



Security+ Session 2

**with Michael J. Shannon - CISSP, Security+, CCNP-SEC, Palo Alto PCNSE7,
ITIL 4 Managing Professional, and OpenFAIR**

Identifying Vulnerability

- Must begin with how organization defines "vulnerability"
- The probability that a threat agent's actions will result in a loss (frequency and magnitude)
- It should be quantified as a percentage of probability and not just a vague list of "scary things"
- Example: a password policy is 25% likely to get exploited by a brute-force or dictionary attack
- It can be a derived value from threat capability of actors combined with the resistance of existing security controls

Identifying Vulnerability

- Can use vulnerability scanners like Nessus, OpenVAS, Core Impact, Nexpose, GFI LanGuard, and QualysGuard
- **Use SaaS cloud solutions to help identify vulnerabilities**
- Involves first doing asset assessment of the following:
 - All client and server operating systems and versions/builds
 - Posture of patches, updates, security fixes
 - Browsers, types of endpoints
 - Methods of access: wired, wireless, VPN, remote teleworkers
 - Assess control types and categories
 - Analyze access control methodologies (2FA)

Identify Common Misconfigurations

- One of the most common vulnerabilities
- Difficult to find without a thorough examination of all applications and code
- Example: Web applications are built on several layers (FE/BE, middleware/business intelligence, database, browsers, and other web-enabled clients) making a configuration error somewhere very possible
- Could be as simple as a system administrator forgetting to delete a default account or ex-employee account with admin/root privileges

Identify Common Misconfigurations

- (L2) Switch configuration best practices is a good place to begin – wireless Aps and controllers
- (L3) Proper routing peer authentication and complete advantage of all firewall and sensor capabilities
- Evaluate server configuration (web, email, ftp, SP, content)
- Endpoint configuration should focus on least privilege access controls – privileged vs. non-privileged users
- Remove/disable any unnecessary features/services
- Examine all custom code

System Vulnerabilities

- Broad term that represents any weakness in the design, implementation, configuration, and ongoing operation of a system or service
- Example: database vulnerabilities
 - Deployment errors
 - Unpatched and unfixed
 - Data leaks and data loss
 - Stolen or damaged backups
 - Lack of segregation
 - Poor RBAC
 - SQL injections



Credentialed vs. Non-credentialed

- Credentialed users and systems have varying degrees of access depending on the architecture: DAC, MAC, RBAC
- At least privileged and non-privileged users
- Pentesting should involve posing as a contractor or vendor
- Guest users that are non-credentialed getting access
- Piggybacking (tailgating) and other social engineering attempts should be part of the process

False Positives and False Negatives

- False positives and false negatives are a big challenge
 - True = accurate (benign)
 - False = error (malicious)
 - Positive = action (alert)
 - Negative = no action (no alert)
- Reducing false positives and negatives is critical to accurate vulnerability analysis and penetration testing



Common Vulnerability Scenarios

- End-of-life systems
 - Continuing to use systems and applications that are no longer supported and security patched
- Embedded systems
 - Often use older and unhardened O/Ss
 - Lack of ongoing vendor support and updates
 - Special logic controllers that are web-enabled and IoT devices
- Lack of continual vendor support
- Lack of patch management processes



Lack of Patch Management

- Patch management is a best practice of upgrading existing software applications to address any weaknesses that could be exploited by hackers
- It is often neglected since it is not easy, and many organizations patch only after an attack. Common reasons:
 - Testing of updates is time-consuming hence the delay
 - The system or application is critical - and the downtime cannot be afforded (no redundancy)
 - The operating system has reached end of life, but a critical application cannot function on a higher O/S version

Poor Coding Techniques

- Improper Input and Error Handling
 - Poorly defined validation rules used in verifying the correctness, completeness, and acceptability of input data
- Race conditions
 - When a system or software tries to do two or more things simultaneously, but due to the type of system, the operations must be done in the correct sequence in order to function properly



Identify Common Misconfigurations

- One of the most common vulnerabilities
- Difficult to find without a thorough examination of all applications and code
- Example: Web applications are built on several layers (FE/BE, middleware/business intelligence, database, browsers, and other web-enabled clients) making a configuration error somewhere very possible
- Could be as simple as a system administrator forgetting to delete a default account or ex-employee account with admin/root privileges

Identify Common Misconfigurations

- (L2) Switch configuration best practices is a good place to begin – wireless Aps and controllers
- (L3) Proper routing peer authentication and complete advantage of all firewall and sensor capabilities
- Evaluate server configuration (web, email, ftp, SP, content)
- Endpoint configuration should focus on least privilege access controls – privileged vs. non-privileged users
- Remove/disable any unnecessary features/services
- Examine all custom code

System Vulnerabilities

- Broad term that represents any weakness in the design, implementation, configuration, and ongoing operation of a system or service
- Example: database vulnerabilities
 - Deployment errors
 - Unpatched and unfixed
 - Data leaks and data loss
 - Stolen or damaged backups
 - Lack of segregation
 - Poor RBAC
 - SQL injections



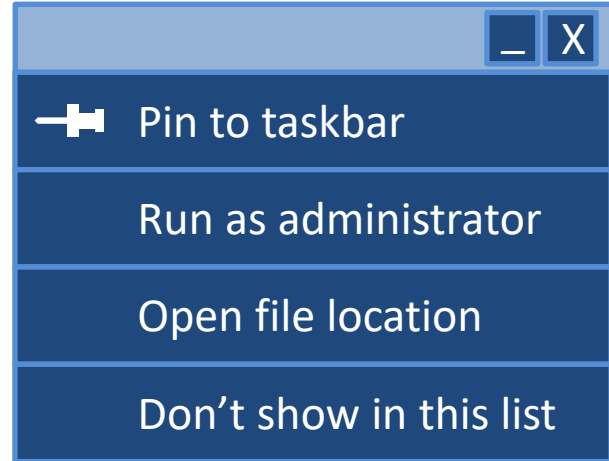
Improperly Configured Accounts

- Local administrative accounts
- Privileged user accounts
- Forest/domain administrators
- Emergency accounts
- Service accounts
- Application accounts



Improperly Configured Accounts

- Biggest issue is overprivileged users
- Logging, auditing, and reporting
- Least privilege principle should be used
- Use separate account for admin tasks (Run as...)
- Proper permission policies
- Use centralized secure systems and directory services
- Vulnerable to privileged insiders



Untrained Users

- Security awareness training and ongoing training of staff is seen as a cost and not an investment
- BYOD has complicated the issue of untrained users
- AUP must be strictly enforced
- Get buy-in from all employees
- Offer incentives



Resource Exhaustion

- Attack on availability aspect of CIA triad
- Often the result of flooding, DoS, DDoS, botnets
- Common examples:
 - Buffer overflows
 - CPU cycle stealing
 - Network bandwidth
 - DNS resources
 - Network device input queues
 - Disk space from worms
 - DHCP lease starvation
 - MAC flooding

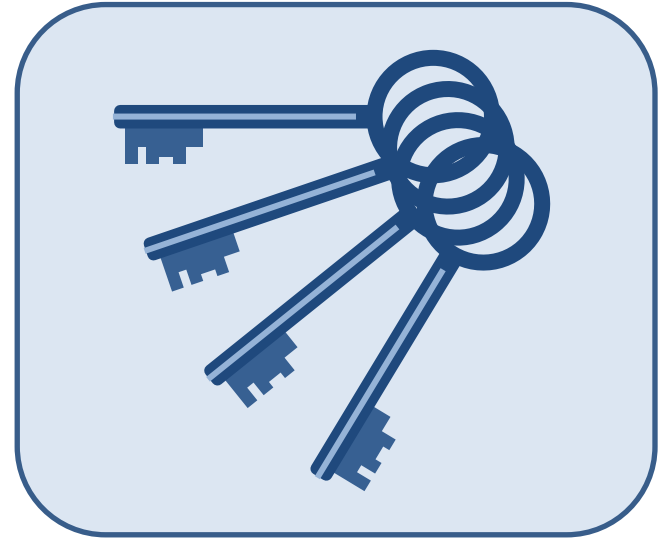


Vulnerable Business Processes

- Unsecure databases of customer and employee PII
 - Unprotected and unpatched e-commerce servers
 - Using clear-text and unsecure protocols
 - Not using modern SSL/TLS and IVEv2
 - Using self-signed certificates
- Not fully vetting cloud and security providers
 - Lack of cyber and business liability insurance
 - Not encrypting front-end/back-end communications
 - Poor authentication and authorization mechanisms

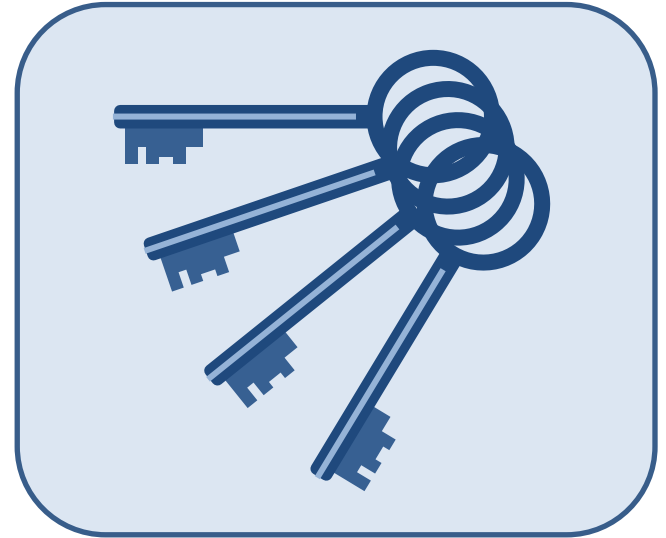
Weak Cipher Suites and Implementations

- Digitally sign as much as possible
- Do not use self-signed certificates
- Avoid sites with certificate errors or warnings
- Stop using RC4, MD5, SHA-1 suites
- Use AES-256 and SHA-256 if available



Weak Cipher Suites and Implementations

- Use Suite B Cryptography (IKEv2) with VPN implementations
- Have solid key management practices
- Use strong pseudo-random passwords
- Implementing HSTS on web servers
- Using secure DNS (cloud-based) like Cisco Umbrella or AWS Route 53



Memory/Buffer Vulnerability

- Memory leak
 - Unintentional memory usage from poor programming
- Integer overflow
 - Common C program attack
- Pointer dereference
 - Null pointer errors are usually assumption violations
- DLL injection
 - Running code of another process



System Sprawl and Undocumented Assets

- The accelerated growth of data and cloud storage is a challenge for enterprises
- Virtual machines, personal cloud services, and personal electronics lead to app and data leakage
- Convert massive amounts of documentation into PDFs and distribute through email and the web
- Removable drives and devices need asset management and provisioning
- Asset tags and inventory systems are critical



System Sprawl and Undocumented Assets

- Digital rights management (DRM) mechanisms are varied access control technologies used to control usage of proprietary hardware and copyrighted works
- DRM technologies attempt to manage the use, modification, and distribution of copyrighted software and multimedia content
- Deploy systems within devices to enforce DRM policies



Architecture and Design Weaknesses

- All architecture and design methodologies have weaknesses and vulnerabilities:
 - Database
 - Network
 - Access control
 - Applications
 - Security
 - Policies
 - Physical and facility
 - Risk management

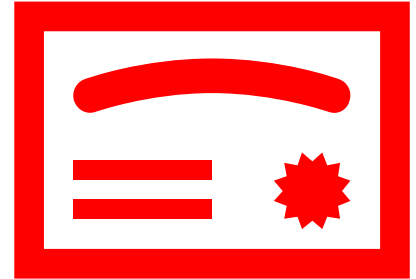


Improper Certificate and Key Management

- Stealing CA signing private keys or root keys allows fake certificates to be issued
- Any suspicion of compromise may force re-issuance of some or all previously issued certificates
- Weak controls over the use of signing keys can allow the CA to be corrupted even if the keys are not compromised
- Theft (or misuse) of keys linked to online certificate validation processes can be leveraged to sabotage revocation processes and allow for malicious use of revoked certificates
- Must log and monitor all aspects of signing activities related to issuance and validation checking

Improper Certificate and Key Management

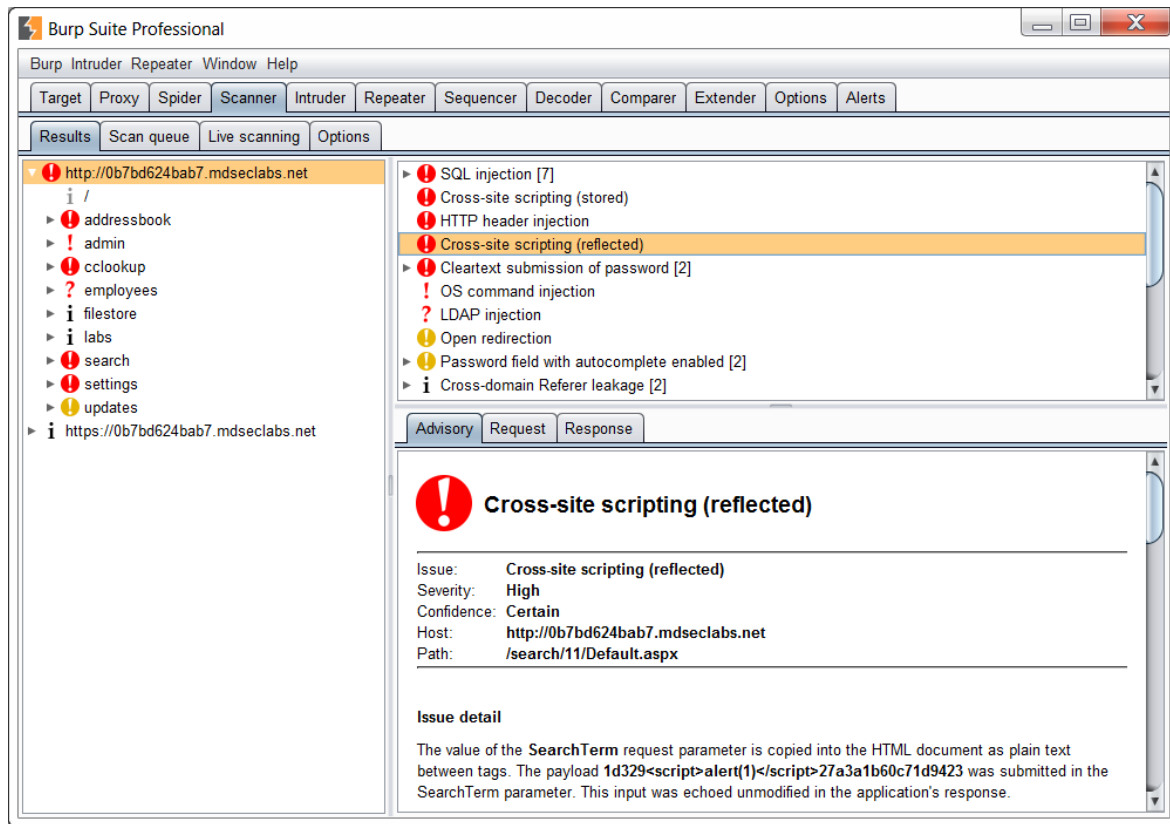
- Use trusted third-party CA services
- Use fully-tested enterprise CA
- Validate certificate chains
- Consider secure OCSP for revocation
- Eliminate risky manual key management processes
- Tightly enforce key management policies
- Use third-party services to help ensure integrity, performance, and manageability of your PKI



Vulnerability Scanners

- Popular pen testing tools that can be dangerous
- Web Application Vulnerability Scanners are most common due to heavy usage of HTTP
- Automated tools can scan web applications and look for security vulnerabilities such as:
 - Cross-site scripting
 - SQL Injection
 - Command Injection
 - Path Traversal
 - Insecure server configuration

Vulnerability Scanners



The screenshot displays the Burp Suite Professional interface. The top menu bar includes 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. Below this is a tabbed interface with 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Options', and 'Alerts'. The 'Scanner' tab is active, showing a list of scan results on the left and a detailed view of a selected issue on the right.

Scan Results (Left Panel):

- http://0b7bd624bab7.mdseclabs.net
 - /
 - ! addressbook
 - ! admin
 - ! cclookup
 - ? employees
 - i filestore
 - i labs
 - ! search
 - ! settings
 - ! updates
 - i https://0b7bd624bab7.mdseclabs.net

Vulnerability Details (Right Panel):

Cross-site scripting (reflected)

Issue: Cross-site scripting (reflected)
Severity: High
Confidence: Certain
Host: http://0b7bd624bab7.mdseclabs.net
Path: /search/11/Default.aspx

Issue detail

The value of the **SearchTerm** request parameter is copied into the HTML document as plain text between tags. The payload `1d329<script>alert(1)</script>27a3a1b60c71d9423` was submitted in the **SearchTerm** parameter. This input was echoed unmodified in the application's response.

Wireless Scanners and Crackers



Protocol Analyzers

- Devices that capture and analyze network traffic between two or more systems
- Traffic can be filtered and decoded to visualize what processes are occurring
- Protocol analyzers can be used find network bottlenecks, troubleshoot, and analyze malware behavior
- Advanced analyzers can also generate statistics for trend analysis and network optimization
- Crackers can use them to gather information or even clear-text usernames and passwords among other things

Protocol Analyzers

The image shows a Wireshark window titled "test.pcap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with icons for file operations, capture, and analysis, and a filter bar with a "Filter:" input field and buttons for "Expression...", "Clear", and "Apply".

The main display area shows a list of captured packets. The selected packet is packet 36, which is a TCP window update and acknowledgment. The packet details pane shows the following information:

- Frame 36 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d:75:9a), Dst: 192.168.0.2 (00:0b:5d:20:cd:02)
- Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 3197 (3197), Seq: 20, Ack: 190, Len: 0
- Source port: http (80)
- Destination port: 3197 (3197)
- Sequence number: 20 (relative sequence number)
- Acknowledgement number: 190 (relative ack number)
- Header length: 20 bytes

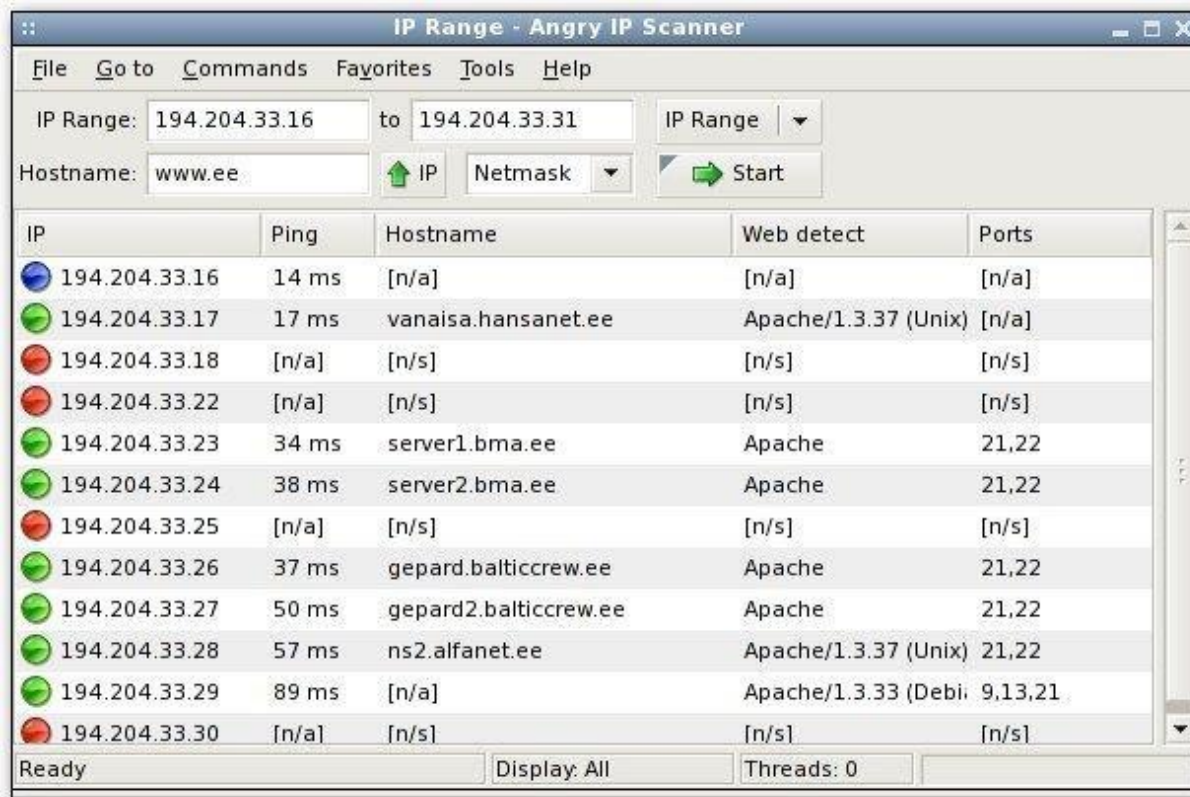
The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII representation shows the sequence number 20 and the acknowledgement number 190.

The status bar at the bottom indicates "Acknowledgement number (tcp.ack), 4 bytes" and "P: 120 D: 120 M: 0".

Network Scanners

- Can be used to scan IP addresses, ports, and device locations presented in a customized graphical XML view
- Most provide network monitoring and management capabilities to detect, diagnose, and resolve network issues and outages
- Advanced IP Scanners is also work remote administration software to add capabilities and vulnerability
- Angry IP Scanner is popular open-source utility
- Active malware worms are also considered network scanners

Network Scanners



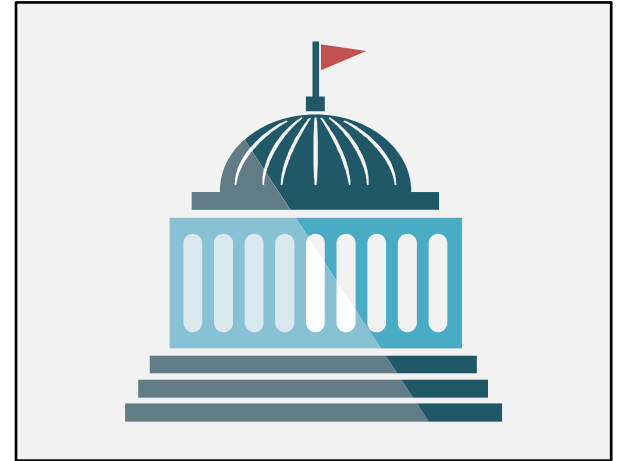
Configuration Compliance Scanners

- Carrying out a compliance audit is different than performing a vulnerability scan
 - although there can be some overlap
- A compliance audit decides if a system is configured in agreement with a recognized governance policy
- A vulnerability scan determines if the system is exposed to known vulnerabilities
- Sometimes compliance involves auditing more sensitive data and systems



Configuration Compliance Scanners

- There are many diverse forms of financial and government compliance requirements
- Typically the compliance requirements are minimal baselines that can be taken differently depending on the goals of the organization
- Compliance requirements must be in line with the business goals to ensure that risks are correctly recognized and alleviated



Other Command Line Tools

- ping
- netstat
- Tracert/traceroute
- nslookup/dig
- arp
- ipconfig/ifconfig
- tcpdump
- nmap
- netcat

Pentesting vs. Vulnerability Scanning

- **Vulnerability scanning** is an easier and often more focused process looking for unpatched systems and open ports
- Often automated, routine basis (weekly, quarterly) taking a few hours
- **Pentesting** is a thorough investigation of all known vulnerabilities and an actual ethical attempt to exploit the vulnerabilities
- More manual activity often taking days

Active vs. Passive Reconnaissance

- Wired and wireless packet sniffers and analyzers allow for the passive capture of data packets
- These tools are also being used by crackers to intercept data packets
- Passive reconnaissance involves using packet sniffers, passive scanners, or taps to gather copies of frames and packets to observe the contents
 - Also capturing phone and VoIP packets – wiretapping

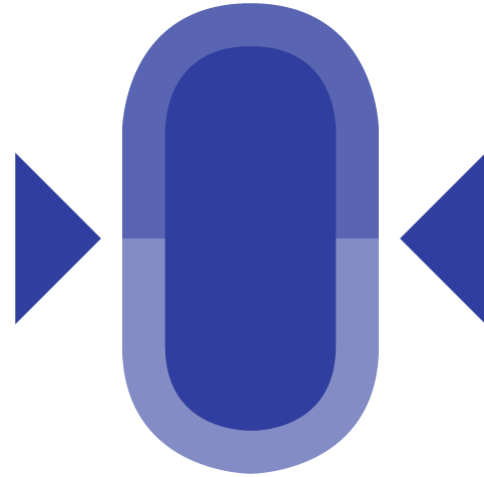


Passively Testing Security Controls

- Less-intrusive process to daily operations and employee productivity
- Involves scanning and snooping tools to gather information for analysis
- Uses intrusion detection (copies of frames) as opposed to inline intrusion prevention (IPS)
- Run security devices in monitor-only mode
- Firewalls and other appliances have CLI-based and GUI packet tracer capabilities

Actively Testing Security Controls

- Active information gathering (reconnaissance) typically involves an action on a target endpoint or network that could be traced back to the attacker
- Examples:
 - Running a web application scan
 - Port and address scanning
 - Vulnerability scanning
 - Banner grabbing
 - Active system fingerprinting



Pivoting

- Pivoting allows you to jump from one segment, domain, or system to another
- Also used by VLAN hopping, port forwarding, trust exploits, etc.
- Example: VPN pivoting in Metasploit Pro allows users to route traffic through an exploited host to a different network
- VPN pivoting mounts hooks at the kernel level of the target system without making a permanent/persistent change to the O/S – gives the pentesting machine an IP address on the network of the exploited host

Initial Exploitation

- Before performing pentesting, the following processes should precede the initial exploit:
 - Planning and preparation
 - Information gathering and analysis
 - Vulnerability assessment
- When performing penetration testing the initial exploit will often involve one of the following:
 - Social engineering
 - Passive reconnaissance and packet sniffing
 - Vulnerability scanning unpatched apps and O/S
 - Finding weaknesses in physical security



Persistence

- Malware persistence is composed of various small elements that execute each other, sometimes in an indirect way:
 1. Run key is placed in the registry then link to the key
 2. A batch script runs the file with a new extension
 3. A command in the registry handles the added extension
 4. JavaScript with XOR reads other dropped registry keys and runs the next...
 5. PowerShell script with Base64
 6. PowerShell script decodes and runs the shellcode
 7. Shellcode reads the dropped registry key, unpacks the PowerShell PE file from it, and loads it into memory

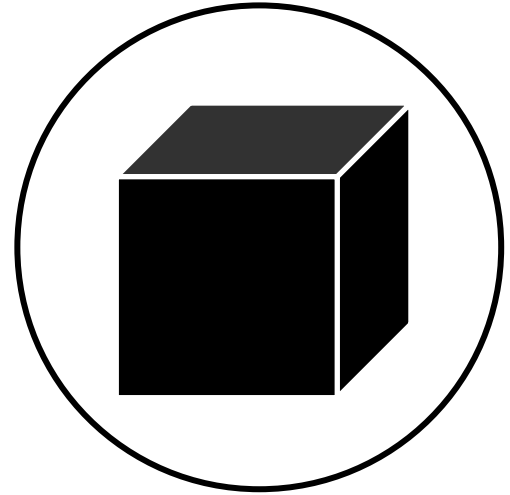
Escalation (elevation) of Privilege

- Usually the next phase after the initial compromise
- Leverages programming errors and system design flaws to give an attacker elevated access to the network and related systems, data, and applications
- Vertical vs. horizontal
- During pentesting it is difficult to get access to a system with administrator privileges in the initial attempt
- Beginners: check out **g0tm1k** on the Web



Black vs. White Box

- With black box, the penetration tester assumes the role of an average external attacker
- No internal knowledge of the target applications, systems, and services
- Testers are not given any architecture diagrams or source code that is not publicly available
- This pentest determines the vulnerabilities in a system that are exploitable from outside the network
- Black box testing is also an application testing method in which the internal structure/design/implementation of the item being tested is NOT known to the tester

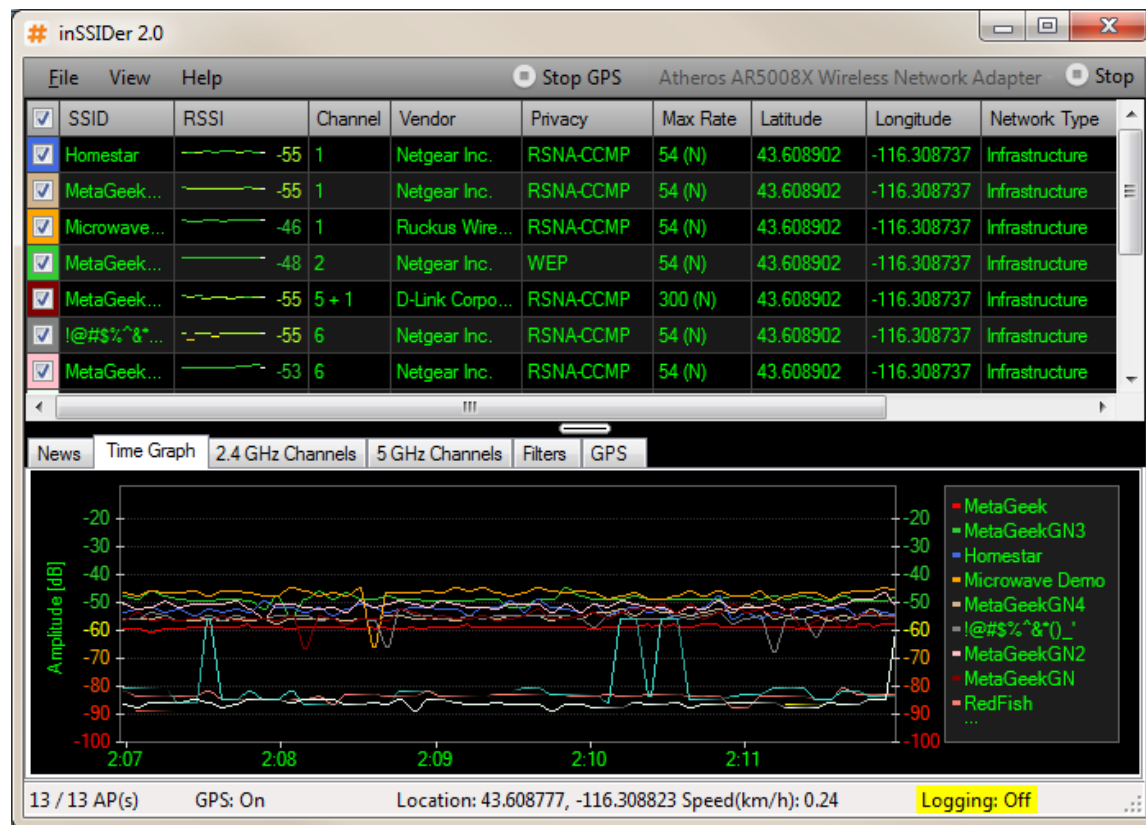


Black vs. White vs. Gray Box

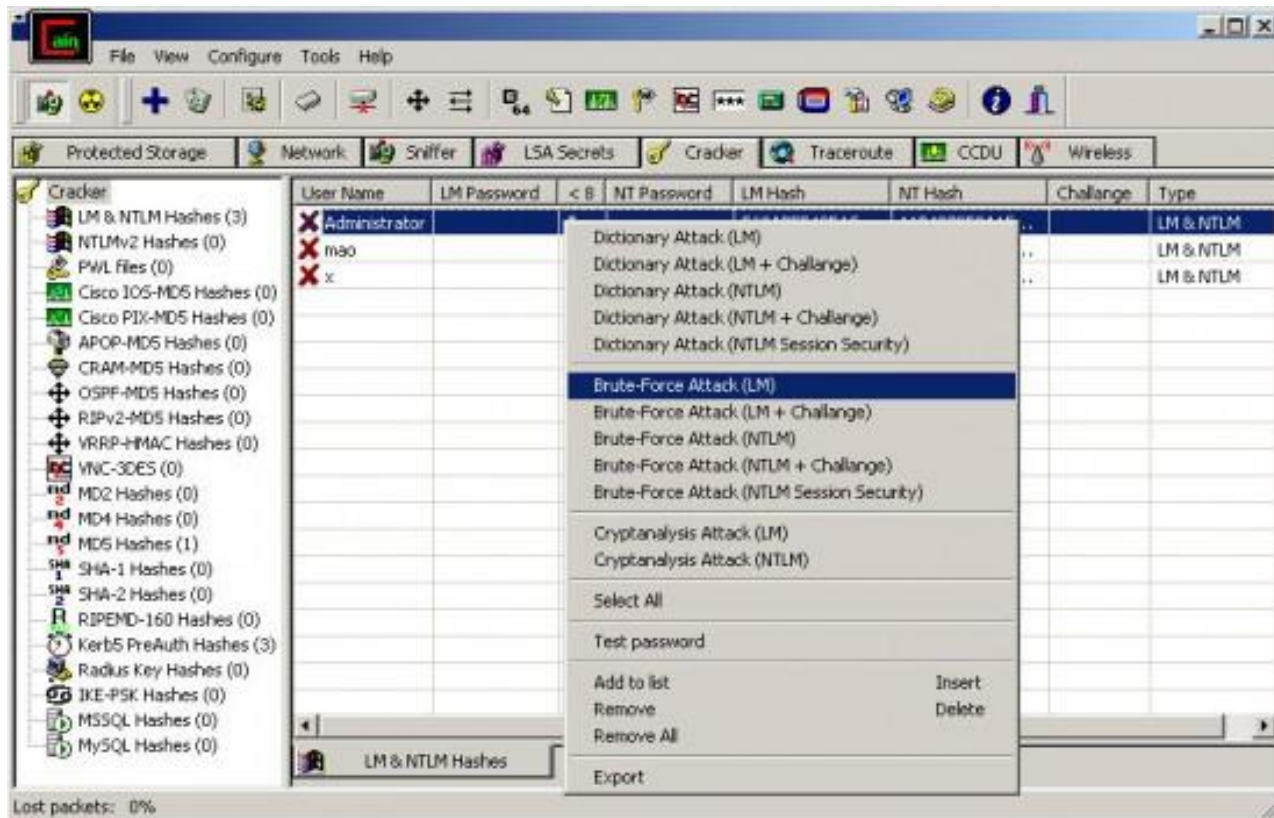
- White-box testing is also called clear-box, open-box, auxiliary and logic-driven testing
- It is the opposite of black-box testing since pentesters are given full access to architecture documentation, systems design, service deployment, source code, and more
- The main challenge of white-box testing is processing the huge amount of data available to identify potential points of weakness
- This is the most time-consuming type of penetration testing
- Can be credentialed or non-credentialed



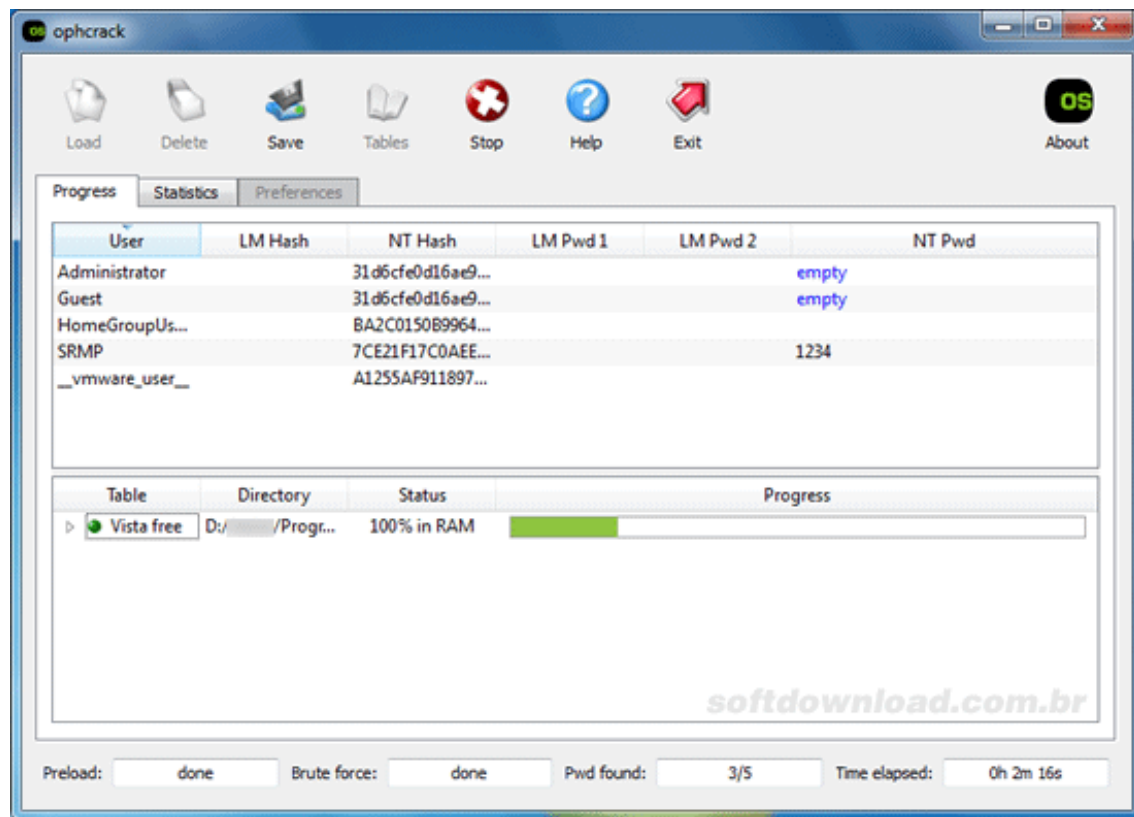
Wireless Scanners and Crackers



Password Crackers



Password Crackers



Banner Grabbing

- The “banner” usually refers to a message that a service sends when another host or program is first connecting
- Banner grabbing has good and bad purposes
- Administrators can use it for system inventory and asset management
- Ethical hackers use it during penetration testing

Banner Grabbing

- Malicious hackers use as part of reconnaissance attack:
 - Services run on remote system
 - Open ports and channels
 - Web and FTP servers respond to requests
- Malicious hackers banner grabbing to find vulnerable hosts and enumerate server systems
- Default banners often reveal the type of software and version, known exploits can be launched in next phase
- Layer 5/7 security can remove banner functionality at the firewall or ALG

Exploitation Frameworks

- Exploitation kits 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-black hat hackers
- Can be used to prioritize vulnerabilities and threat in the enterprise



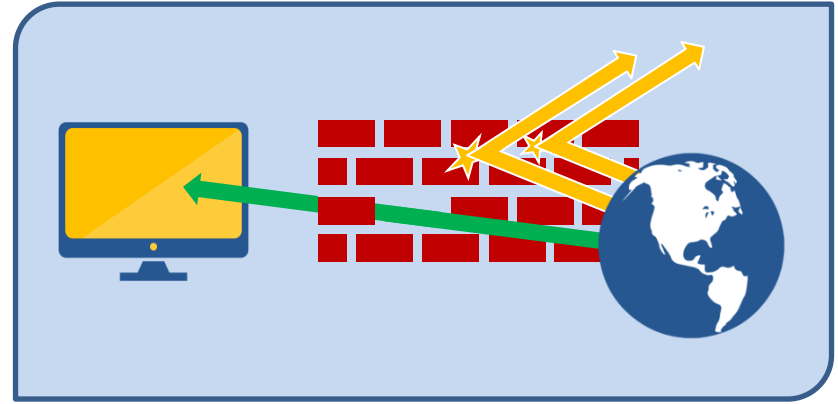
Exploitation Frameworks

- The Browser Exploitation Framework (BeEF)
- PowerSploit Framework
- Canvas
- Core Impact
- Elliot exploitation framework
- RouterSploit
- ExploitHub
- MetaSploit

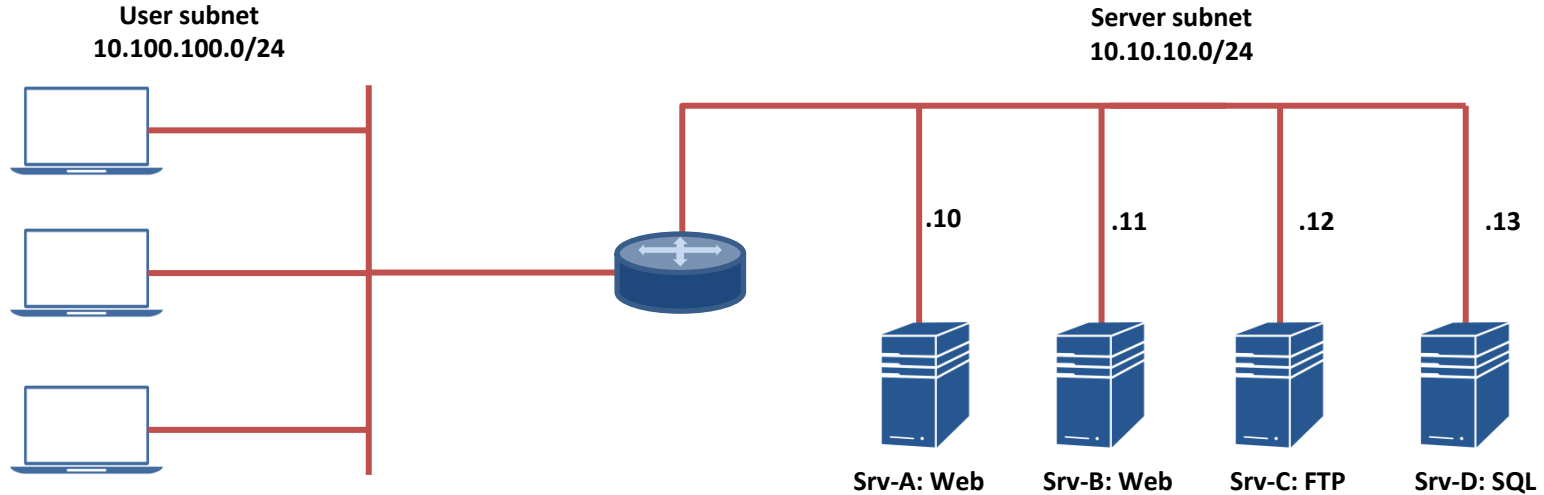


Firewalls

- Firewalls are integrated systems of threat defense functioning at layers 2-7
- Between all zones, domains, partitions
- Network or Application
- Restrictive vs. permissive
- Stateless vs. stateful
- Classic FWs use ACLs and inspection rules that are interface based



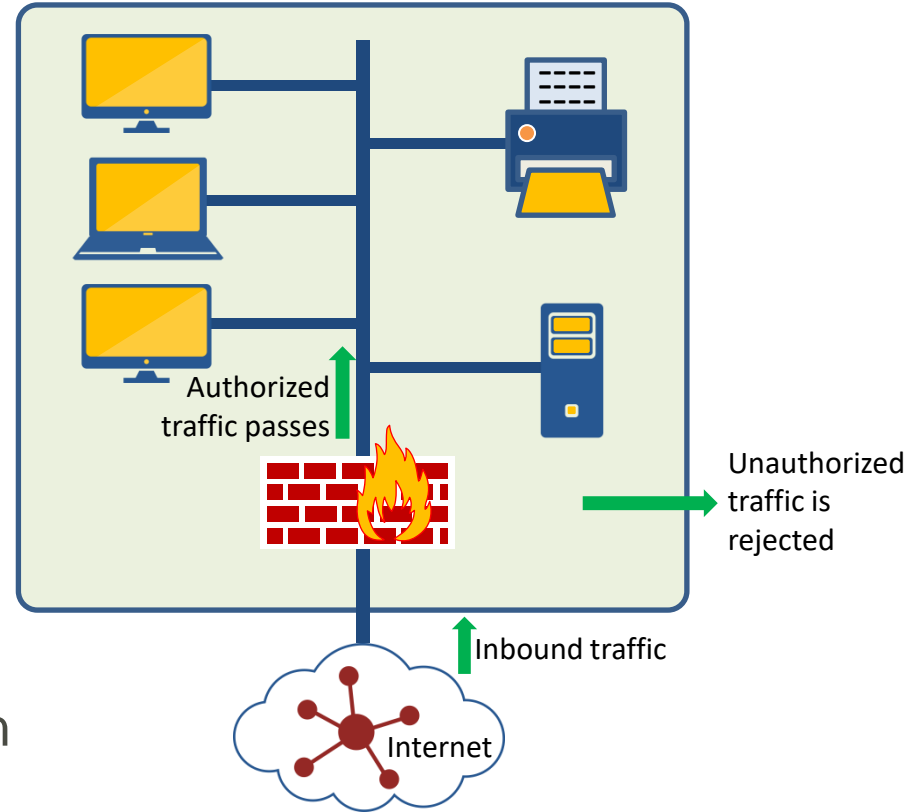
Firewall Access Control Lists (ACLs)



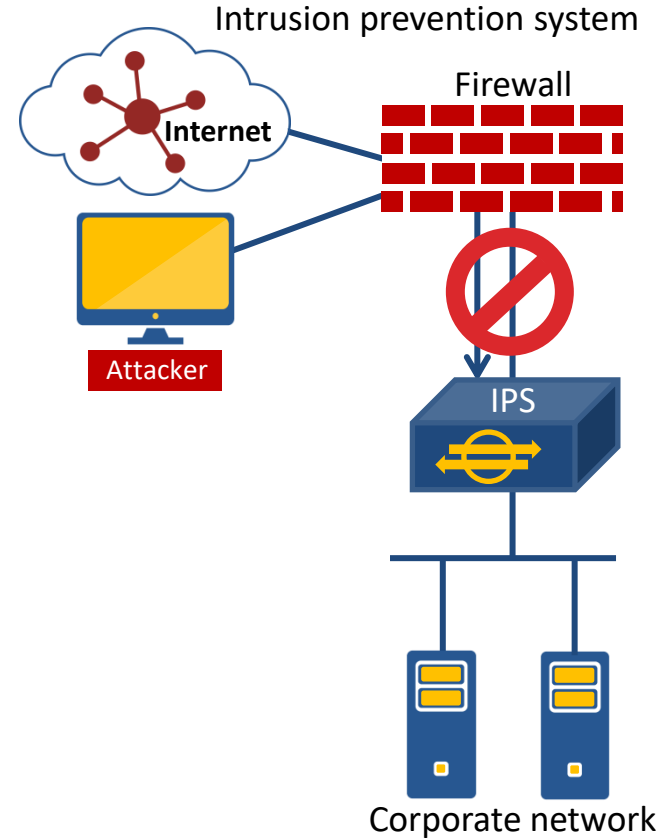
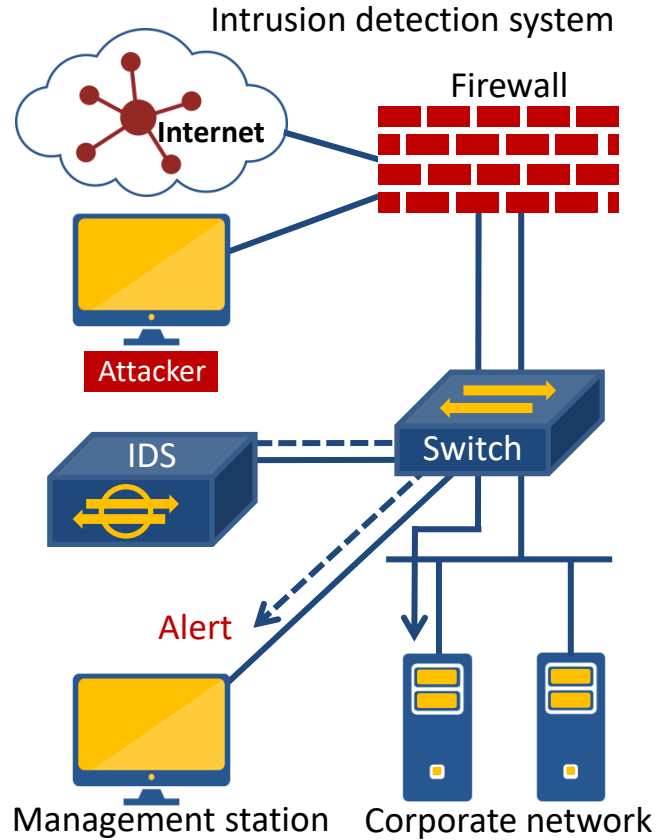
```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data
access-list 100 deny ip any any log
```


Firewalls

- Next-Generation (NGFW)
 - Layer 5-7 policies
 - Authentication proxy
 - Identity services
 - Integrated IDS/IPS
 - Content security
 - Advanced malware protection
 - URL filtering
 - Botnet filtering
 - Cloud correlation and participation



NIDS and NIPS



NIDS and NIPS

- Network-based intrusion detection and intrusion prevention
- Monitor mode (promiscuous mode or passive)
- Inline (IPS) mode
- In-band vs. OOB
- Signature based
- Anomaly based
- Heuristic/Behavioral (UBA)
- Cloud based (ML/AI)



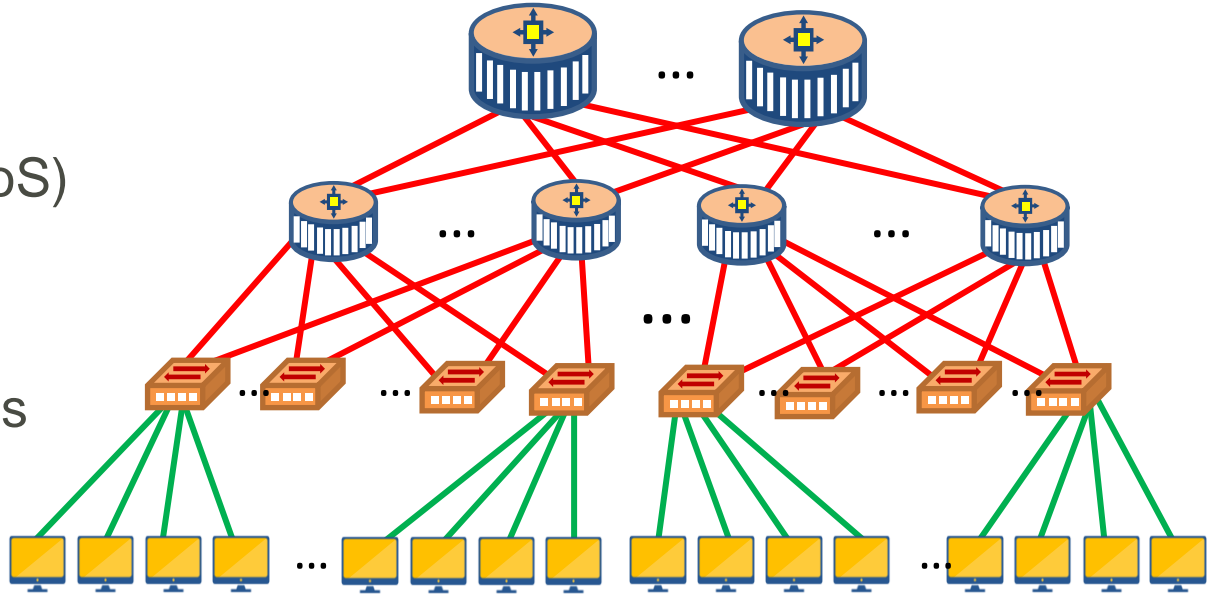
False Positives and False Negatives

- False positives and false negatives are a big challenge
 - True = accurate (benign)
 - False = error (malicious)
 - Positive = action (alert)
 - Negative = no action (no alert)
- Reducing false positives and negatives is critical to accurate vulnerability analysis and penetration testing



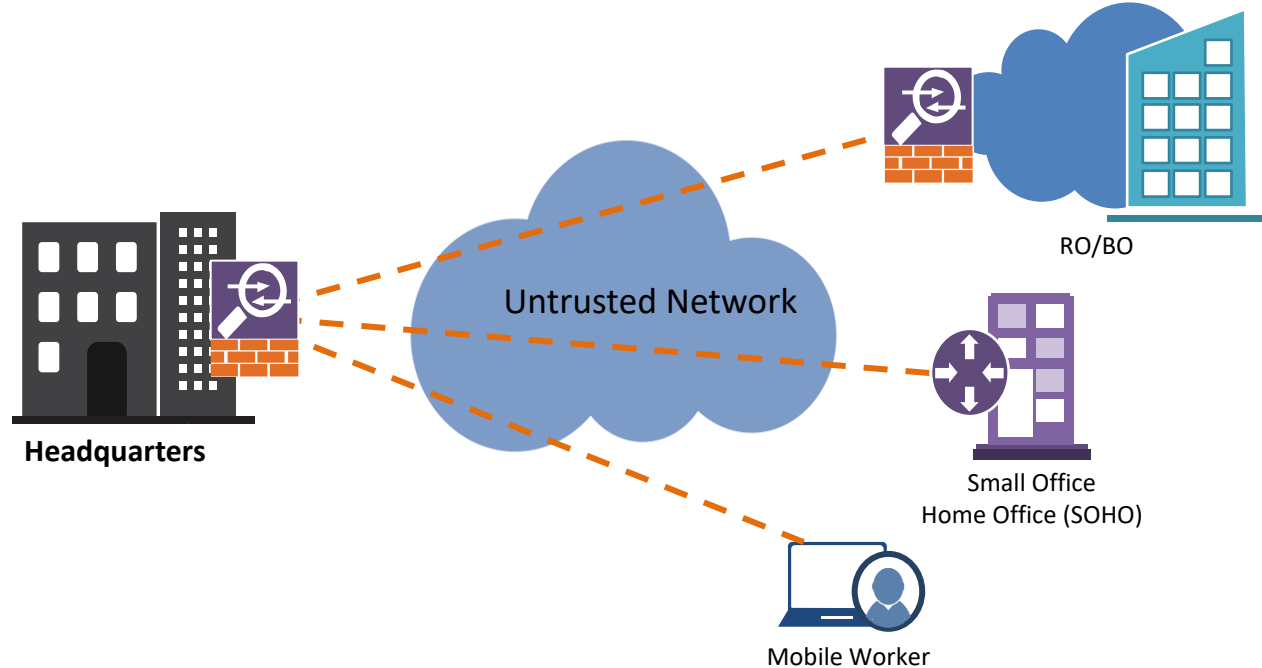
Routers

- Modern routers can also provide a wide variety of services:
 - NAT and PAT (firewall)
 - Firewall services
 - VRF
 - Quality of Service (QoS)
 - Voice-over-IP
 - IDS/IPS
 - VPN gateway services
 - URL filtering
 - Proxy services



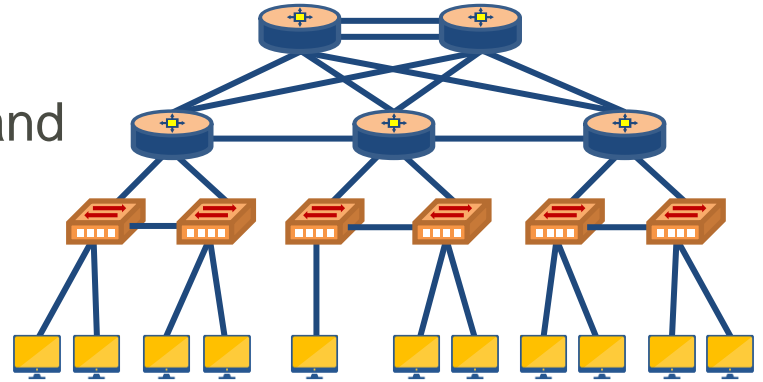
VPN Gateways (Concentrators)

- Site-to-Site VPN
- Remote Access VPN
- Client or clientless
- IPsec IKEv1 or IKEv2:
 - Tunnel mode or transport mode
 - AH or ESP
 - Split tunnel vs. full tunnel
 - Always-on VPN
- IPv4 and/or IPv6
- CSP-based (AWS, GCP, Azure)



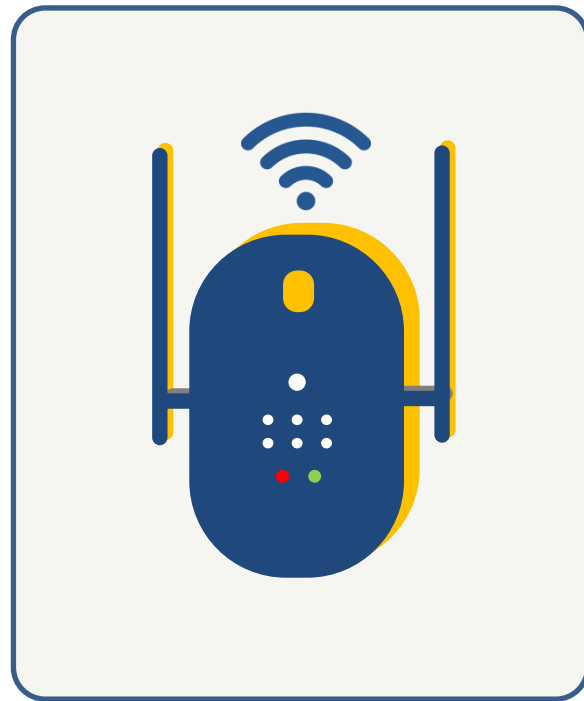
Switches

- Operate at Layers 2-4 and above with extensive capabilities and flexibility
- Access switches and aggregate switches
- Physical or virtual (SDN)
- VLANs and PVLANS enforce trust model and layer 2 security
- Switch port security is tantamount
- Loop prevention and flood guard
- DHCP snooping, DAI, IP SourceGuard
- 802.1X and MACsec are important features



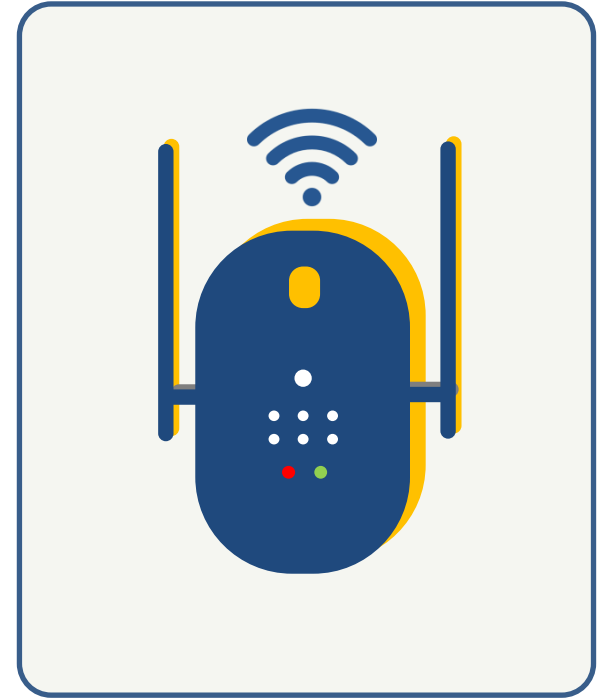
Wireless Access Points

- SSID/MAC filtering
- Control design and signal strength
- Antenna types and placement
- Controller-based vs. standalone
- Wireless IPS
 - Rogue access points
 - Rogue DHCP services
 - Wireless analysis
- WPA3 has arrived (not on exam)



Wireless Access Points

- Wireless Access Points (WAPs) typically operate Layers 1 and 2 of the OSI model and create wireless LANs
- Beginning with a single AP replacing a cable, Wi-Fi networks are a true extension of the wired LAN – sometimes distributing over warehouses or entire campuses
- Offer simultaneous network connectivity to thousands of laptops, tablets, smart phones
- Standalone vs. infrastructure and internal vs. external



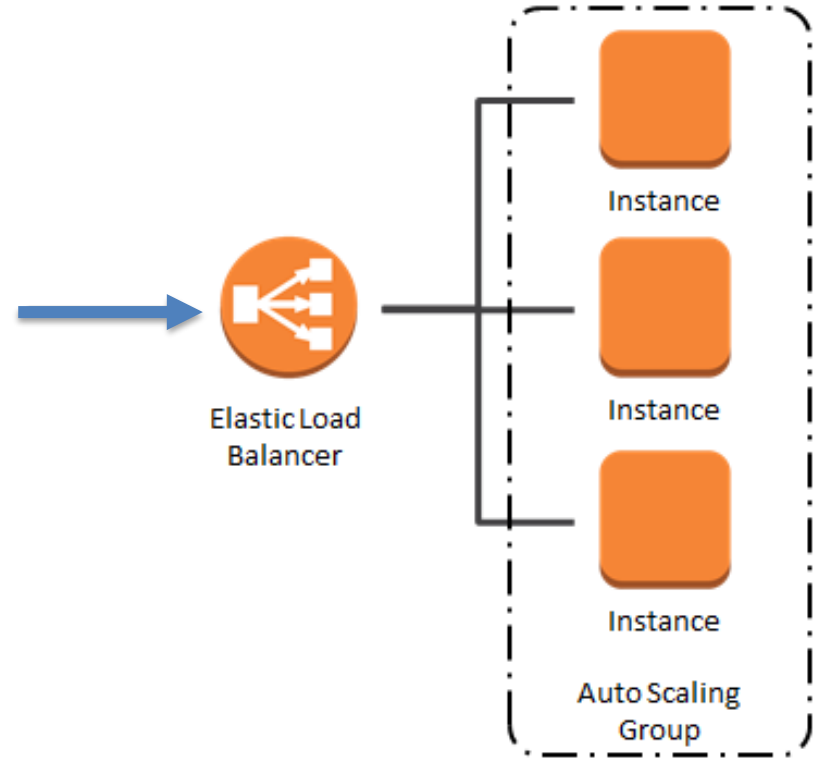
Proxy Services

- A proxy or proxy server is a generic term for a service that acts as an intermediary on behalf of clients and servers
- Man-in-the-middle systems for the following:
 - Translation (NAT, business logic, XML)
 - Authentication and identity services
 - Application Layer Gateways (ALGs)
 - Encryption proxies – can be SSL/TLS accelerators and SSL decryptors as well
 - URL filtering and caching (Web proxy)

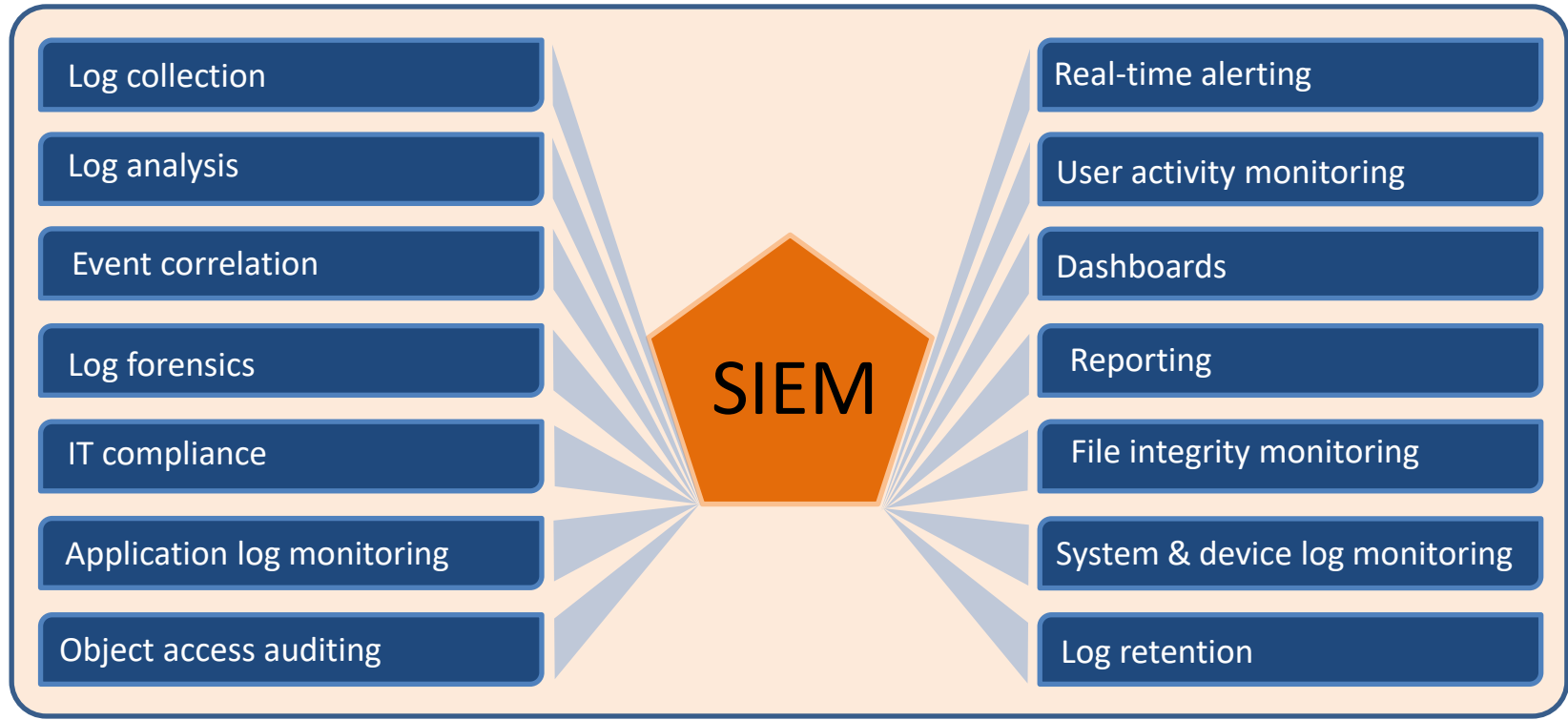


Elastic Load Balancers at CSPs

- Network or Application load balancing
- Represents virtual network to the public
- Performs health checks on instances
- Produces flow logs
- Runs the TLS listener
- Can also have layer 3/4 and web application firewall (WebACL)

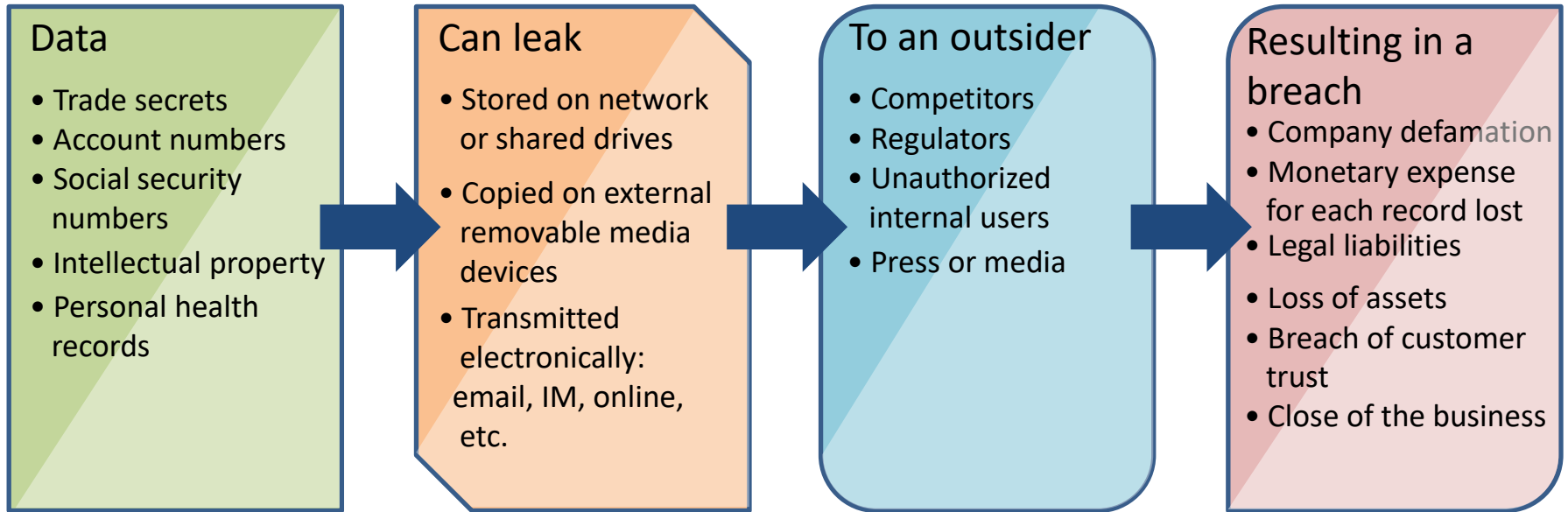


SIEM Systems



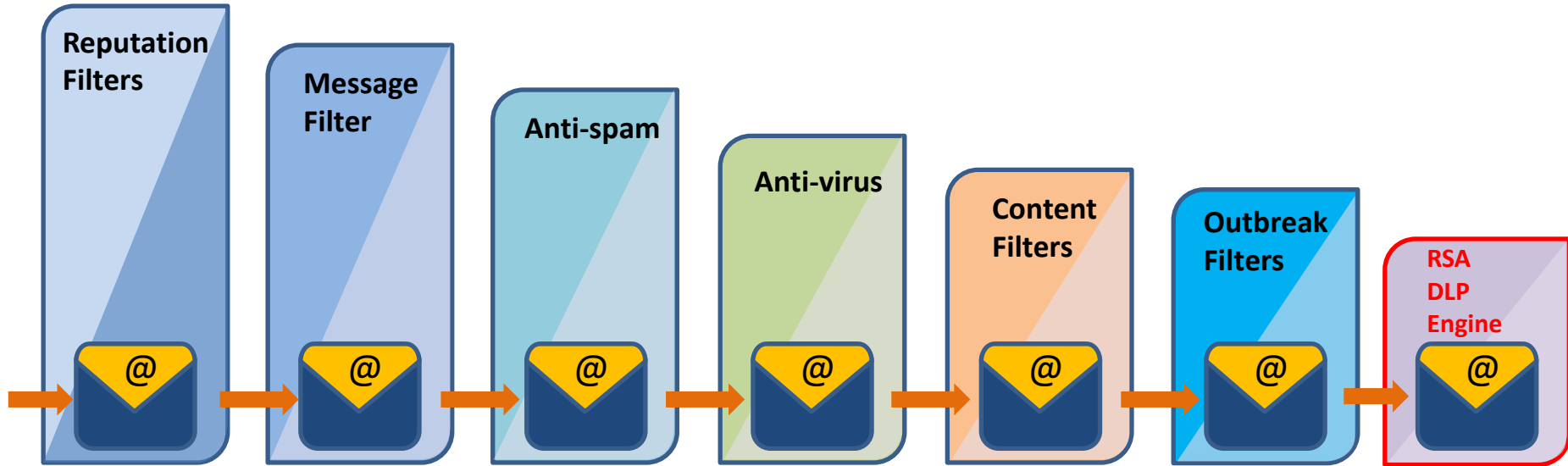
DLP Systems

Can be cloud-based (MSSP), perform USB blocking, and be part of email security solutions



Mail Gateways

Mail Gateway: Outbound Traffic



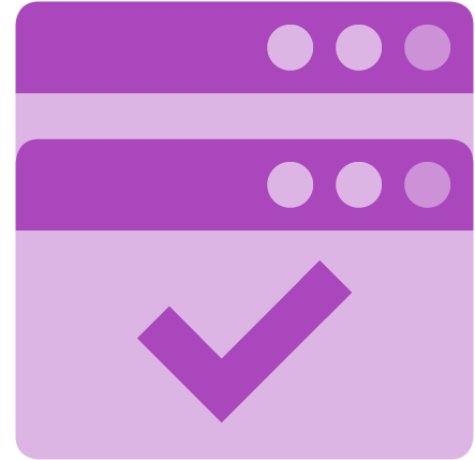
NAC Gateways

- NAC was an industry initiative sponsored by Cisco
- Network Admission Control (NAC) gateway features:
 - Dissolvable vs. permanent
 - Host health checking
 - Agent vs. Agentless
- Replaced by next-gen systems like Cisco ISE, EDR, and MSSPs



File Integrity Checkers

- Can be used in intrusion detection and vulnerability assessments
- Computes a unique hash for every guarded file
- Hash is recomputed in the future
- A different hash means the file has been modified
- Can leverage cloud computing for analysis (machine-learning)

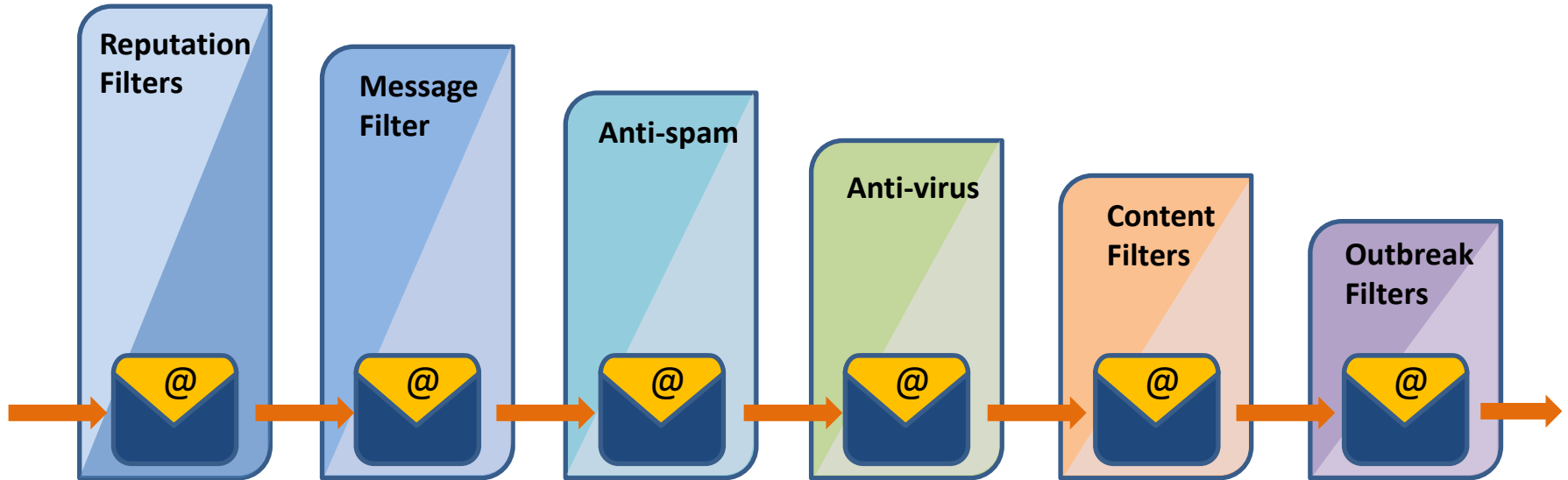


Mail Gateways

- Serve as enterprise-wide message transfer agents (MTAs)
- Control and secure email leaving the organization and entering the organization
- Can perform anti-spam, anti-virus, encryption, DLP, and more
- Physical, virtual, and hybrid solutions
- Example: Cisco Email Security Appliance

Mail Gateways

Mail Gateway: Inbound Traffic



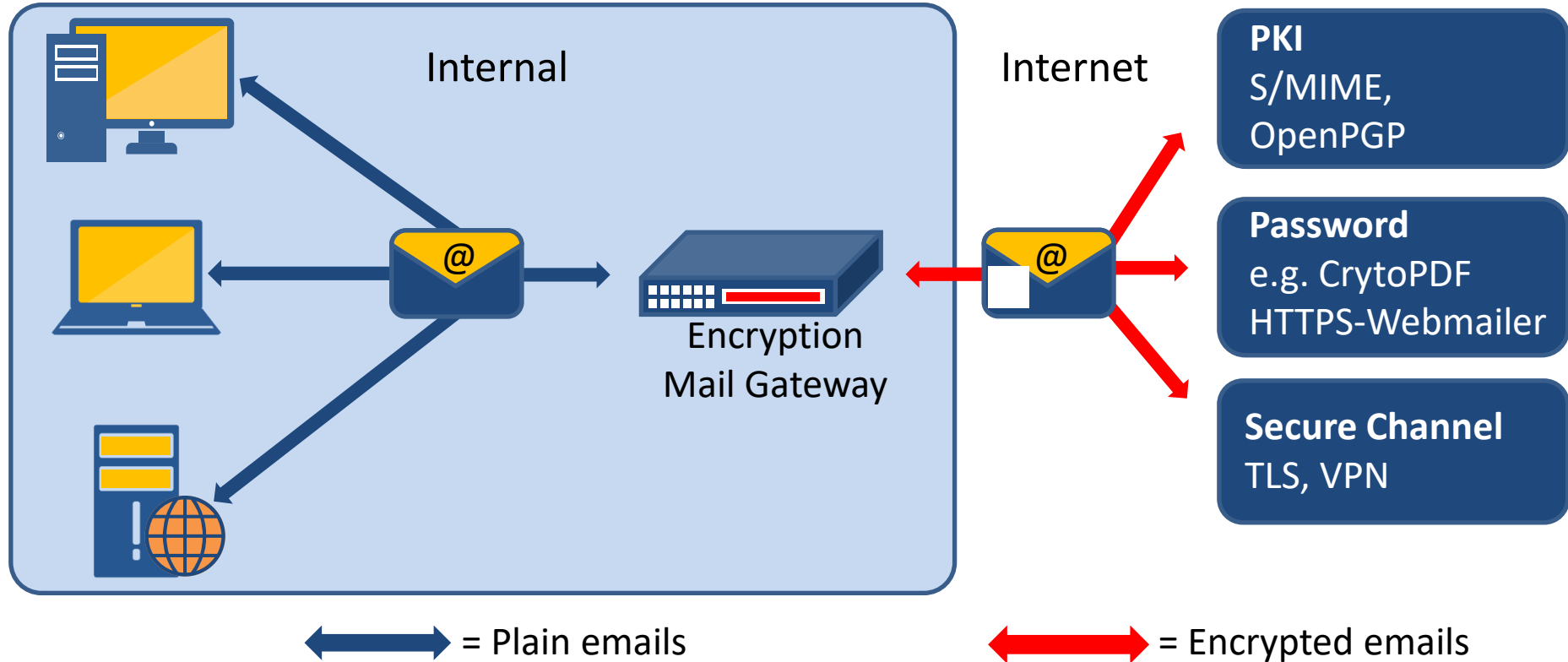
Media Gateways

- Media gateways translate and convert media streams between different technologies such as POTS, SS7, and 3G, 4G, LTE networks and PBX systems
- Media gateways allow multimedia communications across packet-switching networks using protocols like ATM and IP
- Main function is to convert between different transmission and coding techniques, provide echo cancellation, DTMF services, and sending tones

Encryption Gateways

- A wide variety of appliances and devices can decrypt and re-encrypt voice and data as encryption proxies
- SSL/TLS, IPsec, web gateways, email gateways, and authentication proxy services
- VPN gateways will proxy Suite B Cryptography and IKEv2 to TLS and vice versa
- Cloud encryption gateways like Cisco Umbrella and Secure Internet Gateway (SIG) are emerging technologies
- AWS Elastic Load Balancer runs SSL Listener service

Encryption Gateways



Specialty Appliances

- Physical, virtual, hybrid, cloud-based services for all aspects of networking and security
- Integrated Firewalls
- Web Security Appliances
- Hardware Security Modules (HSM)
- Database Activity Monitors
- Endpoint Security

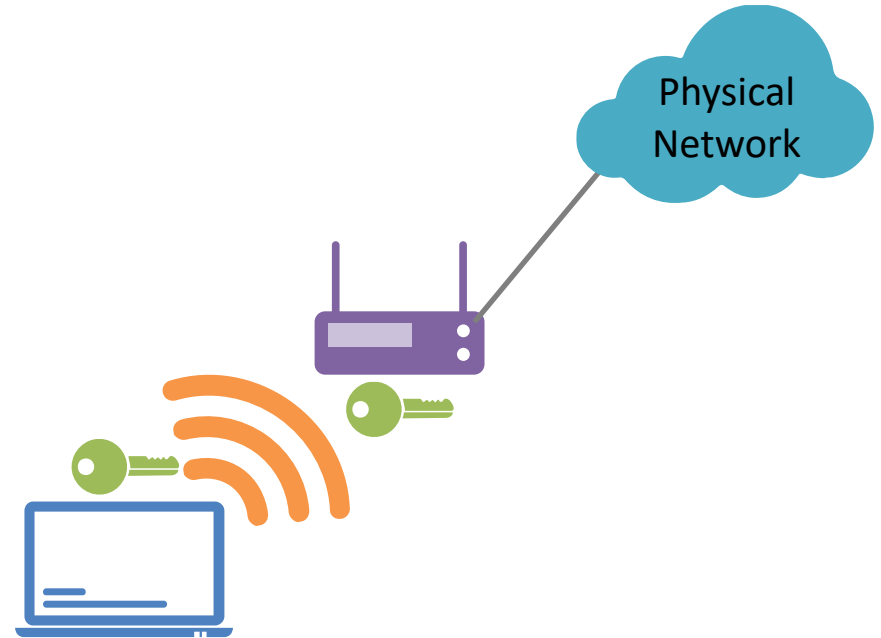


Web Application Firewall (WAF)

- WAFs protect against various types of attacks
 - DoS/DDoS
 - Cross-site scripting
 - Cross-site Request Forgery
 - SQL injection
- Create rules that match based on
 - IP addresses, geography, pattern matching (regex) in URI, 8K into packet, HTTP request headers, heuristics, machine-learning algos
- Rules are then placed into WebACLs

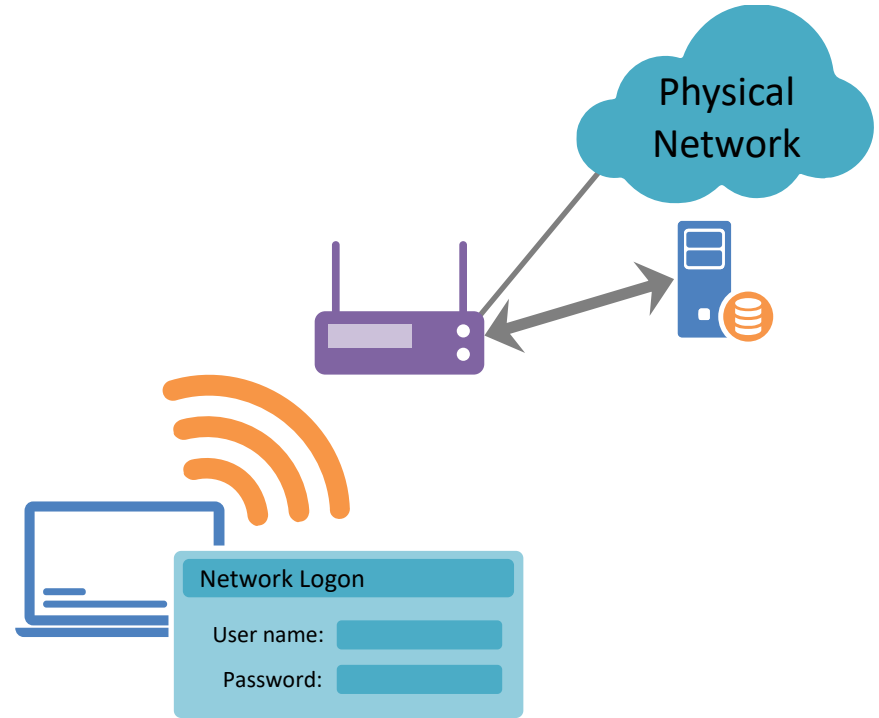
Types of Wireless Networks

- Pre-shared key wireless
 - Also known as personal authentication
 - A pre-shared key is configured (AP and wireless devices)
 - Adds a challenge and a response between client and AP



Types of Wireless Networks

- Enterprise wireless
 - Also known as 802.1x or RADIUS wireless authentication
 - Client provides credentials to AP
 - AP contacts RADIUS server and provides client credentials
 - RADIUS server verifies credentials in database
 - RADIUS server notifies AP if client is allowed
 - AP allows or denies client



WPA and WPA2

- WPA
 - A temporary fix to WEP shortcomings (2003)
 - Uses TKIP for encryption and integrity
 - Supports PSK and Enterprise authentication
 - Deprecated (should not be used)
 - Still available on products for SOHO deployments
- WPA2
 - Replacement for WPA (2004)
 - Devices require testing and certification from Wi-Fi Alliance (2006)
 - Uses CCMP for encryption
 - Supports PSK and Enterprise authentication

WPA and WPA2

- WPA modes

- PSK (personal)

- Shared secret key is used
 - Manually configured on devices and AP
 - Local access controls
 - TKIP used for encryption

- Enterprise (802.1X)

- Authentication server is required
 - RADIUS used for authentication and key distribution
 - Centralized access control
 - TKIP used for encryption

- WPA2 modes

- PSK (personal)

- Shared secret key is used
 - Manually configured on devices and AP
 - Local access controls
 - AES used for encryption

- Enterprise (802.1X)

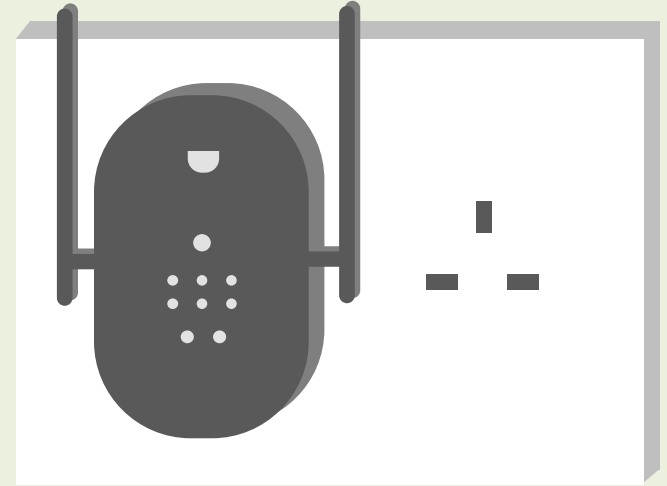
- Authentication server is required
 - RADIUS used for authentication and key distribution
 - Centralized access control
 - AES used for encryption

Wireless Encryption

- CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
 - Based on the AES (Advanced Encryption Standard)
 - Designed as the replacement for WEP and any interim solution (TKIP)
 - Used with WPA2
 - Provides strong message encryption with CCM
 - Provides authenticity and integrity checking with CBC-MAC

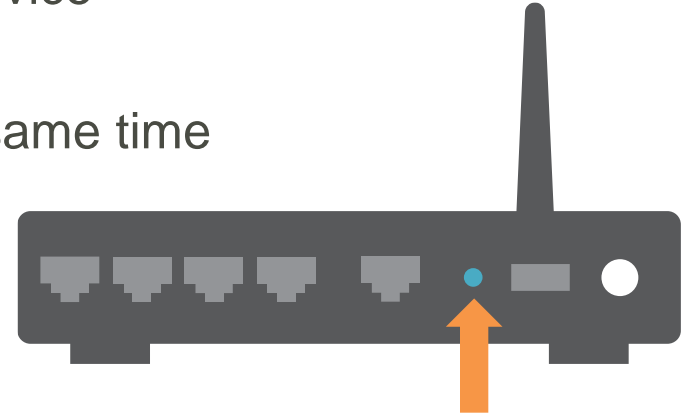
WPS (Wi-Fi Protected Setup)

- Wi-Fi Protected Setup (WPS) is a Wi-Fi Alliance standardized method for simplifying station setup and initial configuration
- WPS was previously called Wi-Fi Simple Config
- Newer wireless routers are less vulnerable



WPS (Wi-Fi Protected Setup)

- PIN
 - A pin number associated with device is entered on AP
 - A pin number generated by AP entered on device
- Push button
 - Physical or virtual on both AP and device at same time
- NFC
 - Device is placed very close to AP to make association
- USB
 - Out-of-band transfer of information between device and AP



Press the Wi-Fi
Protected Setup button

WPS Security Concerns

- Attacks on pin
 - Online and offline brute-force attacks
 - Capture packets to determine pin to gain unauthorized access
 - Pin is printed on device or listed in configuration menu
 - If the device does not allow the pin to be changed, unauthorized access is possible
- Attacks on push button
 - AP is accessible by anyone, just push the button
- WPS is not part of WPA2, and should be avoided and turned off due to many known weaknesses and attacks against it
- WPS should never be used in the enterprise

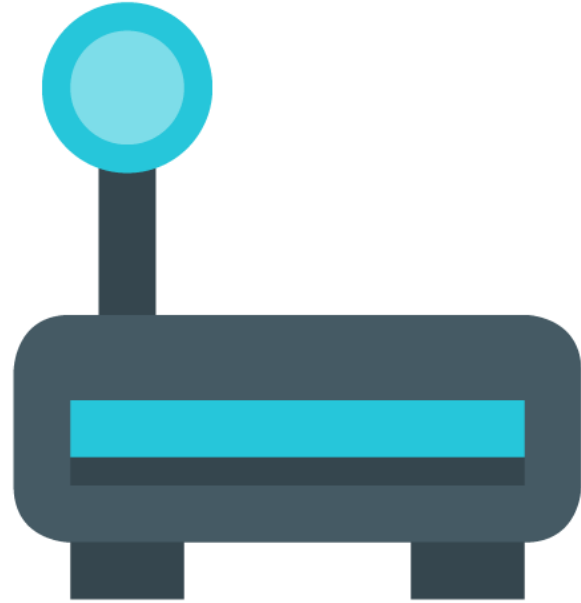
Initialization Vector Weaknesses

- WEP was been deprecated due to the following reason:
 - The initialization vector (IV) is a clear-text 24-bit field – a pseudo-random number used along with the secret key for data encryption
 - The small space guarantees the re-use of the same key stream
 - The weakness is NOT with the RC4 protocol per se



Wireless Replay Attacks

- A cybercriminal eavesdrops on a secure wireless network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the they wants
- Upgrade from WEP or WPA to WPA2/3 as soon as possible

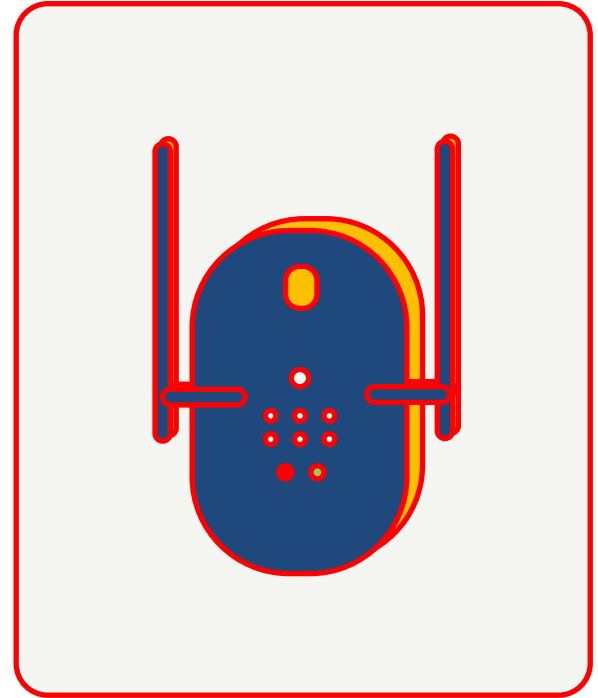


Evil Twins APs

- Malicious rogue APs, used to take sensitive data like usernames, passwords, and PII, fall into two categories: Honeypots and evil twins
- An evil twin AP replaces an existing network so users will connect to the fake one instead of the real one
- Evil twin is described as a wireless man-in-the-middle attack
- Evil twin is similar to a honeypot except that the attacker attempts to appear as the valid network
- Evil twins spoofing a public hotspot can also be a serious concern

Rogue Access Points

- Any wireless AP that has been introduced into a wireless infrastructure without the authorization.
- Can also provide a pivot point through poorly configured intermediate device to the enterprise wired infrastructure
- Rogue APs are often set up by:
 - Employees who want internet access where none is readily available
 - Internal structured attackers
 - Penetration testers
 - Accidental introduction of exploit tools



Jamming

- A form of wireless DoS attack is jamming
- Jamming floods the RF with interference or excessive traffic so that wireless links cannot be sustained
- Exploit kits have several jamming modules and scripts included for hard and soft APs
- Some DoS attacks may not be due to malicious activity, but rather poorly written drivers on endpoint Wireless NICs

Disassociation Attacks

- Wireless clients use control and management frames, such as authentication and deauthentication, association and disassociation, beacons, and probes, to choose an AP and initiate a session for network service
- AP impersonation is a common attack against wireless networks where the attacker spoofs the AP MAC address and sends management frames, usually deauthentication or disassociation messages, to valid clients
- The goal is typically to perform a DoS attack against the network or to force the client to reauthenticate

Management Frame Protection (MFP)

- To keep your Wi-Fi infrastructure safe from attack, you can implement Management Frame Protection (MFP) features
- With client MFP, management frames that are sent between APs and clients are protected, so that both APs and clients can detect and drop invalid or spoofed management frames
- APs can be set up to not emit certain broadcast management frames like disassociation, deauthentication, or action frames

Bluejacking

- Bluejacking is an old Bluetooth prank that sends contact information automatically without authentication or authorization
- The attacker creates an address book object and a contact in the contact list
- They spoof a name to appear on your phone saying they have sent you some contact information and would like you to accept it
- Next, a message says something annoying like "You are bluejacked and I'm taking over your phone"
- Information and data is not being stolen – more of an aggravation

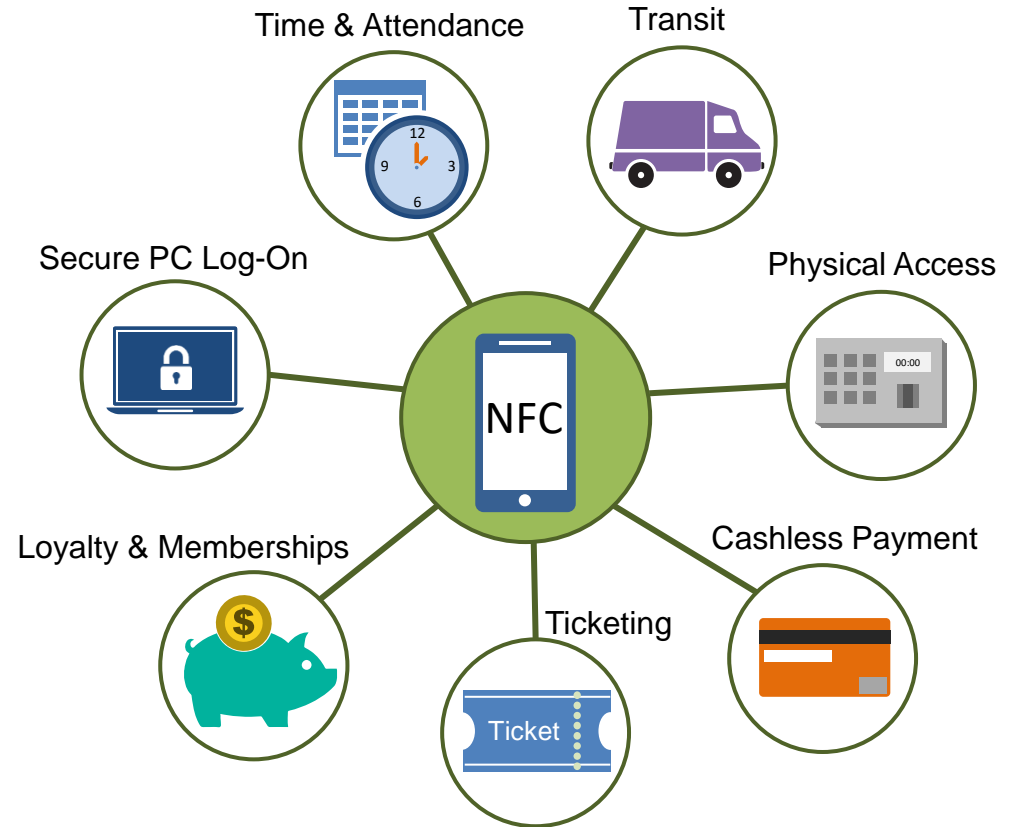
Bluesnarfing

- Bluesnarfing steals data from a wireless device using a Bluetooth connection
- Often between iPhones, Android phones, iPods, iPads, laptops, and assorted PDAs
- Can access contact lists, calendars, emails, and text messages
- Any device with Bluetooth enabled and set to "discoverable" is vulnerable to attack
 - Turning off this feature is one simple countermeasure to bluesnarfing



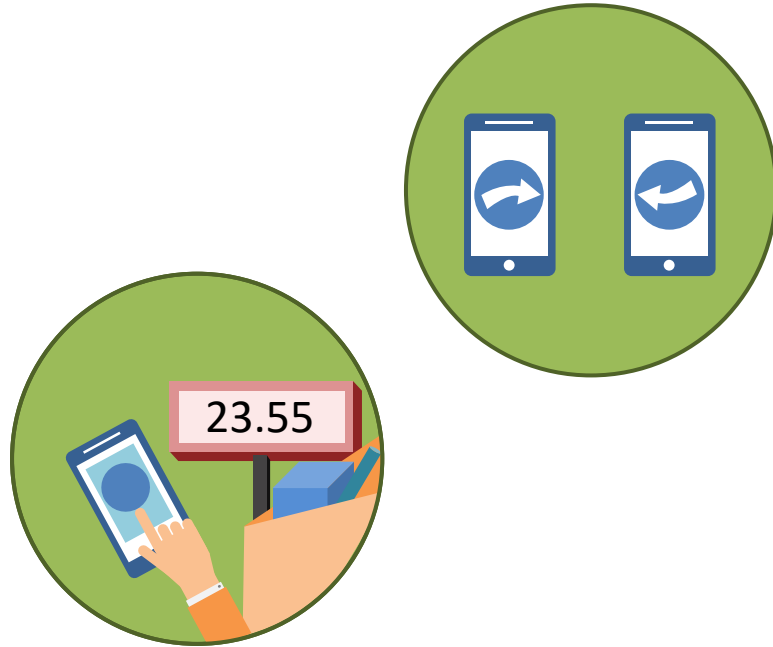
RFID and Near Field Communication (NFC)

- The benefits of rapid and contactless payments and entry/exit without long waiting times are very tempting
- The benefits of RFID/NFC for travelers and shoppers are numerous, and the tech is here to stay



RFID and Near Field Communication (NFC)

- Sniffing, spoofing, and replay
- Man-in-the-middle attacks
- Cloning and emulation
- Denial of service
- Jammer system
- Blocker tags
- RFID zapper
- Tracking
- Relay attacks
- RFID malware



Survey of Connection Methods

- Cellular technology
 - Involves having many small inter-connected transmitters instead of one large one
 - A multiple access technology where multiple voice or data connections are placed into a single radio channel
 - The major enhancements of 4G is mobile broadband Internet services offered to laptops, wireless modems, etc.
 - 5G is not mentioned on the exam
- Wi-Fi is the commercial implementation of 802.11b/g/n/ac
- SATCOM is satellite telephone or "satphone"
 - Links to orbiting satellites instead of ground-based cell towers, while providing similar services

Survey of Connection Methods

- Bluetooth
 - Method of creating personal area networks (PAN) with many applications
 - Both a radio-frequency standard UHF in the 2.4 to 2.485 GHz ISM and an agreement protocol
 - Bluetooth delivers confidentiality, authentication, and key generation with custom algorithms based on the SAFER+ block cipher
- NFC
 - ISO/IEC 14443 defines the ID cards used to store information, such as that found in NFC tags
 - ISO/IEC 18000-3 specifies the RFID communication used by NFC devices
 - 18000-3 is an international standard for all devices communicating wirelessly at the 13.56MHz frequency using Type A or Type B cards



Survey of Connection Methods

- Infrared - there are two types of infrared communication:
 - **Point-to-point**: needs a line of sight between the transmitter and a receiver as in remote control communication
 - **Diffuse**: does not require line of sight and the link between the transmitter and the receiver is preserved by reflection off surface's wireless LAN communication system
 - Transmitting IR data between devices is also called beaming
- Wireless USB - a high-bandwidth wireless radio communication PAN protocol
 - IPv6 is integrated into this technology
 - Maintained by the WiMedia Alliance and is sometimes abbreviated as "WUSB"

Survey of Connection Methods

- ANT
 - A proprietary ultra-low-power, short-range wireless technology (like Bluetooth) designed for sensor networks and comparable applications
 - Also uses the 2.4-GHz ISM band
 - Primary use is in sports and fitness to deploy PANs for performance and health monitoring
 - ANT+ facilitates the collection, automatic transmission, and tracking of sensor data for monitoring various devices

Mobile Deployment Models

- BYOD – bring your own device
- COPE – corporate owned, personally enabled
- CYOD – choose your own device
- Corporate-owned



Mobile Deployment Models

- VDI for mobility devices
 - Challenge is to manage a disparate collection of mobile OSs, versions, apps, and updates
 - VDI separates the device from the app and data, which is stored on managed (MDM) corporate virtual servers
 - Can lower IT management cost and complexity, enhance data security, offer device agility, and improve device uptime
 - Common and popular use for mobile VDI sessions is with tablets using a separate Bluetooth-enabled keyboard

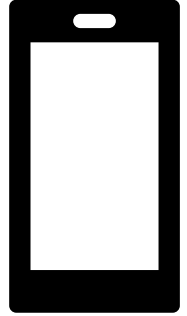
Enterprise Mobility Management

- Organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, O/S, management agent, and the apps used
- Solutions should reduce risk so employees are able to access the necessary data from nearly any location, over any network, using a wide variety of mobile devices
- EMM = MDM + MAM



MDM vs. MAM

- MDM often involves
 - Enrolling devices for management
 - Provisioning settings like digital certificates and profiles
 - Monitoring, measuring, and reporting device compliance
 - Removing corporate data from devices (data leak prevention)
- MAM often involves
 - Publishing mobile apps to users
 - Configuring and updating apps
 - Reporting app inventory and usage
 - Securing and removing corporate data within mobile apps



Mobile Content Management

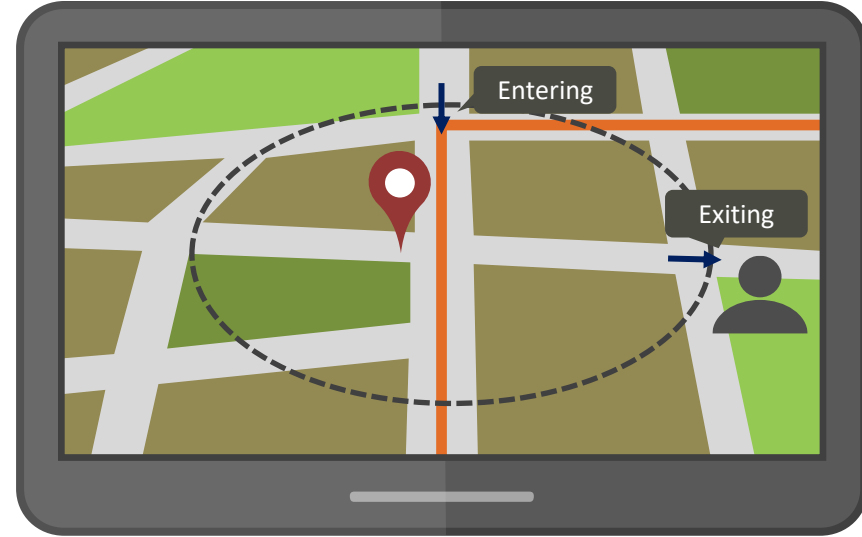
- Automatically publish important documents and media to employee devices
- Use mobile content security controls to prevent unauthorized sharing and enforce DLP policies
- Permit IT to remotely wipe data if the device doesn't comply with corporate security policies
- Leverage FIPS 140-2 validated encryption to protect content stored on mobile devices

Remote Wipe

- Allows administrator or owner of mobile device to send a command that deletes data and apps
- Depends on OS and MDM capabilities
- Remote wipe abilities are offered natively in the enterprise, on most devices using something like Exchange ActiveSync
- If an iOS device, Apple Watch, or Mac is lost or stolen, if you set up "Find My iPhone" you can erase it as well
- Some allow for select wipe of folders and others perform a complete wipe of the device and can reload from the cloud

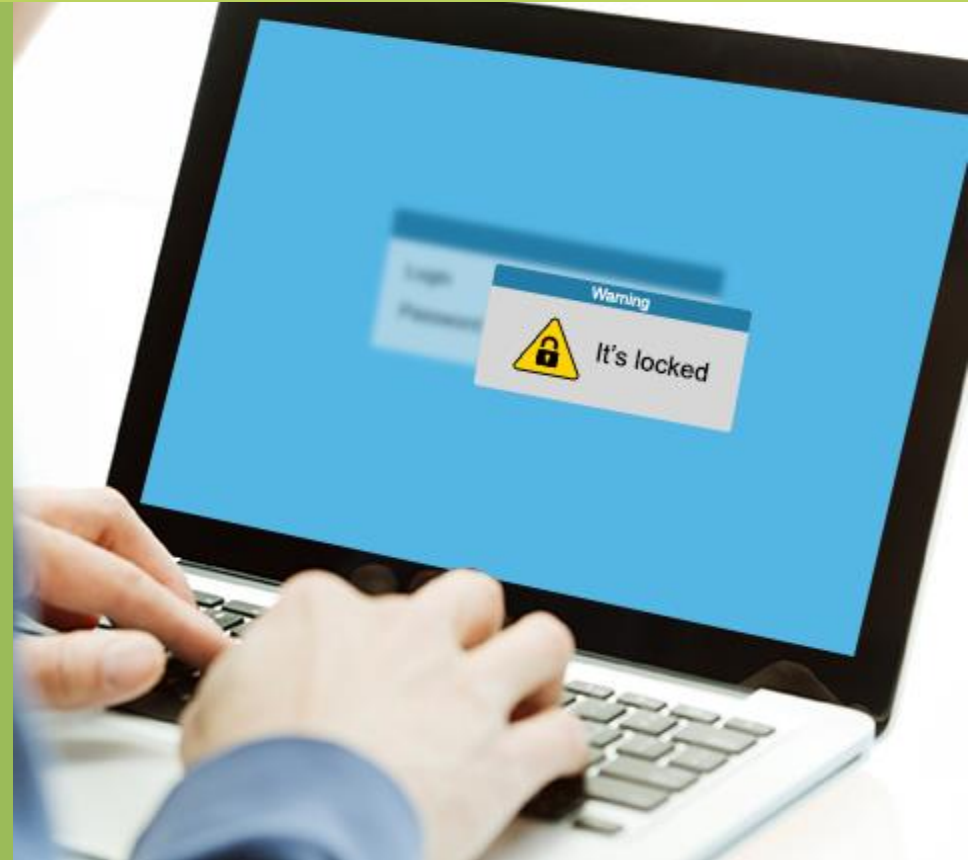
Mobility Security and Privacy Concerns

- Geofencing and geolocation services allow IT to physically track mobile devices
- Geolocation is a point on a map whereas geofencing is a square area on the map
- Administrators can use geolocation to find a lost or stolen device and geofencing can determine when a device moves in and out of a certain (secure) area
- Mobile device management (MDM) systems have added these features for the enterprise



Passwords, Pins, and Screen locks

- Fingerprint lock
- Face lock
- Swipe lock
- Passcode lock



Push Notification Services

- Originally allowed the server to push mail, calendar, and contacts services to network users
- Today services like Amazon Simple Notification Service (Amazon SNS) lets you send individual messages or amplify messages to many recipients
- SNS is a cost-effective way to send push notifications to mobile device users, email recipients, or other distributed services
- Can send notifications to Apple, Google, Fire OS, and Windows devices, as well as SMS messages to mobile device users worldwide
- Can directly access using iOS, Android, Java, Python, PHP, Node.js, or .NET SDKs

Biometrics and Context-aware Authentication

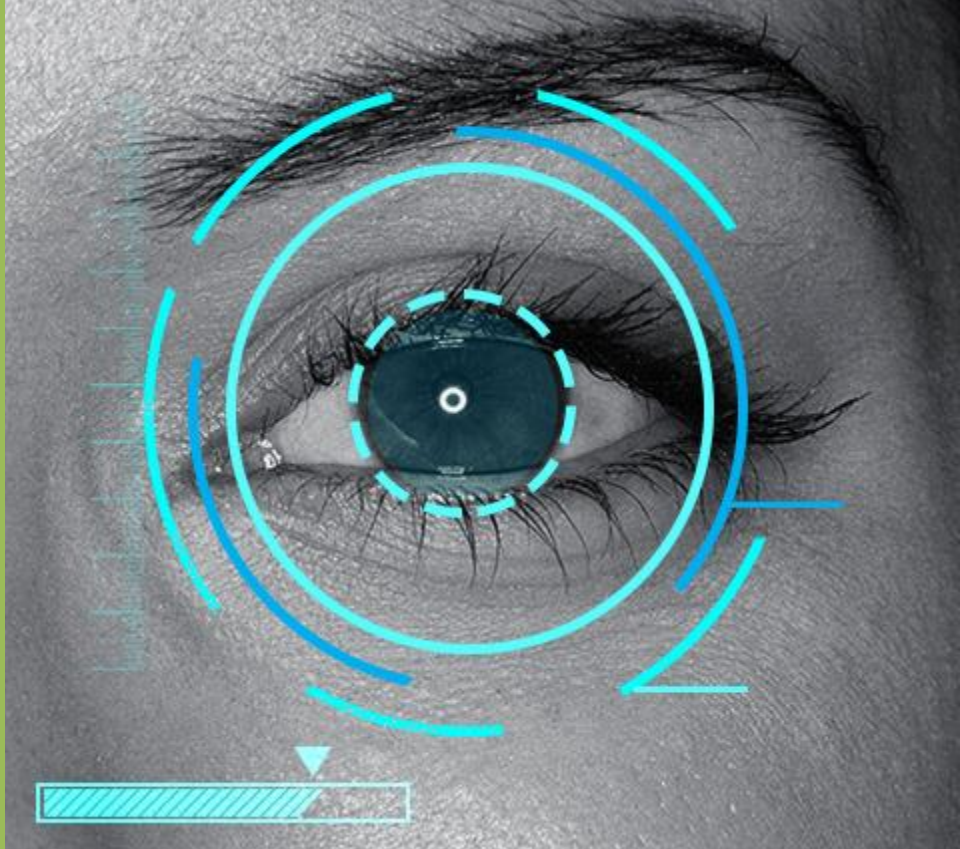
- Biometrics

- Fingerprint readers
- Facial recognition scanners
- Biometric fusion combines face and fingerprint
- Iris recognition
- Behavioral biometrics
 - Swipe patterns



Context-aware Authentication

- Applications include:
 - Multifactor authentication
 - Mobile payments
 - Online banking
 - Immigration services
 - eGovernment
 - Workforce management
 - Healthcare
 - Point of Sale
 - IoT (wearable)



Containerization and Storage Segmentation

- Containerization involves tools that create a separate, encrypted zone or policy area on a user's device where certain (or all) corporate apps and data reside
- Policy controls apply only to the container contents instead of the whole device
- Containerization divides personal and business apps with their associated data to enforce separation at the app level combined with data encryption
- Often offers securely containerized business productivity apps with micro VPN access to organizational resources from BYOD smartphones and tablets
- Tools often function with MDM enterprise software

Full Device Encryption

- Full disk encryption (FDE) is commonly deployed on desktop and mobile devices
- It helps secure vital data and thwarts breaches by encrypting all of the data at rest in storage
- Some products are standalone; some are bundled with other security software; some are built in to operating systems like Microsoft BitLocker and Apple FileVault
- FDE software for mobility should have its own authentication mechanisms or leverage enterprise MFA, such as smart cards, cryptographic tokens, or Active Directory

Rooting

- Rooting grants full access to a device on a level much higher than jailbreaking, giving access to the Android system and beyond
- Every line of code in the Linux-based device becomes editable, with options only restricted by coding skills
- Since Android is open source, you can go into recovery mode and download a modified or even entirely new version of the OS if you want
- You can alter any and all hardware, software, or aesthetic settings on the device

Jailbreaking

- Jailbreaking and rooting are very different, even though they both involve privilege escalation
- Jailbreaking an iPhone basically allows the installation of third-party apps not approved by Apple's strict controls
- Key Raider malware (2015) and a semi-untethered Phoenix tool were released (2017) to jailbreak iOS 9.3.5 on 32-bit devices
- Apple has responded with patching exploits and upgrading hardware to iOS

Sideloading

- Basically refers to the moving of media files to a mobile device using USB, Bluetooth, or Wi-Fi
 - Also, writing to a memory card to insert into a mobile device
- With Android apps, sideloading usually installs an app package in APK format onto a device, with packages typically downloaded from sites other than Google Play
- Sideloaded apps are only likely if the user has allowed "Unknown Sources" in their security settings

Custom Firmware

- Over-the-air (OTA) updates are the wireless delivery of new software (or data) to mobile devices
- Wireless carriers have customarily used OTA updates to deploy firmware and configure phones for use on their networks
 - The initialization of a newly purchased phone, for example, requires an over-the-air update
- Carriers and manufacturers are also using OTA updates for deploying new operating systems to mobile devices
- Firmware updates need to be part of the mobile policy (MDM) as to how and when it is done



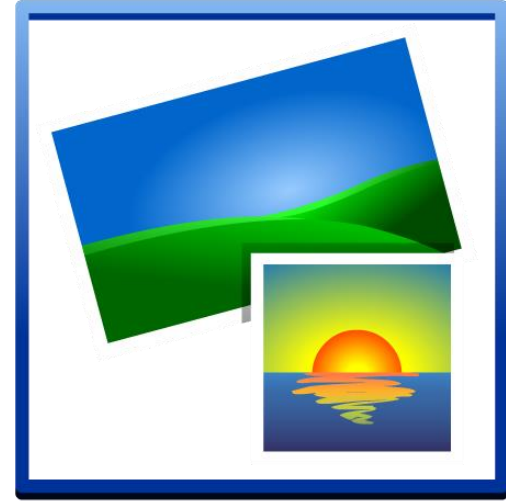
Carrier Unlocking

- Carrier unlocking removes a carrier's SIM restrictions on an iPhone, which will allow you to use other carriers' SIM cards in your iPhone
- Check with your carrier about any other specific circumstances you have
- Plenty of companies will sell you stock unlock codes for your phone thereby circumventing current restrictions by operating in countries not covered by US law
- Unlock Radar is a well-reviewed choice
 - Sometimes it is necessary, if you are a member of the armed forces and are soon traveling overseas, carriers must unlock your phone on request



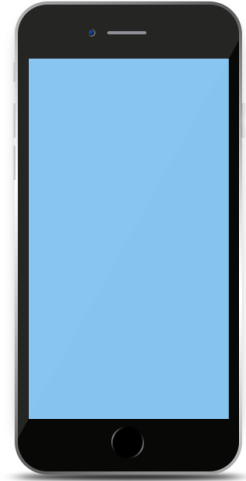
Mobile Camera Use

- Should be part of the mobile section of the AUP for all employees
- Can be part of an over-the-shoulder reconnaissance attack
- Camera use and recording should be forbidden in sensitive areas or throughout the campus
- Use EMM to disable this feature on all onboarded devices in enterprise



Enforcement and Monitoring

- SMS (Short Message Service) and MMS (Multimedia Messaging Service) are used in mobile phones to allow for the sending and receiving of data messages
- External media may also be controlled with AUP
- USB OTG mini-plugs allow connection to a wide variety of external receptacles – DLP problems



Enforcement and Monitoring

- Wi-Fi Direct - allows two devices to establish a direct, peer-to-peer Wi-Fi connection without requiring a wireless router
- Becomes a way of communicating wirelessly, like Bluetooth
- Similar in concept to an "ad-hoc" Wi-Fi mode SSID
- Wi-Fi Direct includes an easier way to automatically discover nearby devices and connect to them
 - You don't have to go through many set-up procedures



Enforcement and Monitoring

- Tethering
 - Using device as a wireless
- Spectrum management
 - New bandwidths opening up
- Unauthorized domain bridging
 - Regular patches and updates on wireless devices to prevent bridging and tethering from others



Tokenization and Mobile Payment Concerns

- Tokenization
 - Used for mobile payments and multifactor authentication (MFA)
- Mobile payments
- Near-field communication (NFC) enabled
- Mobile wallet and cybercurrency wallets
- Peripheral-enabled payments (credit card reader)

