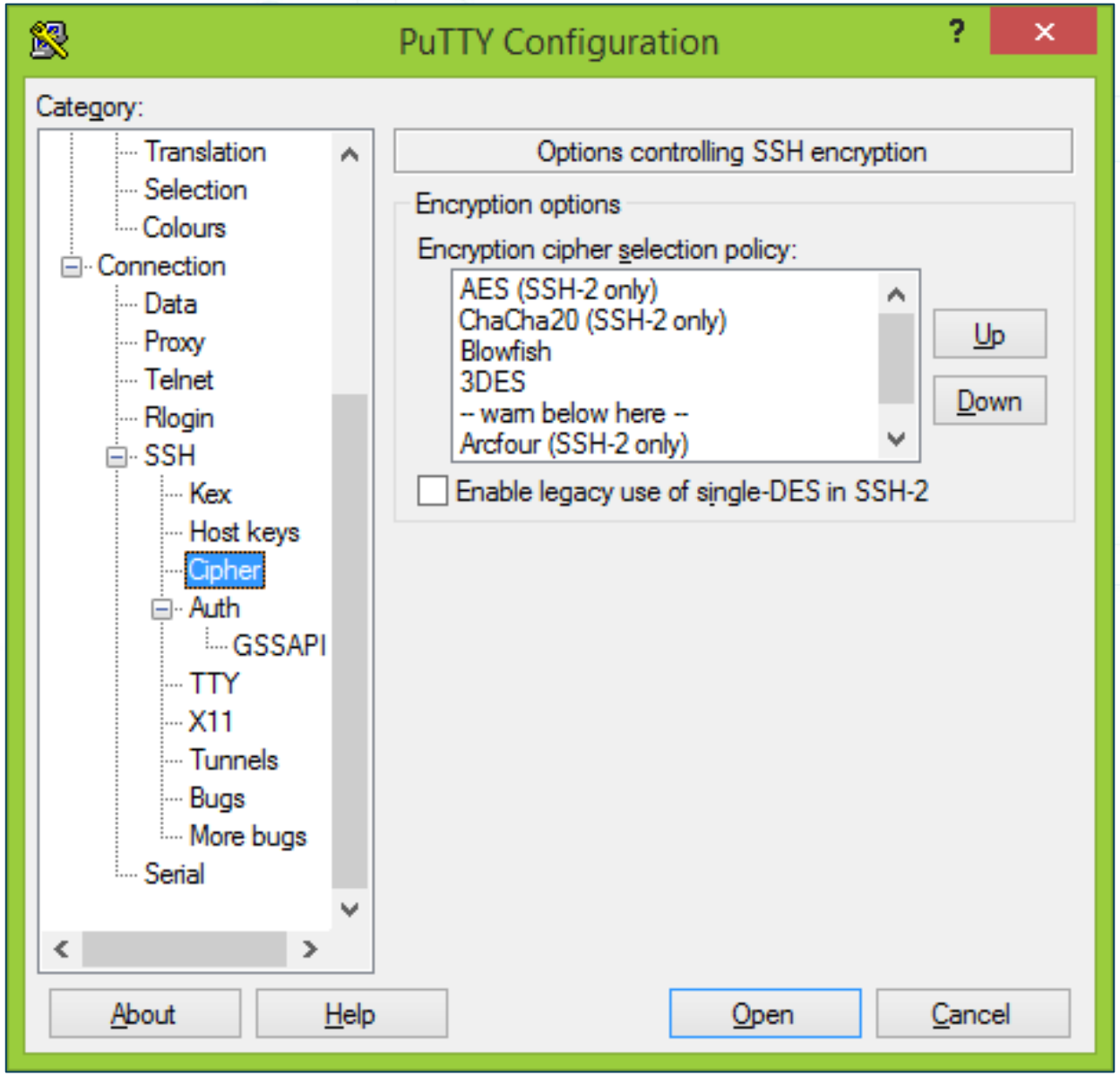
- Management access should be limited to secure protocol alternatives, as in SSH instead of Telnet
- SSH2 is preferable to SSH1 whenever possible
- SSH2 uses symmetric encryption for the bulk data encryption and asymmetric algorithms in their key management processes
- SSH2 uses DH for key exchange



SSH2 on a Cisco Router

- Router(config)#hostname SecplusR1
- SecplusR1(config)#ip domain-name example.com
- SecplusR1(config)#crypto key generate rsa general-keys modulus 2048
- The name for the keys will be: SecplusR1.example.com
- % The key modulus size is 2048 bits
- % Generating 2048 bit RSA keys, keys will be non-exportable...
- [OK] (elapsed time was 0 seconds)
- *Apr 9 19:01:50.517: %SSH-5-ENABLED: SSH 1.99 has been enabled
- SecplusR1(config)#username admin secret S3curitY3Plu5
- SecplusR1(config)#line vty 0 15
- SecplusR1(config-line)#login local
- SecplusR1(config-line)#transport input ssh

SSH with PuTTY



PowerShell

- A command-line configuration and automation management framework introduced by Microsoft
- It is very popular with systems administrators and management users who automate tasks in Microsoft Azure
- It commonly uses cmdlets, filenames, and variables

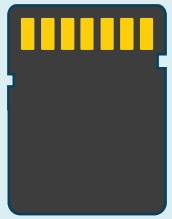
OpenSSL

- A strong, commercial-grade, full-featured toolkit for Secure Sockets Layer (SSL) and primarily Transport Layer Security (TLS) protocols
- Also a general-purpose cryptography library
- Licensed under an Apache-style license, which means that you are free to get and use it for commercial and non-commercial purposes subject to some basic license conditions

Forensic Tools: dd

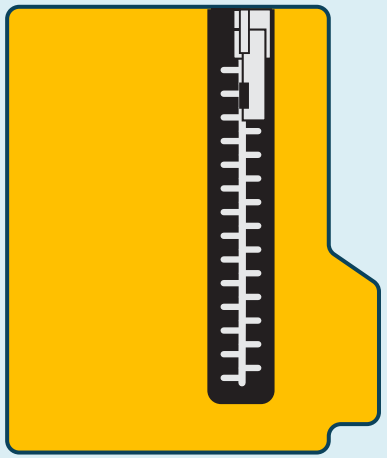
- Write disk image files to memory cards and removable storage
  - Flash IMG files to SD cards
- Create bootable USB stick from ISO files of Linux installations
- Back up and restore IMG files to memory card and disk
- Back up and compress disk image files to significantly reduce the file size of backups
- Install and restore compressed disk image files on the fly
- Supported file formats: IMG, ISO, Zip, GZip, and XZ

Memdump



- Forensics tool that allows you to extract files such as jpg, gif, and pdf from memory dumps
- Supports extraction from any kind of binary files, like .dmp, .bin, and .lime
- Performs automated file signature-based searching inside memory dump and then extracts them
- Selects predefined profiles for specific file types and creates custom profiles for a different file format

FTK Imager



- Data preview and imaging tool
- Assesses electronic evidence
- Creates forensic images of computer
- Uses write-blocking methods
- Helps justify deeper analysis

FTK Imager

AccessData FTK Imager 3.0.0.1443

File View Mode Help

- Add Evidence Item...
- Add All Attached Devices
- Image Mounting...
- Remove Evidence Item
- Remove All Evidence Items
- Create Disk Image...
- Export Disk Image...
- Export Logical Image (AD1)...
- Add to Custom Content Image (AD1)
- Create Custom Content Image (AD1)...
- Verify Drive/Image...
- Capture Memory...
- MetaCarve (Deep Scan)
- Obtain Protected Files...
- Detect EFS Encryption
- Export Files...
- Export File Hash List...
- Export Directory Listing...
- Exit

File List

Name	Size	Type	Date Modified
Inbox - emca.pst	4,233 KB	Regular File	3/19/2009 2:11:...
Inbox - untroubled.pst	4,481 KB	Regular File	3/19/2009 2:11:...
Inbox other.pst	10,681 KB	Regular File	3/19/2009 11:5...

```
020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 7B DC 76 | ..          ··{Üv
030 73 3A 73 3A 00 00 DD 76-73 3A 0A 00 00 00 00 00 | s:s:··Ývs:......
040 42 70 00 73 00 74 00 00-00 FF FF 0F 00 02 FF FF | Bp·s·t···ÿÿ···ÿÿ
050 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF | ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
060 01 49 00 6E 00 62 00 6F-00 78 00 0F 00 02 20 00 | ·I·n·b·o·x····· ·
070 2D 00 20 00 65 00 6D 00-63 00 00 00 61 00 2E 00 | -· ·e·m·c···a·.·
080 49 4E 42 4F 58 2D 7E 31-50 53 54 20 00 AF F8 76 | INBOX-~1PST ·¯øv
090 73 3A 73 3A 00 00 64 71-73 3A 0C 00 00 24 42 00 | s:s:··dqs:···$B·
0a0 42 75 00 62 00 6C 00 65-00 64 00 0F 00 E2 2E 00 | Bu·b·l·e·d···â.·
0b0 70 00 73 00 74 00 00 00-FF FF 00 00 FF FF FF FF | p·s·t···ÿÿ··ÿÿÿÿ
0c0 01 49 00 6E 00 62 00 6F-00 78 00 0F 00 E2 20 00 | ·I·n·b·o·x···â ·
0d0 2D 00 20 00 75 00 6E 00-74 00 00 00 72 00 6F 00 | -· ·u·n·t···r·o·
0e0 49 4E 42 4F 58 2D 7E 32-50 53 54 20 00 4B FD 76 | INBOX-~2PST ·Kýv
0f0 73 3A 73 3A 00 00 64 71-73 3A 95 10 00 04 46 00 | s:s:··dqs:····F·
100 42 73 00 74 00 00 00 FF-FF FF FF 0F 00 33 FF FF | Bs·t···ÿÿÿÿ··3ÿÿ
110 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF | ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
120 01 49 00 6E 00 62 00 6F-00 78 00 0F 00 33 20 00 | ·I·n·b·o·x···3 ·
130 6F 00 74 00 68 00 65 00-72 00 00 00 2E 00 70 00 | o·t·h·e·r···.·p·
140 49 4E 42 4F 58 4F 7E 31-50 53 54 20 00 65 04 77 | INBOXO~1PST ·e·w
150 73 3A 73 3A 00 00 CF 5E-73 3A 16 22 00 E4 A6 00 | s:s:··Ï^s:·"·ä¦·
```

FTK Imager

AccessData FTK Imager 3.0.0.1443

File View Mode Help

Evidence Tree

- Spam.E01
  - NONAME [FAT16]
    - [root]
      - Documents and Settings
        - Administrator
          - Local Settings
            - Application Data
            - Microsoft
              - Outlook
      - [unallocated space]

File List

Name	Size	Type	Date Modified
Inbox - emca.pst	4,233 KB	Regular File	3/19/2009 2:11:...
Inbox - untroubled.pst	4,481 KB	Regular File	3/19/2009 2:11:...
Inbox other.pst	10,681 KB	Regular File	3/19/2009 11:5...

Create Image

Select Image Destination

Image Destination Folder

Browse

Image Filename (Excluding Extension)

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption ☐

Filter by File Owner ☑

< Back Finish Cancel Help

Custom Content Sources

Evidence:File System|Path|File

*

New Edit Remove Remove All

Properti

Gene

Name	Outlook
File Class	Directory
File Size	1,024
Physical Size	1,024
Start Cluster	11
Date Created	3/19/2009 2:54:57 PM
Date Modified	3/18/2009 7:59:50 PM

```
0d0 2D 00 20 00 75 00 6E 00-74 00 00 00 72 00 6F 00 -· ·u·n·t···r·o·
0e0 49 4E 42 4F 58 2D 7E 32-50 53 54 20 00 4B FD 76 INBOX-~2PST ·Kýv
0f0 73 3A 73 3A 00 00 64 71-73 3A 95 10 00 04 46 00 s:s:··dqs:····F·
100 42 73 00 74 00 00 00 FF-FF FF FF 0F 00 33 FF FF Bs·t···ÿÿÿÿ··3ÿÿ
110 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
120 01 49 00 6E 00 62 00 6F-00 78 00 0F 00 33 20 00 ·I·n·b·o·x···3 ·
130 6F 00 74 00 68 00 65 00-72 00 00 00 2E 00 70 00 o·t·h·e·r···.·p·
140 49 4E 42 4F 58 4F 7E 31-50 53 54 20 00 65 04 77 INBOXO~1PST ·e·w
150 73 3A 73 3A 00 00 CF 5E-73 3A 16 22 00 E4 A6 00 s:s:··Ï^s:·"·ä¦·
```

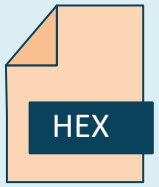
FTK Imager

5_After_Artifact_Analysis - Excel

A25 | 1/16/2017 11:14:54 PM

	A	B	C	
1	Date (Newest to Oldest)	Artifact Involved	Action	
2	1/16/2017 23:29:21	E:\[root]\Documents and Settings\Donald Blake\Application Data\Skype\dblake_personal\chatmsg256.dbb	Chat Messages with Loki - Last Message = "DONE" from DBLAKE	Examination of FTK string sea
3	1/16/2017 23:27:24	C:\Documents and Settings\Donald Blake\My Documents\Business Plans\S	Recycled	INFO2 File - > RECYCLER\S-1-5
4	1/16/2017 23:27:03	F:\ (Workout IPO)	Last Opened	LNK File - Modification Time,
5	1/16/2017 23:27:02	F:\TIVO Research - CONFIDENTIAL - BACKUP2.doc	Last Opened	LNK File - Modification Time,
6	1/16/2017 23:27:02	C:\Program Files\Windows NT\Accessories\WORDPAD.EXE (6)	Wordpad Executed Last	NTUSER.DAT - RR - USERASSIS
7	1/16/2017 23:27:02	WORDPAD.EXE Executed Last	Last Executed	Prefetch
8	1/16/2017 23:26:50	F:\TIVO Research - CONFIDENTIAL - BACKUP2.doc	Copied to F:\ (WORKOUT IPO)	LNK FILE - Target Creation Tim
9	1/16/2017 23:25:30	F:\SECRET\SECRET.zip	Last Opened	LNK File - Modification Time,
10	1/16/2017 23:25:30	F:\SECRET	Last Opened	LNK File - Modification Time,
11	1/16/2017 23:25:28	C:\PROGRA~1\WINZIP\winzip32.exe	Winzip Executed Last	NTUSER.DAT - RR - USERASSIS
12	1/16/2017 23:25:28	WINZIP32.EXE Executed Last	Last Executed	Prefetch
13	1/16/2017 23:25:13	F:\SECRET\SECRET.zip	Copied to F:\ (WORKOUT IPO)	LNK File - Target Creation Tim
14	1/16/2017 23:25:13	F:\SECRET	Folder Created on F:\ (Workout IPO)	LNK File - Target Creation Tim
15	1/16/2017 23:24:06	(F:) USB KEY (Apple iPod)-- iserial# - 000A270010C4E86E	Key Inserted	SETUPAPI.LOG - USBDEVFORE
16	1/16/2017 23:20:59	E:\CONFIDENTIAL_SPREADSHEETS.zip	Last Opened	LNK File - Modification Time
17	1/16/2017 23:20:59	E:\ (Dblake Personal) folder	Last Opened	LNK File - Modification Time,
18	1/16/2017 23:18:30	E:\TIVO Research - CONFIDENTIAL.doc	Last Opened	LNK File - Modification Time,
19	1/16/2017 23:18:26	E:\Blue Harvest Business Plan v1.doc	Last Opened	LNK File - Modification Time,
20	1/16/2017 23:18:26	E:\ (Dblake Personal) folder	First Opened	LNK File - Creation Time
21	1/16/2017 23:18:19	E:\TIVO Research - CONFIDENTIAL.doc	Copied to E:\ (Dblake Personal)	LNK File - Target Creation Tim
22	1/16/2017 23:18:15	E:\CONFIDENTIAL_SPREADSHEETS.zip	Copied to E:\ (Dblake Personal)	LNK File - Target Creation Tim
23	1/16/2017 23:18:10	E:\Blue Harvest Business Plan v1.doc	Copied to E:\ (Dblake Personal)	LNK File - Target Creation Tim

WinHex



- A universal hexadecimal editor
- Useful for computer forensics, data recovery, low-level data processing, and IT security
- Advanced tool for inspecting and editing all types of files
- Recovers deleted files or lost data from hard drives with corrupt file systems or from digital camera cards

Autopsy

- According to https://www.autopsy.com/, this is a:
  - Rapid, comprehensive, and very efficient forensic hard drive investigation framework and platform
  - Used by many law enforcement professionals and enterprise cyber detectives around the world
  - Can be a primary forensic tool, an extension of a current forensic toolset, and/or as validation of findings discovered using other tools

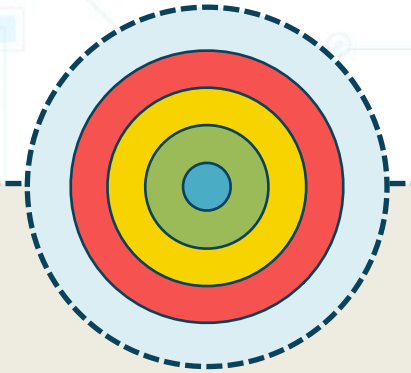
Exploitation Kits and Password Crackers

- Exploitation kits are used by penetration testers and crackers to find vulnerabilities and attack vectors
- Often specialize in certain components, like routers, browsers, embedded devices, PowerShell, etc.
- Often open source initiatives with broad cooperation from white, gray, and black hat hackers
- Can be used to prioritize vulnerabilities and threats in the enterprise
  - RIG EK and RIG-v
  - GrandSoft EK
  - GreenFlash Sundown
  - Ransomware EKs

Password Crackers

- Repeated attempts to identify a user account, password, or both
- Also runs against stored hashes on systems (or offline)
- Hackers use many tools and techniques to crack passwords:
  - Online and offline brute force
  - Dictionaries, word lists
  - Cracked password lists
  - Hybrid cracking
  - Rainbow tables

Rainbow Table Attacks



- A rainbow table is a hash function used in cryptography for storing important data, such as passwords in a backend database for a web service
- Attacker attempts to use a rainbow hash table to crack the passwords stored in a database system
- Sensitive data is often hashed multiple times with the same or different keys in order to avoid rainbow table attacks

Cain Password Cracker

File View Configure Tools Help

Decoders | Network | Sniffer | Cracker | Traceroute | CCDU | Wireless | Query

- Cracker
  - LM & NTLM Hashes (0)
  - NTLMv2 Hashes (0)
  - MS-Cache Hashes (0)
  - PWL files (0)
  - Cisco IOS-MD5 Hashes (0)
  - Cisco PIX-MD5 Hashes (0)
  - APOP-MD5 Hashes (0)
  - CRAM-MD5 Hashes (0)
  - OSPF-MD5 Hashes (0)
  - RIPv2-MD5 Hashes (0)
  - VRRP-HMAC Hashes (0)
  - VNC-3DES (0)
  - MD2 Hashes (0)
  - MD4 Hashes (0)
  - MD5 Hashes (0)
  - SHA-1 Hashes (0)
  - SHA-2 Hashes (0)
  - RIPEMD-160 Hashes (0)
  - Kerb5 PreAuth Hashes (0)
  - Radius Shared-Key Hashes (0)
  - IKE-PSK Hashes (0)
  - MSSQL Hashes (0)
  - MySQL Hashes (0)
  - Oracle Hashes (0)
  - Oracle TNS Hashes (0)
  - SIP Hashes (26)

Realm	User Name	Password	URI	Nonce	Response	Method	Type	Note
asterisk	6666	6666	sip:10.11.225.125	5cb69f4c	60b06f46012e4...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	11410e18	b43f11c60d851...	REGISTER	MD5	
asterisk	6666	abc123	sip:10.11.225.125	0d2c058a	a0e351b6c736a...	REGISTER	MD5	
asterisk	6666				9c008bf0854ba...	REGISTER	MD5	
asterisk	6666				23e8361d6f39f...	REGISTER	MD5	
asterisk	6666	6666			c66eed5ac6258...	REGISTER	MD5	
asterisk	6666	6666			bcfcbdfb85d8a...	REGISTER	MD5	
asterisk	6666	6666			2abb6d11bba8...	REGISTER	MD5	
asterisk	6666	6666			a8e292e7c3084...	REGISTER	MD5	
asterisk	6666	6666			ed2923d10079...	REGISTER	MD5	
asterisk	6666	6666			d49febde8c04a...	REGISTER	MD5	
asterisk	6666	6666			e50a5d6a7e04c...	REGISTER	MD5	
asterisk	6666	6666			a29f5dbd66ce1...	REGISTER	MD5	
asterisk	6666	6666			6c31056c0a254...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	436ae202	35ca4e899554f...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	0f0d73cd	3c63c477aa887...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	77046c75	67ec3c9d57ea1...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	02467583	cd0b940c67e9...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	061c4d00	34d379ae284a2...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	6491a139	1f1beac97e888...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	4142c59d	536264d753e78...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	22ffdfe7	76701b0171b4...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	7af95f56	5dbe5197ba4b...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	52e61368	450de66414131...	REGISTER	MD5	
asterisk	6666	6666	sip:10.11.225.125	76a6a617	aafc9953c5f59...	REGISTER	MD5	

Dictionary Attack
Brute-Force Attack
Select All
Note
Test password
Remove Delete
Remove All

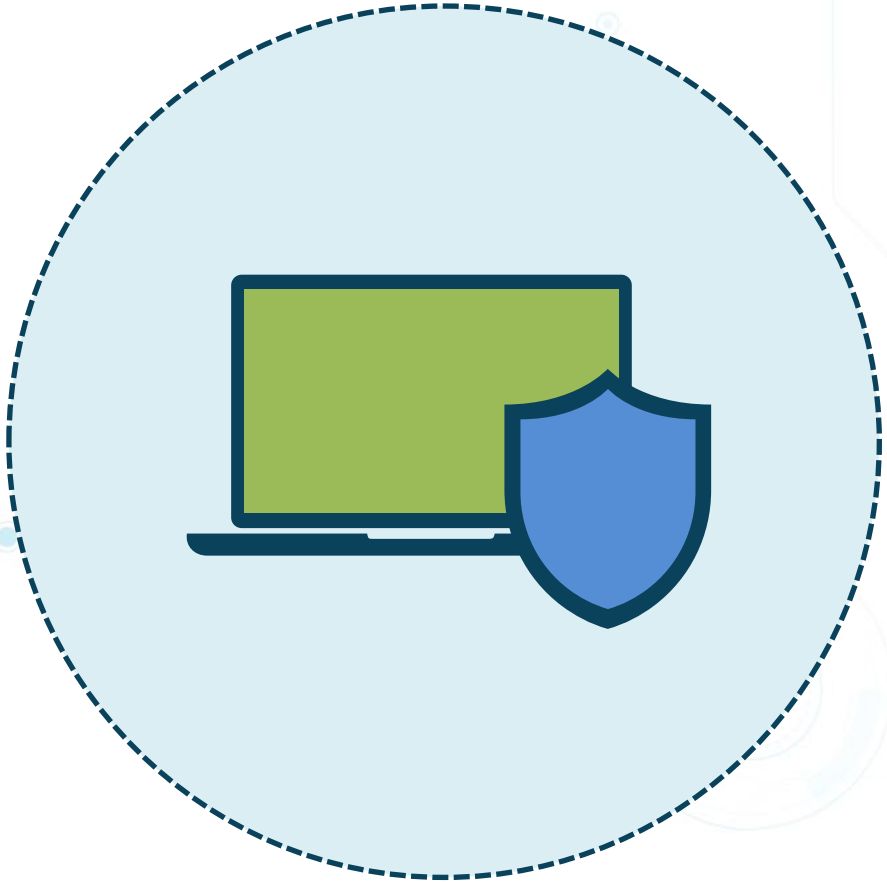
SIP Hashes

http://www.oxid.it

John the Ripper

- Free and open source
- Predominantly distributed in source code form
- John the Ripper Pro is distributed primarily in the form of "native" packages for various target operating systems
- Kali Linux has a command line version called "John" and a graphical version called "John the Ripper"

Reconfiguring Endpoint Security Solutions

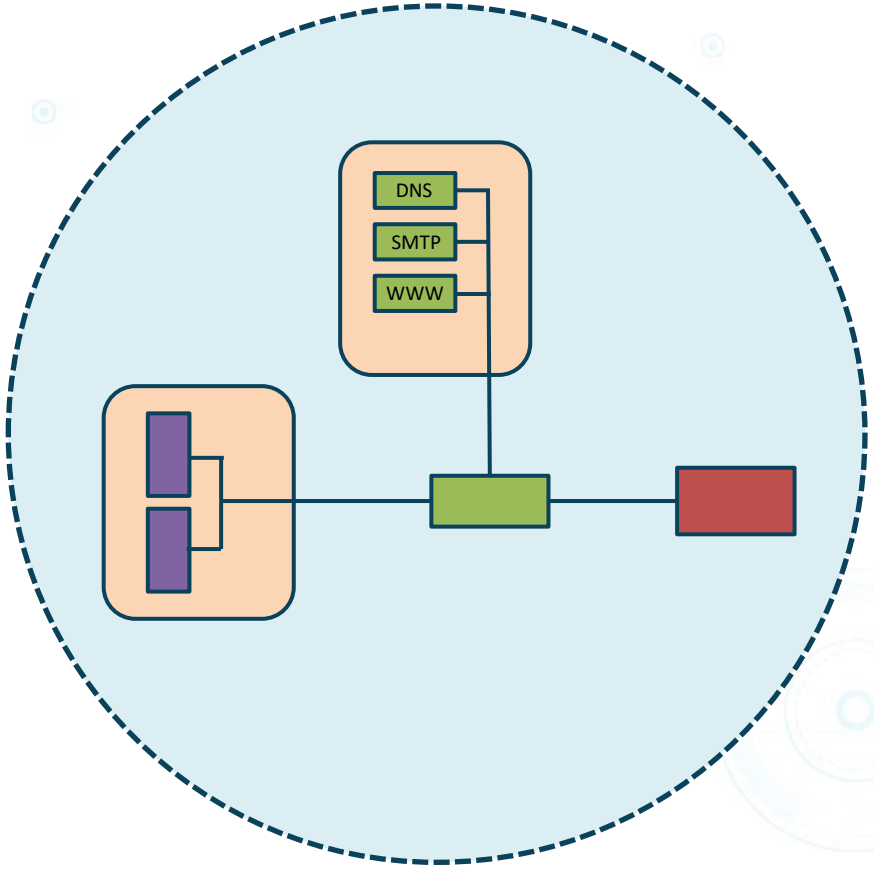


- Application whitelisting
- Application blacklisting
- Quarantine and remediation

Configuration Changes for Mitigation

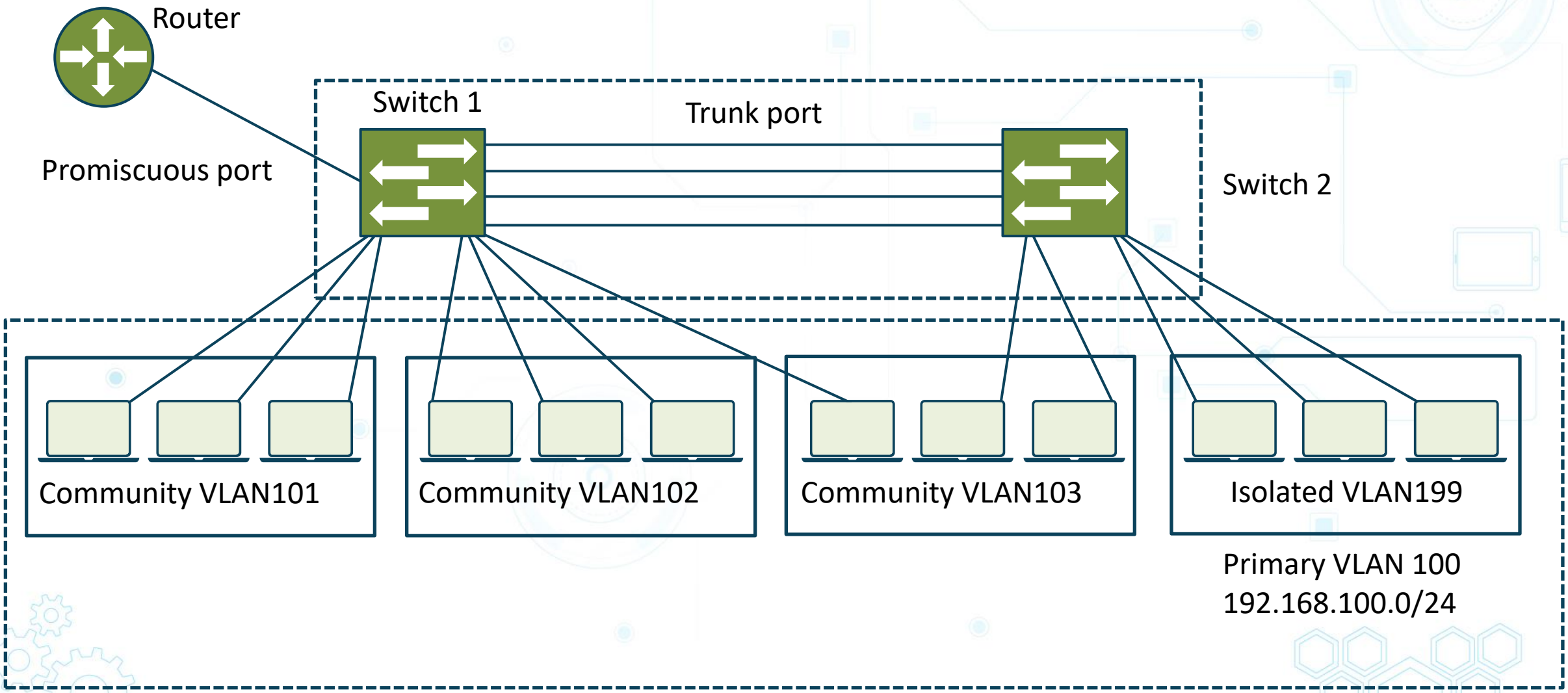
- Firewall rules and WAF WebACLs
- Mobile device management (MDM)
- URL and content filtering
- Data loss prevention (DLP)
- Revoking and updating certificates

Isolation, Containment, and Segmentation



- The most critical control needed to contain an intrusion and curb the spread of malware is network segmentation and software containment tools
- "Flat" network topologies with end-to-end management VLANs are particularly vulnerable

PVLANs for Segmentation and Containment



Secure Orchestration, Automation, and Response (SOAR)

- A collection of contrasting technologies that empower enterprises to collect data and alerts from various sources
- Organizations can perform threat analysis and remediation by using both systems and personnel
- It helps to describe, prioritize, and support incident response activities based on standard workflows
- The tools define response processes and threat analysis in a digital workflow format so that select machine-driven activities can be automated

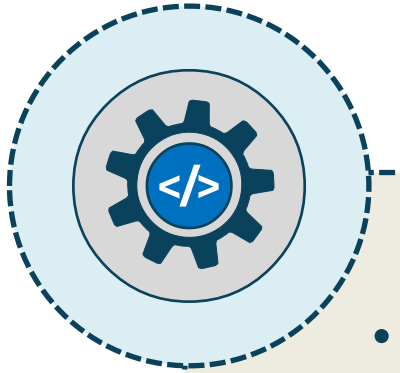
SOAR Services

- Security orchestration and automation
- Threat intelligence
- Incident response

SOAR Playbooks

- A linear checklist of necessary procedures to effectively react to certain incidents and threat occurrences
- Offer basic step-by-step and top-down IR tasks for orchestration
- Assist in developing formalized IR processes during investigations to make sure that the needed steps are systematically followed
- Support both human and automated tasks, but focus more on human intervention-like breach notification and malware reverse engineering

SOAR Runbooks

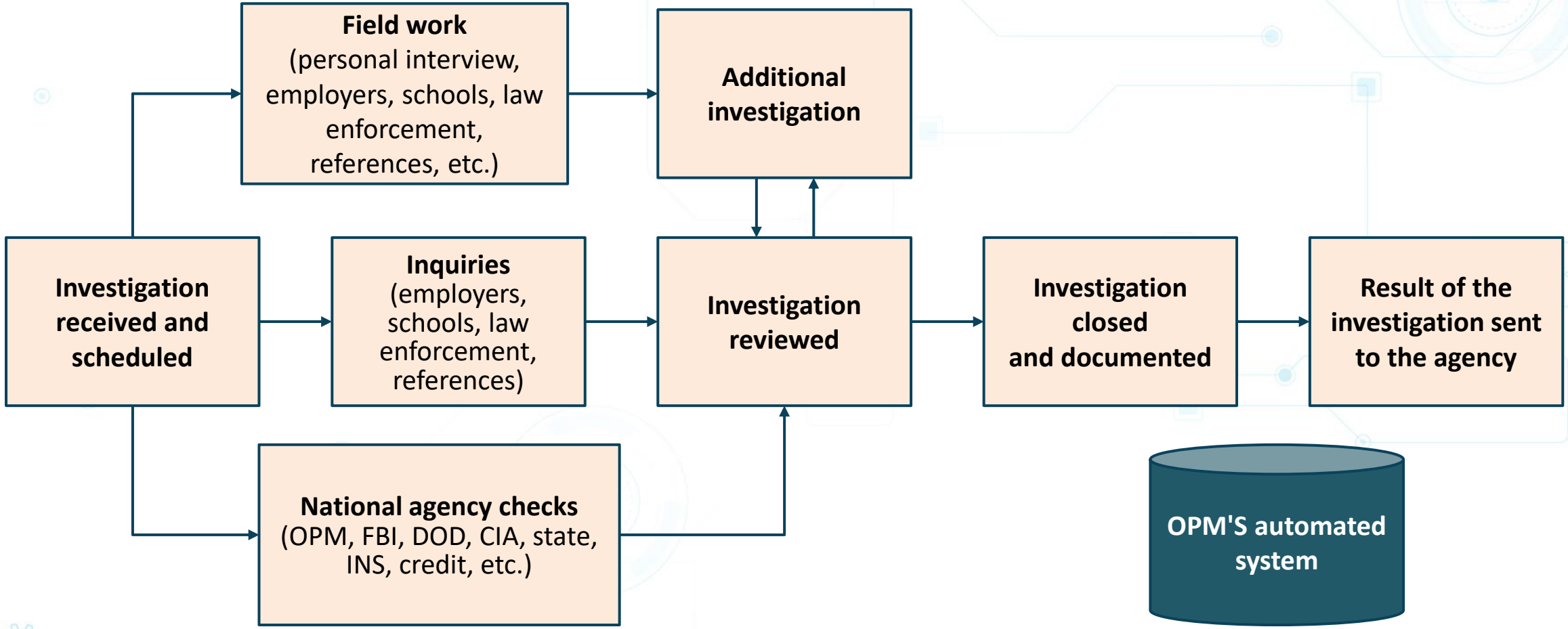


- A series of conditional steps to conduct actions as a function of incident response or security operations, such as threat containment and alert sending automatically
- Automation that assists in hastening the assessment, investigation, and containment of threats to optimize the overall incident response plan
- Although more focused on automation, they can also include human decision-making components when necessary
- Most are primarily action-based

Non-disclosure Agreements (NDAs)

- Legal contract between two or more parties
  - Confidential relationship
  - Business to business/business and employee
- Identifies confidential information they wish to share with each other
  - IP, trade secrets, technologies, campaigns, ideas, new processes, new products, and services
  - Restricts the sharing of that information with others
- Commonly used during interview process

Background Checks and Investigations



Onboarding

- Ramp up new or existing employees
- Provide assets, guidance, knowledge, skills, and behavior needed for role on team
  - Videos, printed material, CBT, lectures, formal and informal meetings, and mentors
- Deliver security awareness and AUP expectations
- Clearly define roles and responsibilities
- Remove any ambiguity and uncertainty

Automating Onboarding

- Enterprises often deploy systems that involve self-service onboarding of personal devices
- Employee registers a new device, and the native supplicant is automatically provisioned for that user and device and installed using a supplicant profile that is preconfigured to connect the device to the corporate network
- Offboarding is the reverse process

Personnel Policies

- Change management processes
- Least privilege policy
- Mandatory vacations
- Separation of duties
- Rotation of duties
- Clean desk policy
- Social media usage

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1	2	3	4	5	6
7	Vacation starts 8	9	10	11	12	13
14	15	16	Vacation ends 17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Acceptable Use Policy (AUP)

- Considered one of the most important sections of a written security policy
- Defines rules of behavior/code of conduct
  - Language
  - Avoid illegal activities
  - Avoid disturbing or disrupting other systems
  - Do not reveal personal information
  - Do not reveal confidential information
- Identifies how employees are expected to use resources in the organization

Acceptable Use Policy (AUP)

- Computer equipment
- Mobile device usage
- Software
- Operating systems
- Removable storage media
- Email and webmail
- Web browsing

Acceptable Use Policy (AUP)

- FTP/file sharing
- Remote access
- Personal cloud storage
- Telephony usage
- Wireless LAN
- Social media usage
- Cloud computing

Standard Operating Procedures (SOP)

- Step-by-step instructions that define how workers carry out routine tasks
- Can greatly improve
  - efficiency
  - quality
  - performance
  - communication, and
  - compliance with regulations

SOP Considerations

- Describe purpose and limits of procedures
- Offer all the steps needed to complete the process
- Clarify concepts and terminology
- Consider health and safety issues
- List the location of all necessary supplemental resources

Security Awareness Training

- Should happen early and often
  - CBT and streaming webinars
  - Email bulletin reminders
  - Classroom sessions
  - Phishing campaigns
  - Gamification of training
    - Capture the flag exercises
  - Self-enabled interactive websites
  - Posters, coffee mugs, and mouse pads

Security Awareness Training

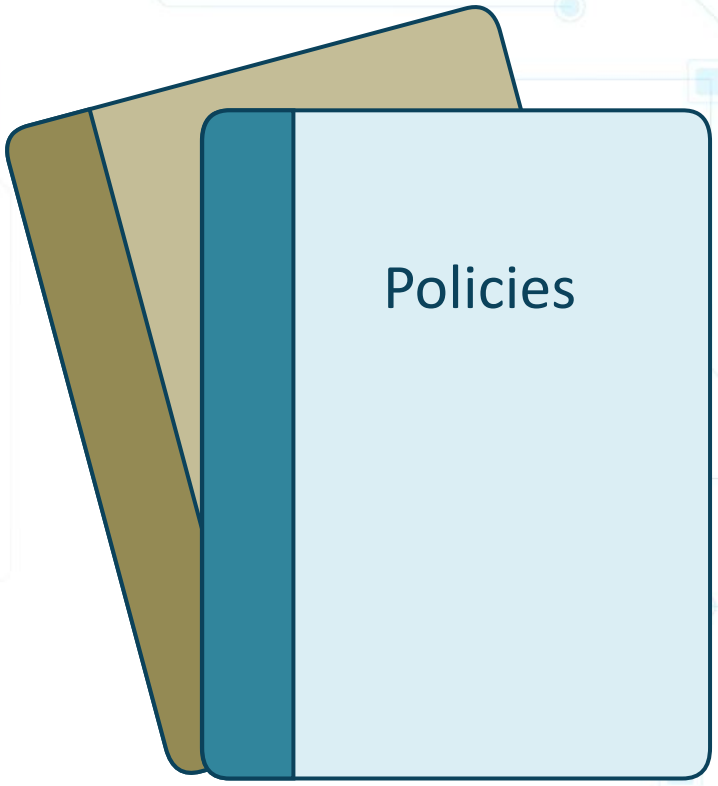
- Organization mission, charter, and vision
- All applicable policies and procedures
- Example security topics:
  - Password and badge policy (MFA)
  - Tailgating/piggybacking
  - Social engineering and phishing awareness
  - Data loss prevention
  - Governance and regulations

Role-based Security Training

- General endpoint users
- Data/system owners
- Data/system custodians and stewards
  - Custodians = technical
  - Stewards = business
- Administrators
- Privileged users
- Executive users
  - Executive management
  - C-suite or C-team
  - Board of directors

Employee Release and Exit Interviews

- Identify factors that led to employee leaving
  - How can the organization improve to keep employees if applicable?
- Remind exiting employee of their agreements and responsibilities
  - Review the NDA that they signed when they started
  - Remind them of what they are forbidden to discuss with others
- Adhere to well-defined offboarding security policies and procedures
  - Collect all corporate assets and property



Third-party Risk Management

- BPA - business partners agreement
  - Agreement between partners for business purposes
  - Purpose of business
  - Contributions of each partner
  - Rights/responsibilities of each partner
- SLA - service level agreement
  - Official commitment between provider and consumer
  - Defines quality, availability levels, responsibilities, support, and conflict resolution
- OLA - organizational level agreement
  - The internal version of SLA

Third-party Risk Management

- ISA - interconnection security agreement
  - Documents and formalizes the connections between two organizations
  - Defines security and safeguards for the connections
    - Examples: AWS Direct Connect and Azure ExpressRoute
- MOU/A - memorandum of understanding or agreement
  - Defines pre-agreement parameters and commitments between two parties
  - Generally non-binding declaration of intent or responsibilities of each party

Measurement Systems Analysis (MSA)

- Mathematical technique for deciphering the degree of deviation that occurs when using a measurement process
- Differences in measurement processes and gathering metrics can directly contribute to overall methodology inconsistency
- Often used to endorse a measurement system by evaluating correctness, precision, and strength

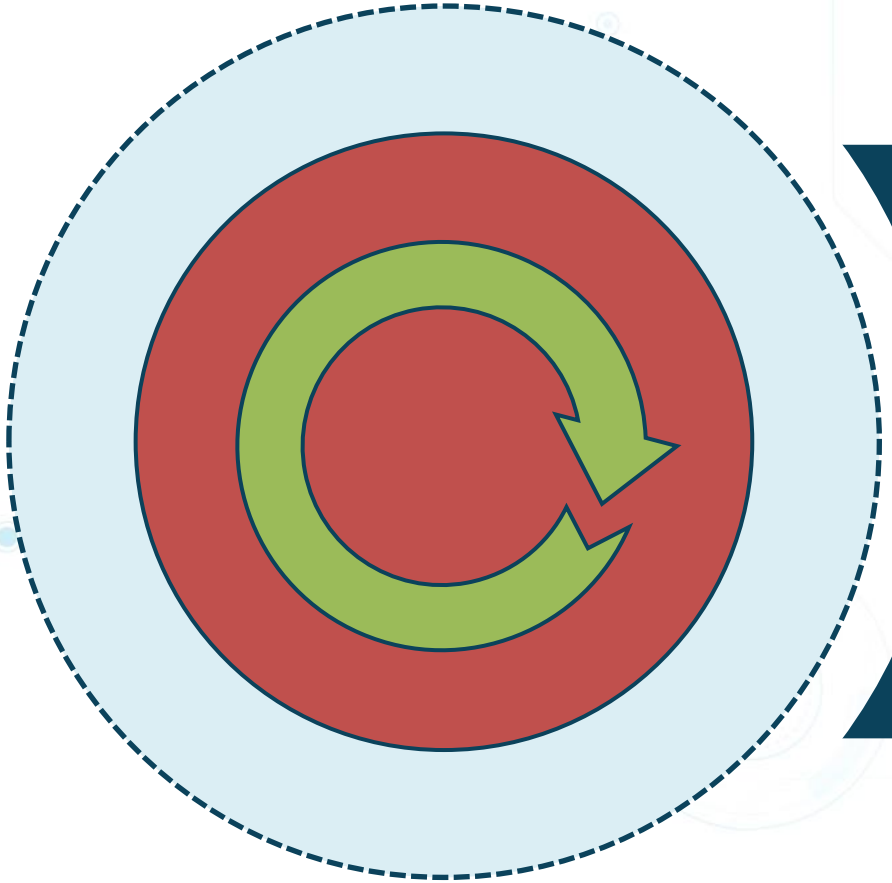
Third-party Risk Factors

- Vendors and supplier reliability
- Supply chain quality and security
- Business partner privacy vulnerability
- End-of-life (EOL) products and services
- End-of-service (EOS) posture

Labeling and Classification

- Labeling is also called "sensitivity levels"
- Used for classification of data, information, and logical/physical assets
  - Can involve physical asset tagging and inventory systems
  - Virtual tags are case-sensitive key-value pairs stored in configuration management document/NoSQL databases
- Assists in determining priority and protections based on risk tolerance
  - Avoidance, acceptance, transference, and mitigation

Attributes for Labeling



- Monetary value
- Age
- Utility
- Personal association (PII/PHI)

Classification Schemes

Military/government

- Top secret
- Secret
- Secret But Unclassified (SBU)
- Confidential
- Unclassified

Commercial

- Corporate confidential
- Personal confidential
- Trade secret/proprietary
- Private
- Public

Handling

- Controls who has access to information and assets
- Can be based on several factors, such as
  - labeling and classification
  - sensitivity levels, and
  - risk treatment (appetite)

Data Roles

Owner

Steward

C-suite

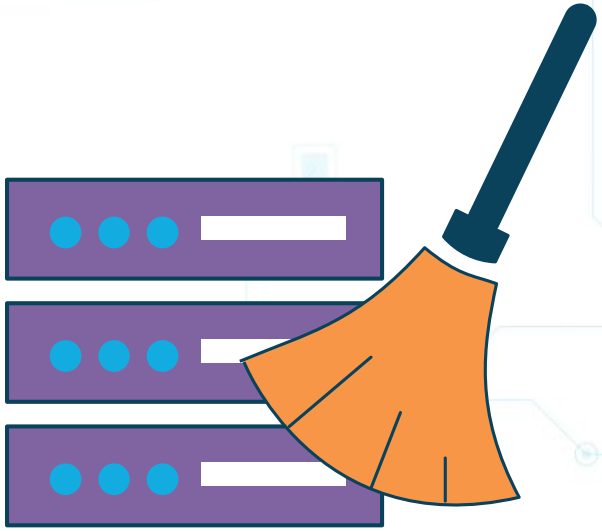
Custodian

Data Retention

- Keeping data until it is no longer needed
  - What does "no longer needed" mean?
- Data retention policies identify how, where, and why data will be retained for the following:
  - Operational use - current and future use
  - Adherence to legal and regulatory requirements and compliance
  - Periodic audits

Data Retention

- Destruction
  - Burning
  - Shredding
  - Pulverizing
  - Pulping
- Sanitization
  - Degaussing - removing the magnetic field of drive
  - Purging - clearing everything off the media
  - Wiping - overwrite every sector of drive with 1s and 0s
  - Encryption - encrypt all files before deletion or disposal of media



User Accounts

- Must be unique per person and not shared
- Often use DAC security model
- Admins should have a separate non-privileged account for normal daily activities
- Best when they are centrally managed
- Least privilege security principles
- MFA is preferable to simple password credentials
- Employ lockout for 3-5 failed attempts
- SSO should be an enterprise goal

Shared Accounts

- Anonymous or guest accounts
- Temporary employee accounts
- Shared administrative accounts
- Batch or script running accounts

Privileged Accounts

- Accounts with elevated access to systems with special credentials
- Typically give non-restricted or at least elevated access to the system, service, or applications
- Designed for systems administrators to deploy and manage IT infrastructure devices, operating systems, databases, applications, and more
- Considered the "keys to the kingdom" and are the prime target in the escalation of the privilege stage of the kill chain

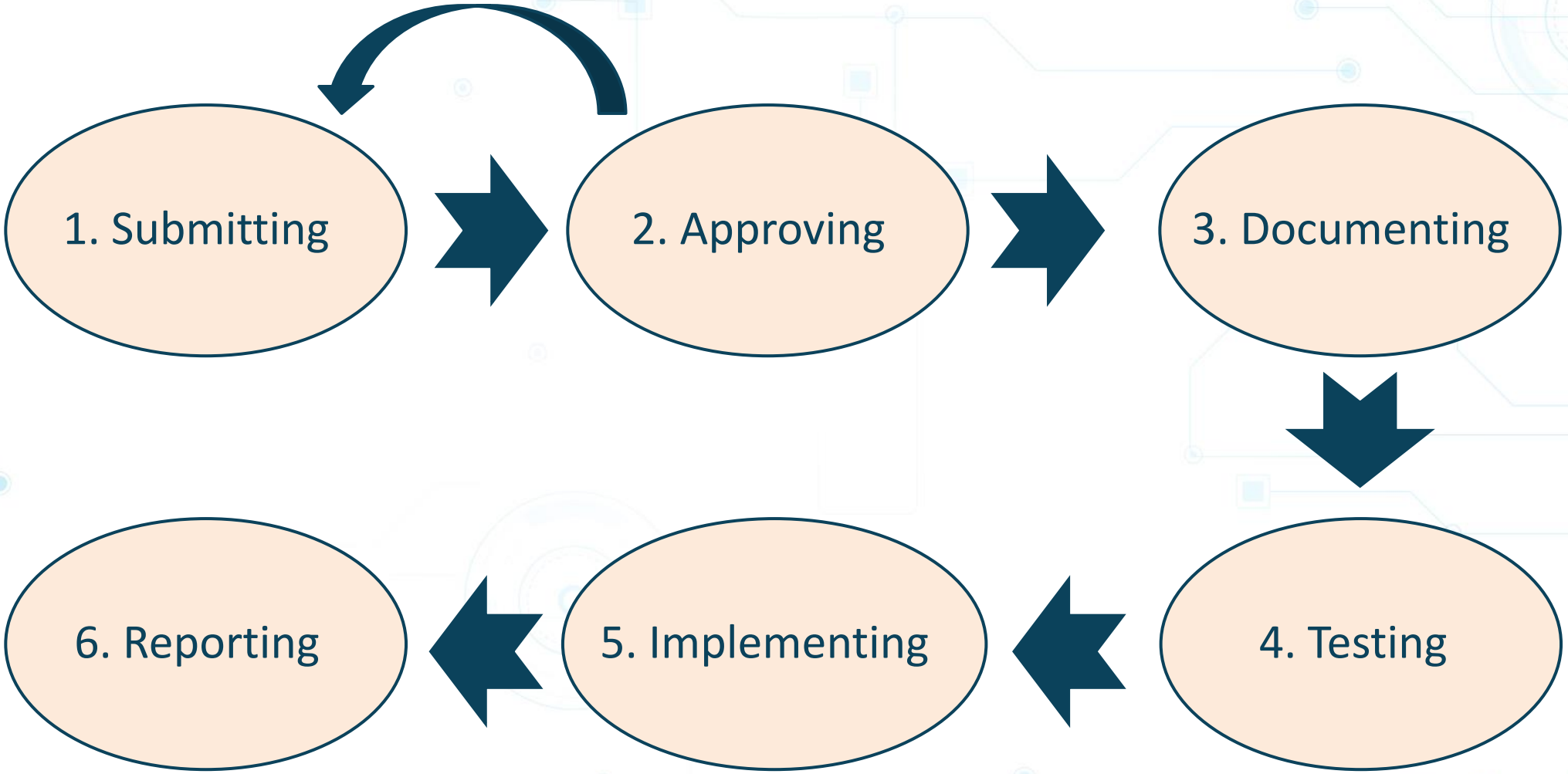
Examples of Privileged Accounts

- Root and privileged exec users
- Local administrative accounts
- Forest and domain administrative accounts
- Emergency accounts
- Application accounts

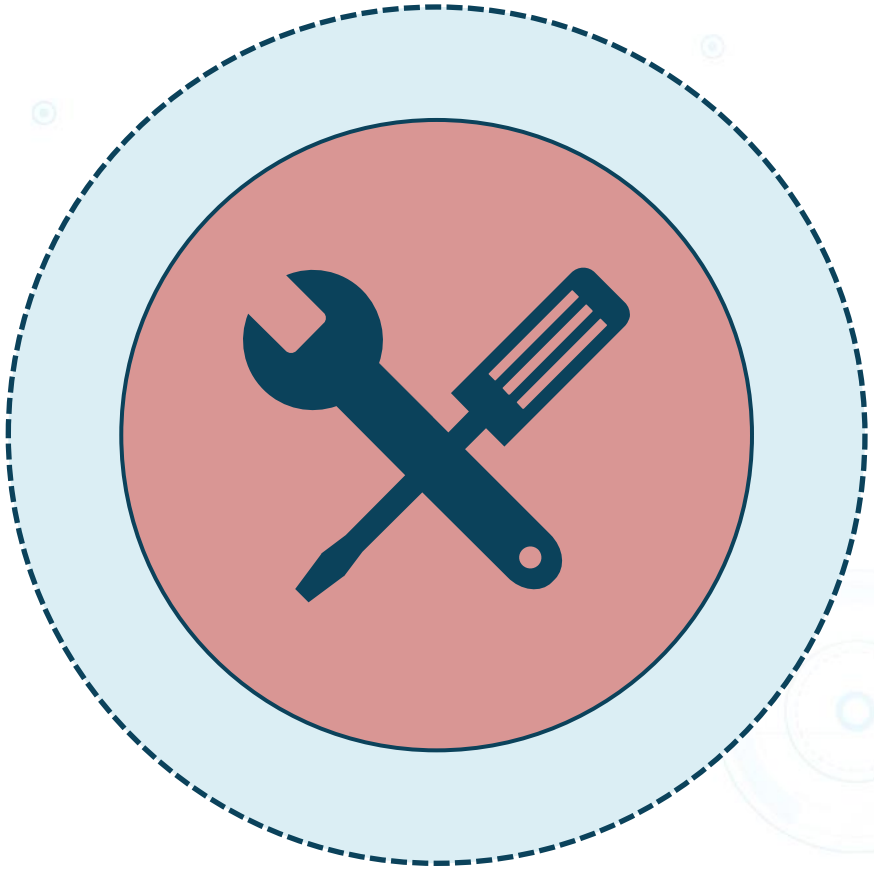
Service Accounts

- Can be privileged local or domain accounts used by an application or service to function with the network operating system
- Some have domain administrative privileges contingent on the application needs, such as corporate mail or database services
- Local service accounts can operate with several different system components, which renders coordination of password changes challenging
- Account passwords are rarely changed, and this can become a significant vulnerability for an enterprise

Change Management



Change Control



- In ITIL 4, change management is now referred to as change control
- The goal is to maximize the amount of successful service and product modifications
- Assuring proper risk assessment, change authorization, and scheduling

Types of Changes

- **Standard** changes are low-risk, pre-authorized and well-documented - often service requests that don't need additional authorization
- **Normal** changes follow a specific process for scheduling, assessment, and authorization - low risk, but do go through an approval process
- **Emergency** changes must be implemented immediately and may involve an advisory board

Asset Management

- Scope covers all hardware, software, network infrastructure, endpoint devices, virtualization hypervisors, and cloud resources
  - Valuation
  - Classification
  - Labeling and tagging
  - Handling
  - Disposition

Purpose of Asset Management

- Maximize value to the provider and consumer
- Control costs and meet business objectives
- Manage risk and align with access control framework
- Support the decision-making process
- Meet regulatory and contractual requirements

Regulations, Standards, and Legislation

- **Regulatory vs. non-regulatory**
  - Regulatory: HIPAA, SOX, General Data Protection Regulation (GDPR)
  - Non-regulatory: NIST, ITIL 4, ISO/IEC, COBIT5, CIS, ISACA

Regulations, Standards, and Legislation

- **Country-specific vs. international**
  - U.S: FISMA, GLBA, COBIT5, HIPAA
  - INTL: GDPR, ITIL4, ISO/IEC, AGATE, IDABC, OBASHI

Regulations, Standards, and Legislation

- Industry-specific frameworks
  - PCI-DSS for credit card companies
  - Sarbanes-Oxley (SOX) for financial services
  - HIPAA for PHI security and privacy
  - GDPR for EU privacy

Key Frameworks

- Frameworks help determine the organization's maturity level by performing gap analysis against best practices and implementing agreed risk controls
  - Center for Internet Security (CIS)
  - Common secure configurations (NIST)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type II/III
  - Cloud Security Alliance (CSA)

Benchmarks

- A technique to improve an organization's information security management by establishing a standard
- CIS Benchmarks™ are best practices to securely configure various systems and are available for more than 140 technologies
- Established using a special method constructed from an accord of global cybersecurity experts from across the globe
- CIS Benchmarks™ are security configuration guides created by government, business, industry, and academia

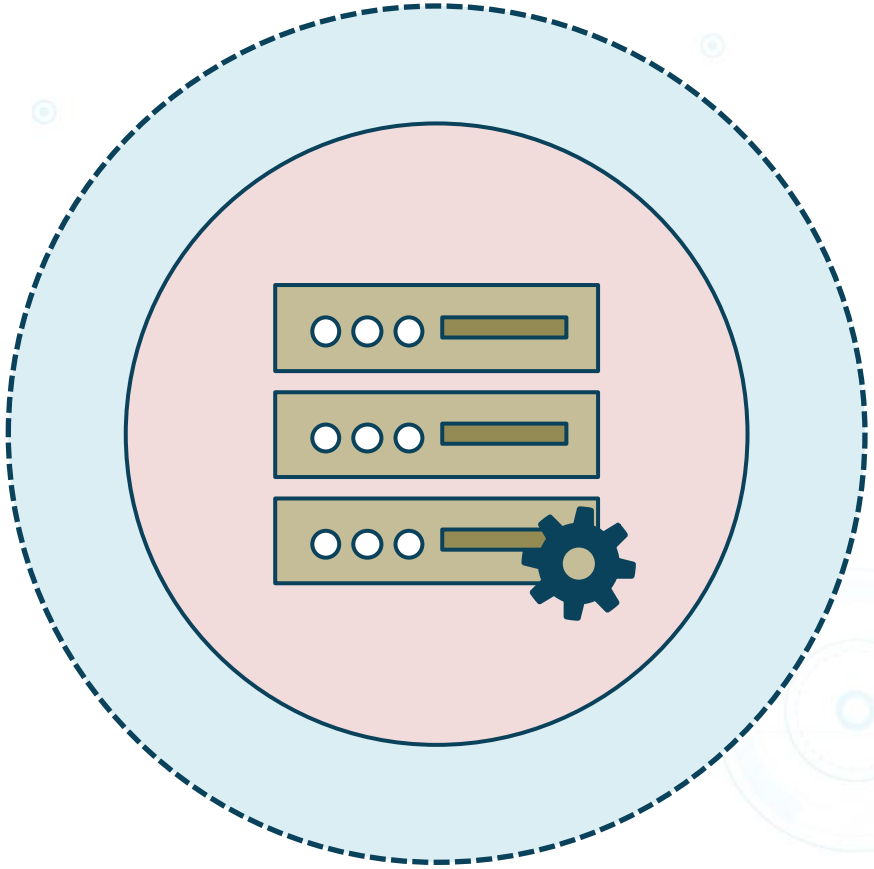
Secure Configuration Guides

- During the implementation phase of the security lifecycle, one will develop and implement security policies, procedures, standards, baselines, and configuration guidelines
- Information is like a standard, but is more flexible and usually not mandatory

Examples

- NIST 800-88 ("Guidelines for Media Sanitization") may be part of decommissioning
- CIS Benchmarks™

Specific Configuration Guides



- Web server
  - OWASP
- Operating system
  - Windows, Linux, Unix, and macOS
  - Mobile - iOS and Android
- Application servers
- Network infrastructure
  - Switches, routers, firewalls, IPS, etc.

Event Viewer

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Logs
  - Subscriptions

Security Number of events: 30,659

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/21/2020 3:09:42 PM	Microsoft Windows secu...	5379	User Account Managem...
Audit Success	8/21/2020 3:09:42 PM	Microsoft Windows secu...	5379	User Account Managem...
Audit Success	8/21/2020 3:09:41 PM	Microsoft Windows secu...	4672	Special Logon
Audit Success	8/21/2020 3:09:41 PM	Microsoft Windows secu...	4624	Logon
Audit Success	8/21/2020 3:08:08 PM	Microsoft Windows secu...	4672	Special Logon
Audit Success	8/21/2020 3:08:08 PM	Microsoft Windows secu...	4624	Logon
Audit Success	8/21/2020 3:04:42 PM	Microsoft Windows secu...	4672	Special Logon
Audit Success	8/21/2020 3:04:42 PM	Microsoft Windows secu...	4624	Logon
Audit Success	8/21/2020 3:04:28 PM	Microsoft Windows secu...	4672	Special Logon
Audit Success	8/21/2020 3:04:28 PM	Microsoft Windows secu...	4624	Logon

Event 5379, Microsoft Windows security auditing.

General Details

Credential Manager credentials were read.

Subject:
Security ID: SYSTEM
Account Name: MLSHANNON$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Read Operation: Read Credential

This event occurs when a user performs a read operation on stored credentials in Credential Manager

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/21/2020 3:09:42 PM
Event ID:	5379	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	MLSHANNON
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

Security
- Open ...
- Creat...
- Impor...
- Clear ...
- Filter ...
- Prope...
- Find...
- Save ...
- Attac...
- View
- Refresh
- Help

Event 5379...
- Event ...
- Attac...
- Copy
- Save S...
- Refresh
- Help

System Log

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Logs
  - Subscriptions

System Number of events: 16,636

Level	Date and Time	Source	Event ID	Task Category
Information	8/21/2020 3:06:49 PM	Service Control Manager	7045	None
Error	8/21/2020 2:01:50 PM	Service Control Manager	7031	None
Warning	8/21/2020 1:11:42 PM	DistributedCOM	10016	None
Warning	8/21/2020 1:11:42 PM	DistributedCOM	10016	None
Information	8/21/2020 12:00:00 PM	EventLog	6013	None
Error	8/21/2020 10:33:00 AM	Service Control Manager	7031	None
Information	8/21/2020 8:13:24 AM	Kernel-General	1	(5)
Information	8/21/2020 8:13:24 AM	Time-Service	35	None
Information	8/21/2020 8:13:09 AM	Time-Service	37	None
Information	8/21/2020 8:13:08 AM	Time-Service	158	None

Event 10016, DistributedCOM

General Details

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
and APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
to the user MLSHANNON\Owner SID (S-1-5-21-932234097-2926425998-237659251-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

Log Name:	System		
Source:	DistributedCOM	Logged:	8/21/2020 1:11:42 PM
Event ID:	10016	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	MLSHANNON\Owner	Computer:	MLSHANNON
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

System
- Open ...
- Creat...
- Impor...
- Clear ...
- Filter ...
- Prope...
- Find...
- Save ...
- Attac...
- View
- Refresh
- Help

Event 1001...
- Event ...
- Attac...
- Copy
- Save S...
- Refresh
- Help

Process Hacker

Process Hacker [MLSHANNON\Owner]+ (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

Search Processes (Ctrl+K)

Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private ...	User name	Description
clientidentifier.exe	6440			25.55 MB	NT AUTHORITY\SYSTEM	clientidentifier
conhost.exe	7000			6.58 MB	NT AUTHORITY\SYSTEM	Console Window Host
AMPWatchDog.exe	4436			2.24 MB	NT AUTHORITY\SYSTEM	AMPWatchDog
svchost.exe	4444			8.16 MB	N...\NETWORK SERVICE	Host Process for Windows Services
svchost.exe	4452			40.79 MB	NT A...\LOCAL SERVICE	Host Process for Windows Services
svchost.exe	4460			23.92 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	4476			6.03 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	4492			9.76 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
MBCloudEA.exe	4500		185 B/s	79.16 MB	NT AUTHORITY\SYSTEM	Malwarebytes Endpoint Agent
Endpoint Agent Tray.exe	10432		185 B/s	40.08 MB	MLSHANNON\Owner	Endpoint Agent Tray
KSchedulerSvc.exe	4512			10.7 MB	NT AUTHORITY\SYSTEM	AMP Offline Scheduler
svchost.exe	4528			1.61 MB	NT A...\LOCAL SERVICE	Host Process for Windows Services
nessus-service.exe	4540			728 kB	NT AUTHORITY\SYSTEM	
nessusd.exe	4776	0.02	10.44 kB/s	46.47 MB	NT AUTHORITY\SYSTEM	
vmnat.exe	4556			2.5 MB	NT AUTHORITY\SYSTEM	VMware NAT Service
vmnetdhcp.exe	4592			7.64 MB	NT AUTHORITY\SYSTEM	VMware VMnet DHCP service
svchost.exe	4600			5.98 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	4608			1.33 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
ManagementAgentNT.exe	4624			6.48 MB	NT AUTHORITY\SYSTEM	Sophos Agent
svchost.exe	4664			4.65 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	4988			3.3 MB	N...\NETWORK SERVICE	Host Process for Windows Services
svchost.exe	5220			1.3 MB	NT A...\LOCAL SERVICE	Host Process for Windows Services
vmware-authd.exe	5292	0.04	104 B/s	6.68 MB	NT AUTHORITY\SYSTEM	VMware Authorization Service
vmware-usbarbitrator64.exe	5300		4 B/s	2.98 MB	NT AUTHORITY\SYSTEM	VMware USB Arbitration Service
svchost.exe	5308			3.63 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
MBAMService.exe	5344			217.18 ...	NT AUTHORITY\SYSTEM	Malwarebytes Service
svchost.exe	5908			2.39 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	6096			3.53 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	6404			1.69 MB	N...\NETWORK SERVICE	Host Process for Windows Services
vmware-hostd.exe	7004			34.13 MB	NT AUTHORITY\SYSTEM	
svchost.exe	2368			1.54 MB	NT A...\LOCAL SERVICE	Host Process for Windows Services
svchost.exe	2932			4.47 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe						

Endpoint Agent Tray.exe (10432) Properties

General Statistics Performance Threads Token Modules

.NET performance GPU Disk and Network Comment

Memory Environment Handles .NET assemblies

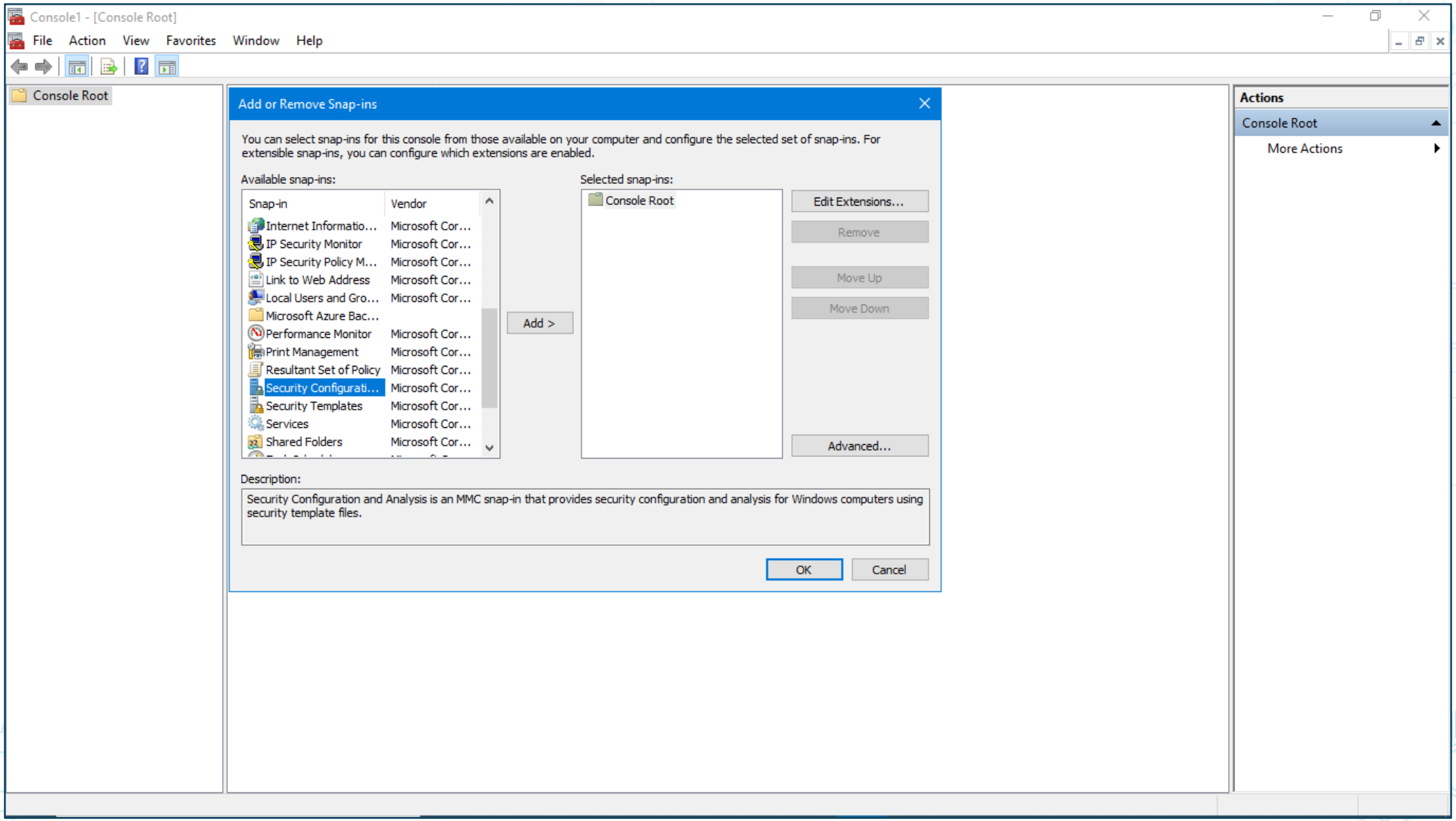
Hide free regions Strings... Refresh

Base address	Type	Size	Protect...	Use
0xa10000	Image	576 kB	WCX	C:\Program Fil
0xaa0000	Map...	64 kB	RW	Heap (ID 2)
0xab0000	Map...	32 kB	R	
0xac0000	Map...	4 kB	R	
0xad0000	Map...	108 kB	R	
0xaf0000	Private	256 kB	RW	Stack (thread
0xb30000	Map...	16 kB	R	
0xb40000	Map...	4 kB	R	
0xb50000	Private	8 kB	RW	
0xb60000	Private	256 kB	RW	Stack (thread
0xba0000	Private	256 kB	RW	Stack (thread
0xbe0000	Private	12 kB	RW	
0xbf0000	Map...	4 kB	RW	
0xc00000	Private	2,048 kB	RW	PEB
0xe00000	Private	1,024 kB	RW	Stack 32-bit (tl
0xf00000	Map...	796 kB	R	C:\Windows\S
0xfd0000	Map...	20 kB	R	C:\Windows\S
0xfe0000	Map...	64 kB	R	C:\Windows\S
0xff0000	Private	256 kB	RW	Stack 32-bit (tl
0x1030000	Private	256 kB	RW	Stack (thread
0x1070000				

Close

CPU Usage: 0.74% Physical memory: 7.34 GB (18.39%) Processes: 213

Secure Configuration Assessment (SCA)



Secure Configuration Assessment (SCA)

Console1 - [Console Root\Security Configuration and Analysis\Local Policies\User Rights Assignment]

File Action View Favorites Window Help

- Console Root
  - Security Configuration and Analysis
    - Account Policies
      - Password Policy
      - Account Lockout Policy
    - Local Policies
      - Audit Policy
      - User Rights Assignment
      - Security Options
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
  - Group Policy Management

Policy	Database Setting	Computer Setting
Access Credential Manager as a trusted caller	Not Defined	
Access this computer from the network	Not Defined	Backup Operators,Users,...
Act as part of the operating system	Not Defined	
Add workstations to domain	Not Defined	
Adjust memory quotas for a process	Not Defined	DefaultAppPool,Admini...
Allow log on locally	Not Defined	Backup Operators,Users,...
Allow log on through Remote Desktop Services	Not Defined	Remote Desktop Users,A...
Back up files and directories	Not Defined	Backup Operators,Admi...
Bypass traverse checking	Not Defined	Backup Operators,Users,...
Change the system time	Not Defined	autotimesvc,Administra...
Change the time zone	Not Defined	Users,Administrators,LO...
Create a pagefile	Not Defined	Administrators
Create a token object	Not Defined	
Create global objects	Not Defined	SERVICE,Administrators,...
Create permanent shared objects	Not Defined	
Create symbolic links	Not Defined	Administrators
Debug programs	Not Defined	Administrators
Deny access to this computer from the network	Not Defined	MLSHANNON\Guest
Deny log on as a batch job	Not Defined	
Deny log on as a service	Not Defined	
Deny log on locally	Not Defined	MLSHANNON\Guest,M...
Deny log on through Remote Desktop Services	Not Defined	
Enable computer and user accounts to be trusted for delega...	Not Defined	
Force shutdown from a remote system	Not Defined	Administrators
Generate security audits	Not Defined	DefaultAppPool,NETWO...
Impersonate a client after authentication	Not Defined	SERVICE,IIS_IUSRS,Admi...
Increase a process working set	Not Defined	Users
Increase scheduling priority	Not Defined	Window Manager Grou...
Load and unload device drivers	Not Defined	Administrators
Lock pages in memory	Not Defined	MLSHANNON\Owner
Log on as a batch job	Not Defined	IIS_IUSRS,Performance L...
Log on as a service	Not Defined	DefaultAppPool,autotim...
Manage auditing and security log	Not Defined	Administrators
Modify an object label	Not Defined	

Actions

User Rights Assignment

More Actions

Automate Monitoring with PowerShell

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Script

```
PS C:\Users\Owner> Get-Command -Module NetSecurity

CommandType     Name                                       Version    Source
-----------     ----                                       -------    ------
Function        Copy-NetFirewallRule                       2.0.0.0    NetSecurity
Function        Copy-NetIPsecMainModeCryptoSet             2.0.0.0    NetSecurity
Function        Copy-NetIPsecMainModeRule                  2.0.0.0    NetSecurity
Function        Copy-NetIPsecPhase1AuthSet                 2.0.0.0    NetSecurity
Function        Copy-NetIPsecPhase2AuthSet                 2.0.0.0    NetSecurity
Function        Copy-NetIPsecQuickModeCryptoSet            2.0.0.0    NetSecurity
Function        Copy-NetIPsecRule                          2.0.0.0    NetSecurity
Function        Disable-NetFirewallRule                    2.0.0.0    NetSecurity
Function        Disable-NetIPsecMainModeRule               2.0.0.0    NetSecurity
Function        Disable-NetIPsecRule                       2.0.0.0    NetSecurity
Function        Enable-NetFirewallRule                     2.0.0.0    NetSecurity
Function        Enable-NetIPsecMainModeRule                2.0.0.0    NetSecurity
Function        Enable-NetIPsecRule                        2.0.0.0    NetSecurity
Function        Find-NetIPsecRule                          2.0.0.0    NetSecurity
Function        Get-NetFirewallAddressFilter               2.0.0.0    NetSecurity
Function        Get-NetFirewallApplicationFilter           2.0.0.0    NetSecurity
Function        Get-NetFirewallInterfaceFilter             2.0.0.0    NetSecurity
Function        Get-NetFirewallInterfaceTypeFilter         2.0.0.0    NetSecurity
Function        Get-NetFirewallPortFilter                  2.0.0.0    NetSecurity
Function        Get-NetFirewallProfile                     2.0.0.0    NetSecurity
Function        Get-NetFirewallRule                        2.0.0.0    NetSecurity
Function        Get-NetFirewallSecurityFilter              2.0.0.0    NetSecurity
Function        Get-NetFirewallServiceFilter               2.0.0.0    NetSecurity
Function        Get-NetFirewallSetting                     2.0.0.0    NetSecurity
Function        Get-NetIPsecDospSetting                    2.0.0.0    NetSecurity
Function        Get-NetIPsecMainModeCryptoSet              2.0.0.0    NetSecurity
Function        Get-NetIPsecMainModeRule                   2.0.0.0    NetSecurity
Function        Get-NetIPsecMainModeSA                     2.0.0.0    NetSecurity
Function        Get-NetIPsecPhase1AuthSet                  2.0.0.0    NetSecurity
Function        Get-NetIPsecPhase2AuthSet                  2.0.0.0    NetSecurity
Function        Get-NetIPsecQuickModeCryptoSet             2.0.0.0    NetSecurity
Function        Get-NetIPsecQuickModeSA                    2.0.0.0    NetSecurity
Function        Get-NetIPsecRule                           2.0.0.0    NetSecurity
Function        New-NetFirewallRule                        2.0.0.0    NetSecurity
Function        New-NetIPsecDospSetting                    2.0.0.0    NetSecurity
Function        New-NetIPsecMainModeCryptoSet              2.0.0.0    NetSecurity
Function        New-NetIPsecMainModeRule                   2.0.0.0    NetSecurity
Function        New-NetIPsecPhase1AuthSet                  2.0.0.0    NetSecurity
Function        New-NetIPsecPhase2AuthSet                  2.0.0.0    NetSecurity
Function        New-NetIPsecQuickModeCryptoSet             2.0.0.0    NetSecurity
Function        New-NetIPsecRule                           2.0.0.0    NetSecurity
Function        Open-NetGPO                                2.0.0.0    NetSecurity
Function        Remove-NetFirewallRule                     2.0.0.0    NetSecurity
```

Commands

Modules: GroupPolicy Refresh

Name:

- Backup-GPO
- Block-GPInheritance
- Copy-GPO
- Get-GPInheritance
- Get-GPO
- Get-GPOReport
- Get-GPPermission
- Get-GPPrefRegistryValue
- Get-GPRegistryValue
- Get-GPResultantSetOfPolicy
- Get-GPStarterGPO
- Import-GPO
- Invoke-GPUpdate
- New-GPLink
- New-GPO
- New-GPStarterGPO
- Remove-GPLink
- Remove-GPO
- Remove-GPPrefRegistryValue
- Remove-GPRegistryValue
- Rename-GPO
- Restore-GPO
- Set-GPInheritance
- Set-GPLink
- Set-GPPermission
- Set-GPPrefRegistryValue
- Set-GPRegistryValue

Run Insert Copy

Completed Ln 1 Col 1 100%

Linux Logging Utilities

- syslog-ng
  - A newer replacement for syslog in many builds
  - Takes log messages from various sources and forwards them to destinations using powerful filter directives
- syslogd
  - Reads and logs messages to the system console, log files, other machines and/or users as designated by a configuration file
- logrotate
  - Offers automatic rotation, compression, disposal, and emailing of log files
  - Each log file can be handled daily, weekly, monthly, or when too large

Open ▾ logrotate.conf /etc Save

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
#dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

Auditd

- Red Hat and SELinux logging for
  - command execution
  - file and directory access, and
  - network connections
- Rules are managed by the audit.rules file or the `auditctl` command
- ausearch, aureport, and autrace tools

Linux ls -l

root@kali: /etc

File Edit View Search Terminal Help

```
root@kali:/etc# ls -l
total 1548
-rw-r--r-- 1 root   root     2981 Oct 16  2018 adduser.conf
-rw-r--r-- 1 root   root       44 Oct 26  2018 adjtime
-rw-r--r-- 1 root   root      185 Oct 16  2018 aliases
drwxr-xr-x 2 root   root    20480 Oct 26  2018 alternatives
drwxr-xr-x 2 root   root     4096 Oct 26  2018 amap
-rw-r--r-- 1 root   root      401 May 29  2017 anacrontab
drwxr-xr-x 8 root   root     4096 Oct 26  2018 apache2
-rw-r--r-- 1 root   root      433 Oct  1  2017 apg.conf
drwxr-xr-x 3 root   root     4096 Oct 26  2018 apm
drwxr-xr-x 3 root   root     4096 Oct 26  2018 apparmor
drwxr-xr-x 7 root   root     4096 Oct 26  2018 apparmor.d
-rw-r--r-- 1 root   root      769 Aug  4  2018 appstream.conf
drwxr-xr-x 6 root   root     4096 Oct 26  2018 apt
drwxr-xr-x 2 root   root     4096 Oct 26  2018 arpwatch
drwxr-xr-x 3 root   root     4096 Oct 26  2018 avahi
-rw-r--r-- 1 root   root     1994 Jun 17  2018 bash.bashrc
-rw-r--r-- 1 root   root       45 Mar 18  2018 bash_completion
drwxr-xr-x 2 root   root     4096 Oct 26  2018 bash_completion.d
drwxr-xr-x 2 root   root     4096 Oct 26  2018 bdfproxy
drwxr-xr-x 2 root   root     4096 Oct 26  2018 beef-xss
-rw-r--r-- 1 root   root      367 Jan  5  2018 bindresvport.blacklist
```

netstat

```
root@kali:/etc# netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     17151    /run/NetworkManager/private-
dhcp
unix  2      [ ACC ]     STREAM     LISTENING     13827    /var/run/pcscd/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     13831    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     13835    /var/run/dbus/system_bus_soc
ket
unix  2      [ ACC ]     STREAM     LISTENING     17432    /run/user/133/systemd/privat
e
unix  2      [ ACC ]     STREAM     LISTENING     22435    @/tmp/.ICE-unix/1129
unix  2      [ ACC ]     STREAM     LISTENING     17439    /run/user/133/gnupg/S.dirmng
r
unix  2      [ ACC ]     STREAM     LISTENING     17534    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     17442    /run/user/133/gnupg/S.gpg-ag
ent
```

ps -ef

```
root@kali:/etc# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 17:01 ?        00:00:01 /sbin/init
root         2     0  0 17:01 ?        00:00:00 [kthreadd]
root         3     2  0 17:01 ?        00:00:00 [rcu_gp]
root         4     2  0 17:01 ?        00:00:00 [rcu_par_gp]
root         5     2  0 17:01 ?        00:00:00 [kworker/0:0-mpt_poll_0]
root         6     2  0 17:01 ?        00:00:00 [kworker/0:0H-kblockd]
root         8     2  0 17:01 ?        00:00:00 [mm_percpu_wq]
root         9     2  0 17:01 ?        00:00:00 [ksoftirqd/0]
root        10     2  0 17:01 ?        00:00:00 [rcu_sched]
root        11     2  0 17:01 ?        00:00:00 [rcu_bh]
root        12     2  0 17:01 ?        00:00:00 [migration/0]
root        13     2  0 17:01 ?        00:00:00 [watchdog/0]
root        14     2  0 17:01 ?        00:00:00 [cpuhp/0]
root        15     2  0 17:01 ?        00:00:00 [cpuhp/1]
root        16     2  0 17:01 ?        00:00:00 [watchdog/1]
root        17     2  0 17:01 ?        00:00:00 [migration/1]
root        18     2  0 17:01 ?        00:00:00 [ksoftirqd/1]
root        20     2  0 17:01 ?        00:00:00 [kworker/1:0H-kblockd]
root        21     2  0 17:01 ?        00:00:00 [kdevtmpfs]
root        22     2  0 17:01 ?        00:00:00 [netns]
root        23     2  0 17:01 ?        00:00:00 [kauditd]
```

top

```
top - 17:29:13 up 27 min,  1 user,  load average: 0.00, 0.02, 0.05
Tasks: 173 total,   2 running, 171 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   1991.6 total,    406.6 free,    796.1 used,    788.8 buff/cache
MiB Swap:   2045.0 total,   2045.0 free,      0.0 used.    999.9 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    1 root      20   0  124632   8716   6676 S   0.0   0.4   0:01.96 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    5 root      20   0       0      0      0 I   0.0   0.0   0:00.46 kworker/0:0-even+
    6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-kbl+
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
    9 root      20   0       0      0      0 S   0.0   0.0   0:00.05 ksoftirqd/0
   10 root      20   0       0      0      0 R   0.0   0.0   0:00.39 rcu_sched
   11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_bh
   12 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
   13 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 watchdog/0
   14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
   16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 watchdog/1
   17 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/1
   18 root      20   0       0      0      0 S   0.0   0.0   0:00.05 ksoftirqd/1
   20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-kbl+
```

Protocol Analyzer Output

slammer.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	213.76.212.22	65.165.167.86	DCERPC	418	Ping: seq: 16843009

```
> Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits)
v Ethernet II, Src: Cisco_55:46:2c (00:00:0c:55:46:2c), Dst: Megahert_55:98
  > Destination: Megahert_55:98:1e (00:00:86:55:98:1e)
  > Source: Cisco_55:46:2c (00:00:0c:55:46:2c)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 213.76.212.22, Dst: 65.165.167.86
v User Datagram Protocol, Src Port: 20199, Dst Port: 1434
    Source Port: 20199
    Destination Port: 1434
    Length: 384
    Checksum: 0x5405 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Ping,
```

```
0020  a7 56 4e e7 05 9a 01 80  54 05 04 01 01 01 01 01   ·VN····· T·......
0030  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0040  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0050  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0060  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0070  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0080  01 01 01 01 01 01 01 01  01 01 01 dc c9 b0 42 eb   ........ ......B·
0090  0e 01 01 01 01 01 01 01  70 ae 42 01 70 ae 42 90   ........ p·B·p·B·
00a0  90 90 90 90 90 90 90 68  dc c9 b0 42 b8 01 01 01   .......h ···B····
00b0  01 31 c9 b1 18 50 e2 fd  35 01 01 01 05 50 89 e5   ·1···P·· 5····P··
00c0  51 68 2e 64 6c 6c 68 65  6c 33 32 68 6b 65 72 6e   Qh.dllhe l32hkern
00d0  51 68 6f 75 6e 74 68 69  63 6b 43 68 47 65 74 54   Qhounthi ckChGetT
00e0  66 b9 6c 6c 51 68 33 32  2e 64 68 77 73 32 5f 66   f·llQh32 .dhws2_f
00f0  b9 65 74 51 68 73 6f 63  6b 66 b9 74 6f 51 68 73   ·etQhsoc kf·toQhs
```

Wireshark · Follow UDP Stream (udp.stream eq 0) · slammer.pcap

```
.......................................................................
.................B........p.B.p.B.......h...B.....1...P..
5....P..Qh.dllhel32hkernQhounthickChGetTf.llQh32.dhws2_f.etQhsockf.toQhsend....B.
E.P..P.E.P.E.P..P....B....=U..Qt.....B....
1.QQP...........Q.E.P.E.P..j.j.j...P.E.P.E.P....
...<a...E...@...........).......E.j..E.P1.Qf..x.Q.E.P.E.P....
```

1 client pkt, 0 server pkts, 0 turns.

Entire conversation (376 bytes) | Show and save data as ASCII | Stream 0

Protocol Analyzer Output

teardrop.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

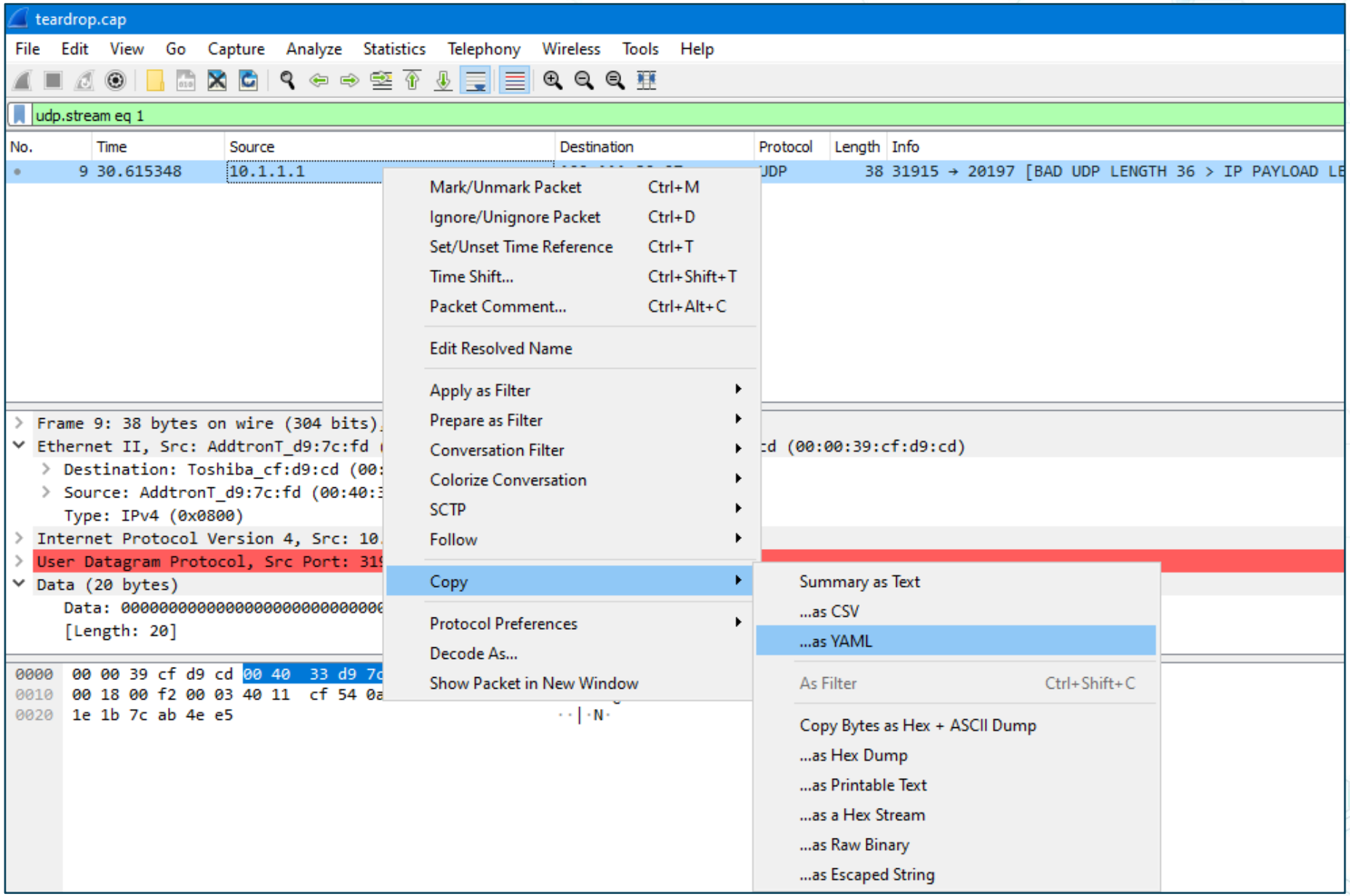
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
5	30.069467	Cisco_7c:eb:3d	CDP/VTP/DTP/PAgP/UD…	CDP	333	Device ID: gramirez-isdn.tivoli.com Port ID: Ethernet0
6	30.292923	10.0.0.6	151.164.1.8	DNS	78	Standard query 0x7d9e A picard.uthscsa.edu
7	30.612811	151.164.1.8	10.0.0.6	DNS	289	Standard query response 0x7d9e A picard.uthscsa.edu A 129.111
• 8	30.614993	10.1.1.1	129.111.30.27	IPv4	70	Fragmented IP protocol (proto=UDP 17, off=0, ID=00f2) [Reasse
• 9	30.615348	10.1.1.1	129.111.30.27	UDP	38	31915 → 20197 [BAD UDP LENGTH 36 > IP PAYLOAD LENGTH] Len=28
10	35.285494	AddtronT_d9:7c:fd	Toshiba_cf:d9:cd	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
11	36.285487	AddtronT_d9:7c:fd	Toshiba_cf:d9:cd	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
12	37.285485	AddtronT_d9:7c:fd	Toshiba_cf:d9:cd	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
13	38.285500	AddtronT_d9:7c:fd	Broadcast	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
14	38.287366	Toshiba_cf:d9:cd	AddtronT_d9:7c:fd	ARP	60	10.0.0.254 is at 00:00:39:cf:d9:cd
15	40.061851	Cisco_7c:eb:3d	Cisco_7c:eb:3d	LOOP	60	Reply

```
> Frame 9: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)
v Ethernet II, Src: AddtronT_d9:7c:fd (00:40:33:d9:7c:fd), Dst: Toshiba_cf:d9:cd (00:00:39:cf:d9:cd)
  > Destination: Toshiba_cf:d9:cd (00:00:39:cf:d9:cd)
  > Source: AddtronT_d9:7c:fd (00:40:33:d9:7c:fd)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.1.1.1, Dst: 129.111.30.27
> User Datagram Protocol, Src Port: 31915, Dst Port: 20197
v Data (20 bytes)
    Data: 0000000000000000000000000000000000000000
    [Length: 20]
```

```
0000  00 00 39 cf d9 cd 00 40  33 d9 7c fd 08 00 45 00   ··9····@ 3·|···E·
0010  00 18 00 f2 00 03 40 11  cf 54 0a 01 01 01 81 6f   ····· @· ·T·····o
0020  1e 1b 7c ab 4e e5                                  ··|·N·
```

Protocol Analyzer Output



Cloud Computing Logging and Reporting

- Amazon Web Services has many managed services that can be used on cloud resources as well as on your on-premises infrastructure
- All CSP tools and services provide for enhanced automation, orchestration, and notification through a variety of channels

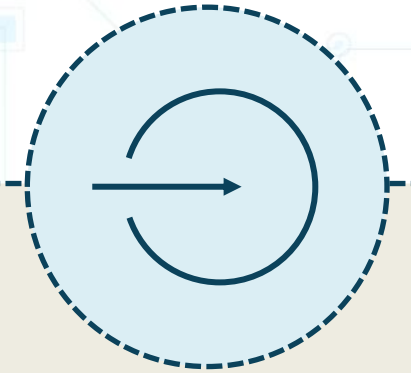
Cloud Computing Logging and Reporting

- CloudWatch and CloudTrail
- VPC Flow Logs
- AWS Config
- Systems Manager
- GuardDuty

Log Aggregation and Correlation

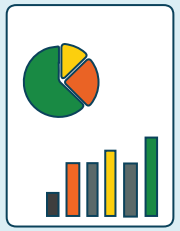
- Gather logs and alerts from as many sources as possible:
  - Various logs (system, security, application, firewall, sensors, and proxies)
  - Simple Network Management Protocol (SNMP) traps
  - NetFlow collection (Version 9 is preferred)
  - Next-Generation Intrusion Prevention Systems
  - Database activity monitors
  - VPN Gateway flow logs
  - Next generation syslog tools
  - Cloud-based visibility tools
  - ML and AI data analysis tools

Application Log Aggregation



- Input validation weaknesses
- Authentication attempts and failures
- Access control failures
- Tampering attempts
- Use of invalid or expired session tokens
- Exceptions raised by the OS or programs
- Use of administrative or elevated privileges
- Transport Layer Security failures
- Cryptographic errors

Visibility and Reporting Best Practices



- Collect all reports from vulnerability scans and penetration testing and visualize results for non-technical executive managers
- Reports should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)

Visibility and Reporting Best Practices

- Understand components of visual communications
  - Avoid three-dimensional representation
  - Use a palette of sequential colors
  - Avoid pie charts for scatterplots, bars and bubble charts, histograms, density plots, and boxplots

Visibility and Reporting Best Practices

- CSP tools - CloudWatch, CloudTrail, Stackdriver, Insights
- R programming and Python modules
- Automated system reports
- PDF files
- Charts and graphs
- Dashboards for visibility
- Written summaries
- After-action reports
  - Include "lessons learned" section

Lessons Learned and After-action Reports

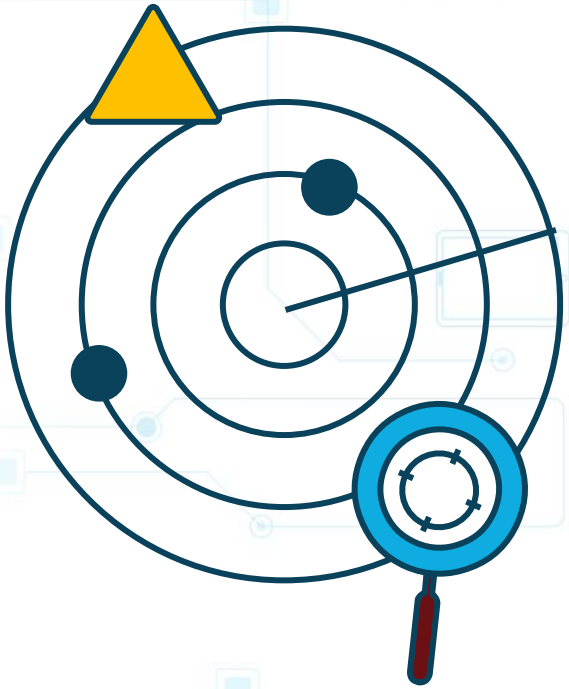
- Knowledge gained from the process of conducting the program, project, or task included in after-action report (AAR)
- Formal "lessons learned" sessions usually held at the project close-out, near the completion of the initiative
- Recognized and documented at any point during the life cycle

Lessons Learned

- The purpose of documenting lessons learned is
  - to share and use knowledge derived from an experience
  - endorse the recurrence of positive outcomes, and
  - prevent the recurrence of negative outcomes

Incident Response Reporting

- Root-cause analysis
  - Examines and determines the core reasons for any incident or failure
  - Phases: collect, record, analyze, and then recommend
- IR after-action report
  - Any type of retroactive analysis of a series of goal-oriented activities typically performed by the originators of the exercises
  - **Analytical AARs have three key goals:**
    - identifying problematic issues and areas for improvement
    - recommending measures to counteract challenges, and
    - finding "lessons learned"

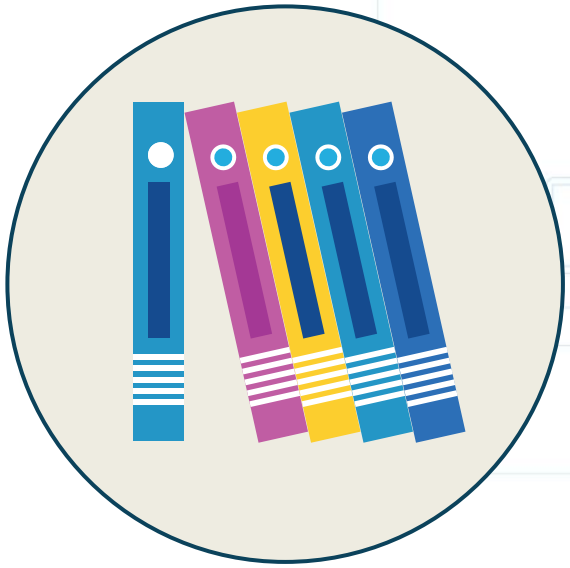


Forensic Reporting

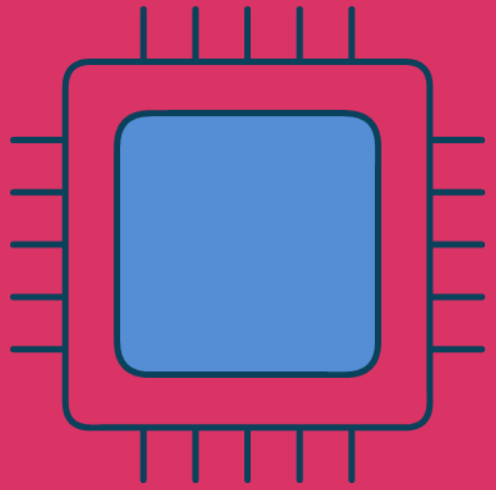
- Meet with proper authorities
  - Provide documents of all findings
  - Provide expert testimony
  - Provide any needed clarification
  - Identify overall impact on business
  - Recommend any countermeasures
- Tracking people hours and expenses
  - Who, what, when, how -
    important for court and other proceedings

After-action Report Structure

1. Overview
2. Stated objectives
3. Analysis of results
4. Analysis of the critical task performance
5. Summary
6. Recommendations

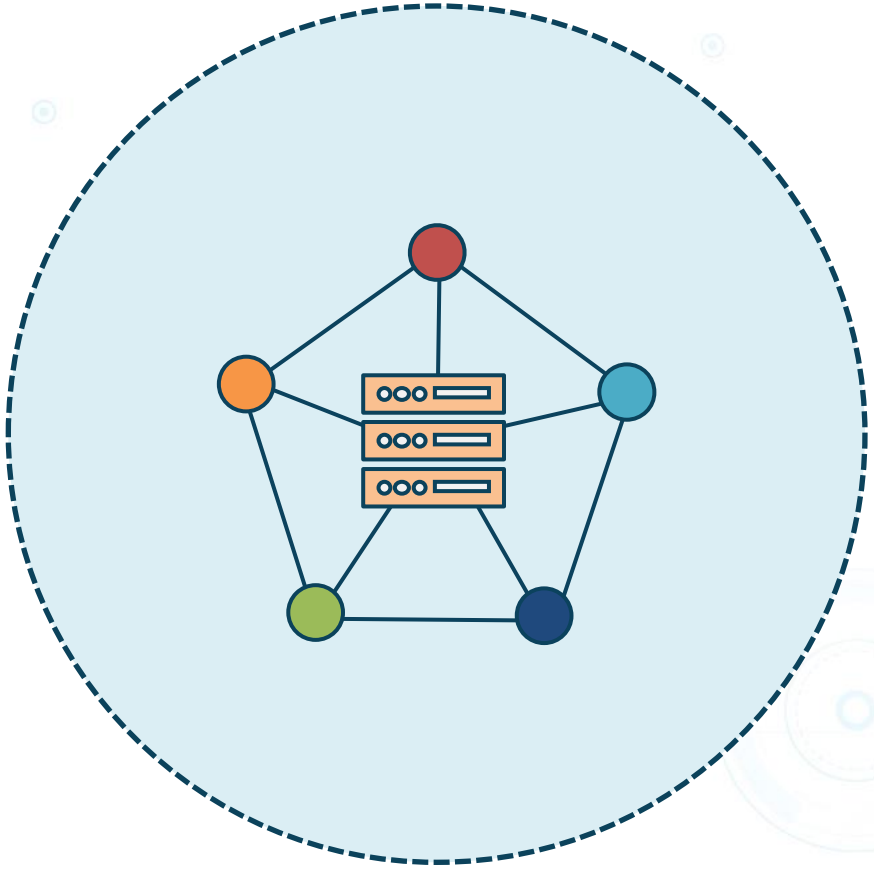


Boot Integrity



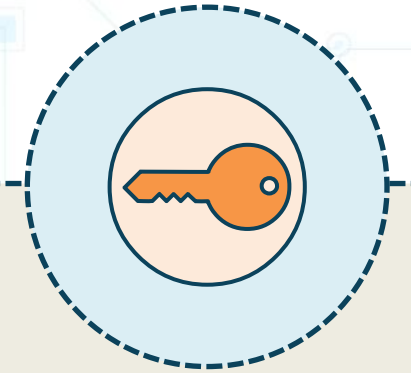
- UEFI – Unified Extensible Firmware Interface replaces legacy BIOS (basic input/output system)
  - Low-level software for booting the device
  - Tests the hardware components (POST)
  - Gets the OS up and running
- Offers the ability to protect the device at a lower level with passwords
- Restricts people from booting from removable devices
- Prevents users from changing BIOS or UEFI settings without permission
- Prevents users from booting other OSs or installing over current OS

Database Security: Tokenization



- Tokenization involves sending sensitive data through an API call (or batch file) to a provider that replaces the data with non-sensitive placeholders called tokens
- Unlike encrypted data, the tokenized data is irreversible and unintelligible

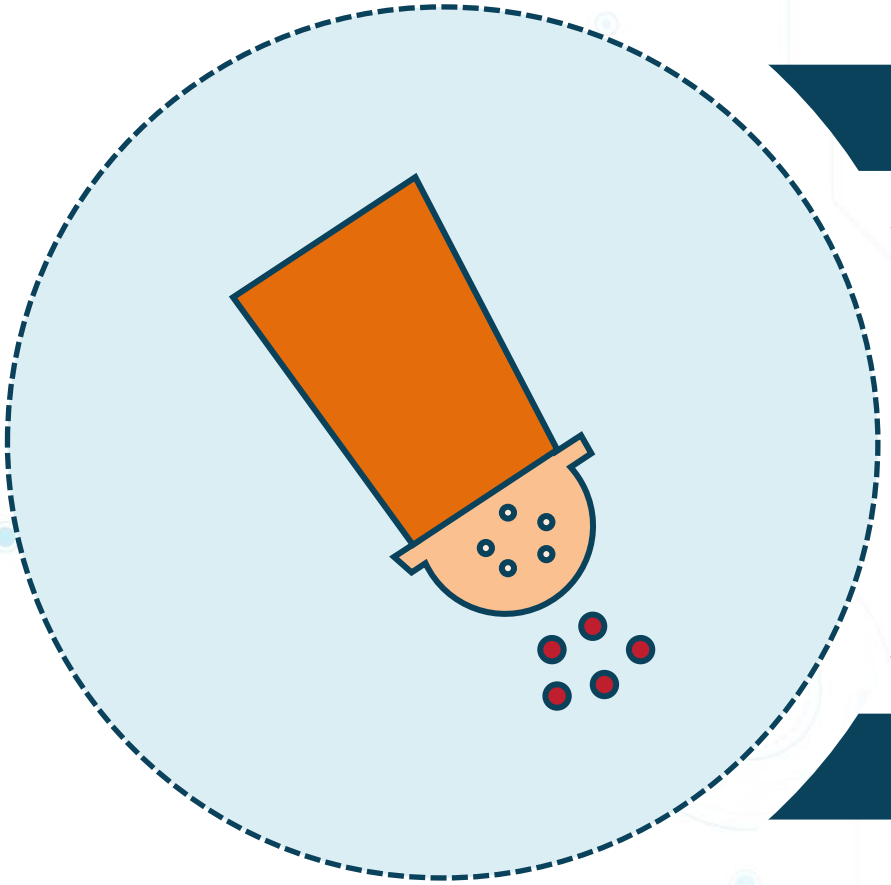
Database Security: Hashing



In a database management system, hashing transforms a string of characters into a typically shorter fixed-length value or key that represents the original string

Hashing is often used to index and retrieve items in a database because it is faster to find the data item using the shorter hashed key than using the original value

Database Security: Salting



- Relates to password hashing
- A value appended to password to create a different hash
- The added value is called a "salt"
- Protects against brute force attacks
- A "pepper" is secret and must not be stored with the output

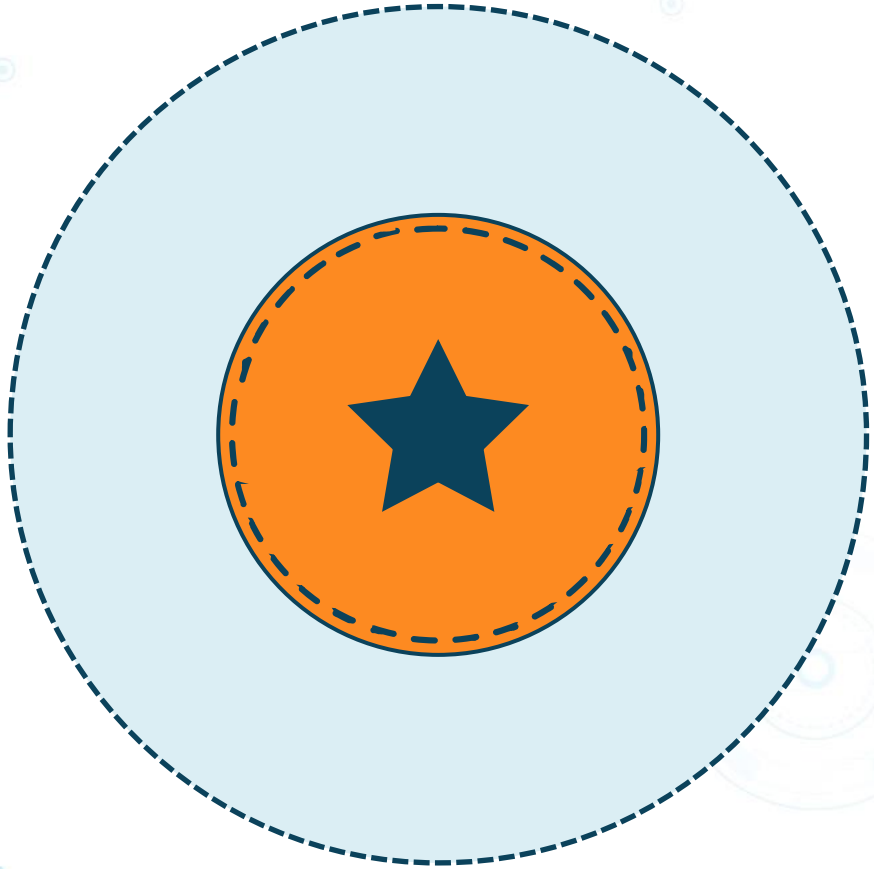
Secure Coding Practices

- Proper input validation
  - Verifying the input before entering it into the system
  - Also includes proper error/exception handling
  - Errors should be captured with secure logging (SIEM)
- Normalization
  - Involves ensuring there is no redundancy in data, and that similar items are stored together

Secure Coding Practices

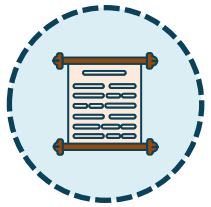
- Stored procedures
  - Precompiled groups of code, statements, and commands that can be called later
  - Also called "code re-use", where one deliberately leverages existing, tested, and validated code that can be used again
- Obfuscation/camouflage
  - Involves writing code that humans have a hard time understanding
- Code signing
  - Digitally signing code to prove author and ensure integrity

Securing Cookies

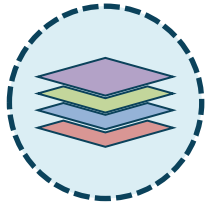


- Cookies were originally poorly designed
- Out of sync with browser same-origin policy (SOP)
- Cookie manipulation attacks are rampant
- Need to validate cookie integrity and deploy HTTP Strict Transport Security (HSTS) with subdomain coverage

Securing HTTP Headers

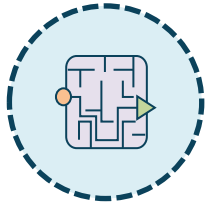


Cross-site scripting

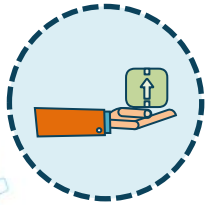


Buffer overflows

SQL injection attacks



Path traversal exploits



Request forgery

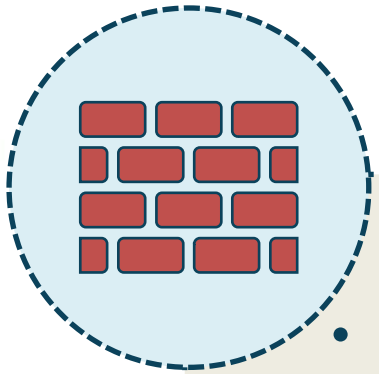
Whitelisting and Blacklisting

- Whitelisting usually involves a stateful firewall that permits traffic based on IP addresses, services, and port numbers while implicitly denying all other traffic
- Blacklisting typically uses stateless access control lists and firewall rules to deny specific traffic based on layer 3 and metadata in IPv4 and IPv6 headers

Analyzing Code

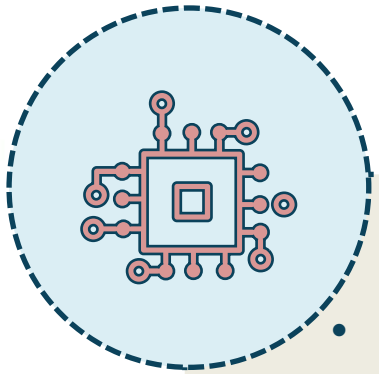
- Static code analysis
- Dynamic code analysis
- Manual code review
- Fuzzing

Hardening Targets



- This involves reducing the attack surface of infrastructure devices, client endpoints, and servers
  - Vulnerability scanning for open ports and services
- Use the Windows Registry Editor to implement IP protocol security and change default permissions
- Deploy full disk encryption, like BitLocker
- Employ self-encrypting drives (SED)
- Have mature and automated patch management

Hardware Root of Trust



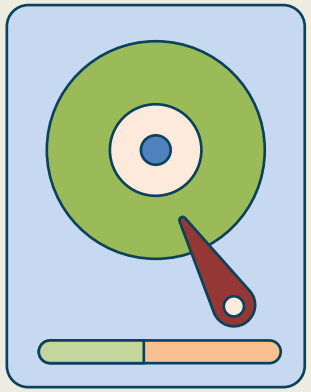
- Hardware root of trust
  - Anchoring the trustworthiness of a system to hardware not software
  - Hardware solutions are more secure than software solutions
  - Less susceptible to attacks since security solutions are on-chip
- Foundations of a Trusted Execution Environments (TEE) or Trusted Computing (TC):
  - TPM – module embedded in a system
  - SED – self-encrypting drives
  - HSM – dedicated crypto processor

Boot Integrity

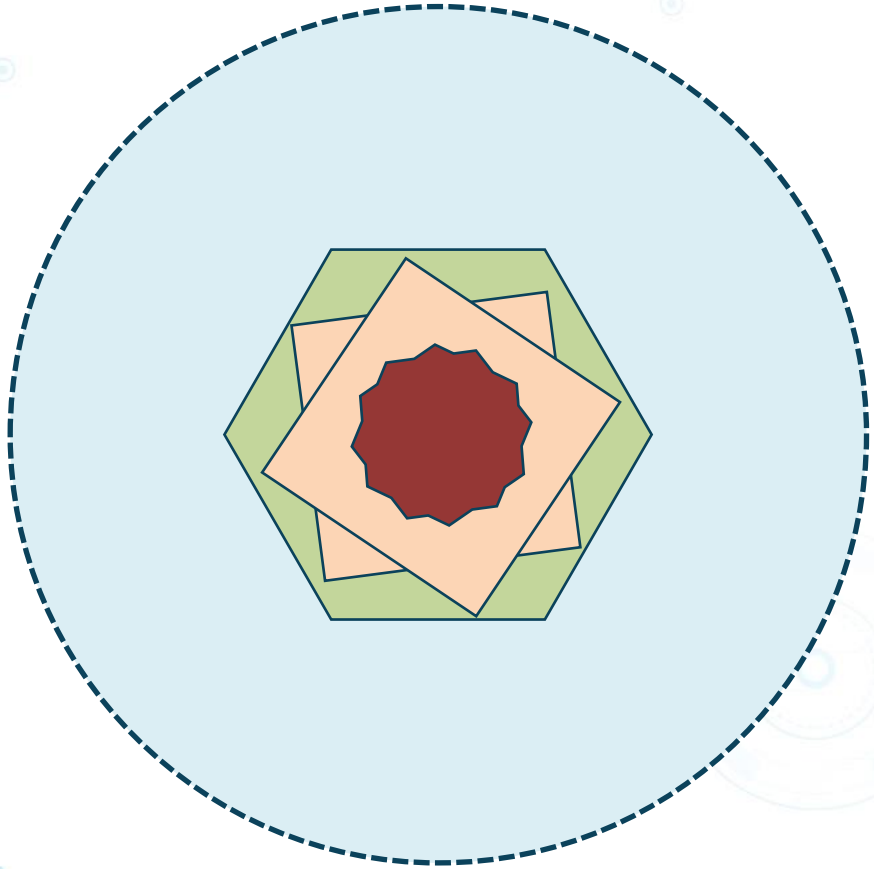
- Computer chip (microcontroller)
  - Installed on the device or built into PCs, tablets, and phones
  - Tamper-resistant security chip
  - Stores info needed to authenticate the platform
    - Passwords, certificates, and encryption keys
  - Provides the following for the platform:
    - Integrity (ensures system has not been altered at a low level)
    - Authentication (ensures system is in fact the correct system)
    - Privacy (ensures system is protected from prying eyes)

Self-encrypting Drives (SED)

- Implements full disk encryption (FDE)
- Hardware-based data encryption
  - All contents on the drive are encrypted, including keys always
  - Encrypts data as written and decrypts data as read
  - Invisible to the end user and can’t be turned off
  - Less susceptible to threats when compared with software-based encryption
  - Stolen keys, repurposed drives, theft of device, end-of-life
- Provides:
  - Pre-boot authentication, endpoint security, and device authentication
  - Encryption, key management, network access control, and policy compliance



OPAL



- The TCG Opal Security Subsystem Class (SSC) is a group of specifications for SEDs created by the Trusted Computing Group (TCG)
- The Opal SSC defines a hierarchy of security management standards to secure data from theft and tampering by unauthorized persons who can access a storage device or host system where the storage device resides