**Introduction**

**Vulnerability** - a weakness that might allow an attack to take place.

**Threat** - a force that may exploit a vulnerability.

**Risk** - combination of threat and vulnerability.

**Types of threats:**

* **Adversarial** - deliberately undermine the security of an organization
* **Accidental** - mistakenly undermine the security of an organization.
* **Structural** - failure due to exhaustion of resources, exceeding operational capability or due to age.
* **Environmental** - disasters occurring outside organizational control, both man-made and natural.

**NIST SP 800-30 Risk Assessment**

1. Prepare for assessment
2. Conduct Assessment
   1. Identify threat sources and events
   2. Identify vulnerabilities and predisposing conditions
   3. Determine likelihood of occurrence
   4. Determine magnitude of impact
   5. Determine risk
3. Communicate Results
4. Maintain Assessment

**Qualitative Risk Assessment**

Threats are given a subjective (low, medium, high) rating for their likelihood and impact. Combination of likelihood and impact determines risk. (low, medium, high) Usually displayed as a matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | High | Medium | High | High |
| **Likelihood** | Medium | Low | Medium | High |
|  | Low | Low | Low | Medium |
|  |  | Low | Medium | High |
|  |  |  | **Impact** |  |

**Risk Management**

* Risk Acceptance
* Risk Avoidance
* Risk Mitigation
* Risk Transference

**Types of security controls**

* **Technical** - systems, devices, software and settings that work to enforce CIA requirements.
* **Operational** - practices and procedures that bolster security.

**Building a Secure Network**

**Network Access Control**

**802.1x** - common standard used for NAC. When a device tries to gain access, it is challenged to authenticate using 802.1x.

* **Supplicant** - software on the client device permitting it to authenticate with the network.
* **Authenticator** - software on the switch or access point that passes access requests to the authentication server (like RADIUS) and grants or denies access based on its response.

**Agent-Based** NAC solutions (like 802.1x) require the client to run a supplicant in order to be able to connect to the network.

**Agentless** NAC solutions conduct authentication in the web browser.

**In-band (inline)** NAC solutions run dedicated appliances sitting between devices and resources clients might wish to access. Example: captive portal at a hotel network.

**Out-of-Band** NAC solutions (like 802.1x) use existing network infrastructure to grant or deny access to clients based on their success with the authentication server.

**NAC Admission Criteria**

**Time of day** - certain hours might be off-limits.

**Role** - only certain groups can access certain resources.

**Location** - certain physical locations may be off-limits.

**System Health** - devices that fail to meet minimum security standards might be denied access.

**Firewalls**

**DMZ** - a network zone designed to house systems that receive connections from the outside world (e.g web servers, mail servers, etc)

**Triple-homed** firewall connects to the internet, the internal network and the DMZ.

**Packet Filtering** firewalls check packet characteristics against an ACL. Most rudimentary form of firewall.

**Stateful inspection** firewalls maintain information about the state of each connection. Most basic type sold as an appliance.

**Next-Generation** firewalls use contextual information to make decisions about denying or granting access.

**Web Application** firewalls protect against web application attacks.

**Common TCP ports**

|  |  |
| --- | --- |
| **20, 21** | *FTP* |
| **22** | *SSH* |
| **23** | *Telnet* |
| **25** | *SMTP* |
| **53** | *DNS* |
| **69** | *TFTP* |
| **80** | *HTTP* |
| **110** | *POP3* |
| **123** | *NTP* |
| **143** | *IMAP* |
| **161** | *SNMP* |
| **389** | *LDAP* |
| **443** | *HTTPS* |
| **514** | *Syslog* |
| **1433** | *Microsoft SQL Server* |
| **1521** | *Oracle* |
| **1720** | *H.323* |
| **1723** | *PPTP* |
| **3389** | *RDP* |
| **3306** | *MySQL* |

**Network Segmentation** separates networks from being able to directly communicate with one another.

A **jump-box** may be connected to remotely via SSH or RDP for the administration of a sensitive network.

**Honeypot** is bait for attackers, posing as a vulnerable system.

**DNS Sinkhole** hijacks communication from malware meant for the command and control server.

**Secure Endpoint Management**

**SCCM** - System Center Configuration Manager. Microsoft’s patch management software that can be used to distribute and monitor the patch status of an organization.

**GPO** - Group Policy Object. Microsoft’s mechanism for defining security settings for groups of users or systems.

**MAC** - Mandatory Access Control. Administrators set file permissions and users cannot modify them. Example: NSA’s SE Linux.

**DAC** - Discretionary Access Control. File owners control permissions and can change them at their discretion.

**Penetration Testing**

**NIST 800-115 Penetration Testing Phases**

1. Planning
2. Discovery
3. Attack (and additional discovery)
4. Reporting

**Penetration test planning should take into account:**

* Timing
* Scope
* Authorization

**NIST Attack Phase Steps**

1. Gaining Access
2. Escalating Privileges
3. System Browsing (back to discovery phase)
4. Installing Additional Tools

**Reverse Engineering**

**Decomposition** - philosophy where the reverse engineer starts with the finished product and works his way back to its component parts.

**Code detonation** - suspicious code is automatically sandboxed and monitored for signs of malicious behavior.

**Disassembly** - from machine code to Assembly

**Decompilation** - from machine code to an educated guess at the source code

**Starting Byte Sequences:**

* **Windows**: 5A 4D/4D 5A
* **Linux**: 7F 45 4C 46

**Reconnaissance and Intelligence Gathering**

**Footprinting**

**OSSTMM** - Open Source Security Testing Methodology Manual

**Active reconnaissance**

Uses scanning tools to gather information about systems and networks.

**Things that reveal the topology of a network:**

* Response packet TTL(time to live)
* Traceroute information
* Responses of network and security devices

Firewalls and Security Appliances can stop scan traffic resulting in **incorrect data and** **missing systems or networks**

**Port scanners** have the following features:

* Host discovery
* Port scanning and service identification
* Service version identification
* Operating system identification

**Ports** from 0 to 1023 are **well-known**.

**Ports** from 1024 to 49151 are **registered** with IANA(Internet Assigned Numbers Authority)

**NMAP**

Scans 1000 common ports by default.

Has an official graphical interface - **Zenmap**

**NMAP Flags:**

* -P0 tells NMAP to skip pinging
* -sS tells NMAP to do a TCP SYN scan
* -O tells NMAP to identify operating systems
* -sV tells NMAP to identify service versions by grabbing banners and other means

**Other software with port scanning functionality:**

* Angry IP Scanner
* Metasploit
* Qualys Vulnerability Management Platform
* Nessus

**Operating System Fingerprinting** is done by comparing TCP and UDP responses to packets sent to remote systems (**TCP/IP stack fingerprinting**)

**Passive Reconnaissance**

Is done via packet capture and log/configuration analysis.

**Cisco’s Log Levels**

|  |  |  |
| --- | --- | --- |
| **Level** | **Level Name** | **Example** |
| 0 | Emergency | Device shutdown/failure |
| 1 | Alerts | Temperature limit exceeded |
| 2 | Critical | Software Failure |
| 3 | Errors | Interface down |
| 4 | Warning | Config Change |
| 5 | Notifications | Line up/down |
| 6 | Information | ACL Violations |
| 7 | Debugging | Debug messages |

**Cisco Router logs** can be shown with the *show logging* command.

**Netflow** data consists of IP and port source and destination for traffic. Netflow is a Cisco protocol.

**Similar protocols:**

* Juniper’s Jflow and cflowd
* Citrix’s AppFlow
* HP’s NetStream
* sFlow - sampled flow

**Netstat** - utility for displaying local host network information on Windows, Linux and MacOS.

**Netstat flags:**

* -ta shows active TCP connections
* -u shows active UDP connections
* -w shows RAW
* -X shows Unix socket connections
* -o shows process IDs for connections
* -e provides interface statistics
* -nr shows the routing table
* -ano shows sockets belonging to processes
* -v does the same in Mac OS
* -nap does the same in Linux

**Nbtstat flags:**

* -c displays the name cache, names resolved to IP’s
* -n displays names on the local system
* -R purges the remote cache name table
* -r shows the number of names resolved
* -s shows the current sessions
* -S shows sessions table with destination IP’s

**Net command on Windows:**

* Net use - lists network shares a device uses
* Net user - shows local user accounts
* Net group - domain controller command
* Net config - allows services to be controlled

**DHCP logs** for Linux are typically found in **/var/log/dhcpd.log** or with a ***journalctl*** command.

**DHCP configuration** is stored in **dhcp.conf.**

**Windows logs:**

* **Application logs** - events logged by programs.
* **Security logs** - login events, rights usage, files opened, created, deleted.
* **Setup logs** - created when an application is set up.
* **System logs** - events logged by Windows components.
* **ForwardedEvent logs** - events collected from remote computers.

**DNS lookup** on Windows, Linux and MacOS is done via ***nslookup***. First parameter is the website, second is the DNS server.

Specific DNS records can be looked up with the **-query** flag. *-query=MX/NS/SOA/ANY*

**Registrars** - organizations that manage domain names and are an interface between customers and registries.

Registrars are accredited by generic top-level domain (**gTLD**) registries or country-code top level-domain (**ccTLD**) registries.

**IANA** - Internet Assigned Numbers Authority that manages the global IP address space. It also manages the DNS root zone that assigns gTLDs and ccTLDs.

IANA is divided into 5 **regional Internet registries(RIRs)**:

* **AFRINIC** - *African Network Information Center*
* **ARIN** - *American Registry for Internet Numbers*. The US, Canada, parts of Carribean and Antarctica
* **APNIC** - *Asia-Pacific Network Information Centre*. Asia, Australia, NZ.
* **LACNIC** - *Latin America and Carribean Network Information Centre*
* **RIPE NCC** - *Reseaux IP Europeens Network Coordination Centre*. Central Asia, Europe, Middle East, Russia.

**Zone transfer** - DNS database replication.

To check for zone transfer of a DNS server, do:

* host -t axfr domain.name dns-server
* dig axfr @dns-server domain.name

**SOA** - Start of Authority. Top part of the zone transfer with the names of primary and secondary servers, as well as a contact for them.

Linux **host** command will return information about a system’s IPV4 and IPV6 addresses as well as email servers.

Services like **domainhistory.net** provide a **historical view** of domain registration information.

**Organizational Intelligence**

**theHarvester** gathers emails, domain information, hostnames, employee names, open ports and banners using search engines.

**Vulnerability Management**

**HIPAA -** Health Insurance Portability and Accountability Act.

**Gramm-Leach-Bliley Act (GLBA)** - regulates financial institutions.

**PCI DSS** - regulates merchants who handle credit cards.

* Organizations must run internal and external vulnerability scans
* Scans must be quarterly and after a significant change in a network
* Internal Scans need to be done by qualified personnel
* External scans must be done by approved scanning vendors

**FISMA** - Federal Information Security Management Act that regulates government agencies.

* Mandatory scans in systems and applications, as well as when vulnerabilities are reported
* Mandatory to automate parts of vulnerability management by using standards
* Mandatory scan report and assessment analysis
* Mandatory remediation of legitimate vulnerabilities according to risk assessment
* Mandatory sharing of information obtained from the above process

**NIST 800-53 Requirements for Federal Systems:**

1. Employ scanning tools that are updated for new vulnerabilities
2. Update the list of new vulnerabilities prior to a scan
3. Employ scanner that identifies the scope of a scan
4. Determine what info about a system is discoverable by attackers and take corrective action
5. Give scanners privileged access
6. Automate for trend analysis of vulnerability scan reports
7. Review historic logs to determine if a vulnerability has been exploited
8. Correlate output from scanning tools to determine if multiple vulnerabilities are being exploited

For **moderate** impact systems employ **1, 2 and 5 minimum**

For **high** impact systems employ **1, 2, 4 and 5 minimum**

**FISMA Impact Metrics:**

**Low** - limited adverse effect on operations, assets and individuals.

**Moderate** - serious adverse effect on operations, assets and individuals.

**High** - catastrophic or severe effect on operations, assets and individuals.

**SCAP** - Security Content Automation Protocol. Standardized approach to communicating security information led by NIST.

**CCE** - **Common Configuration Enumeration** provides standard names for discussing configuration issues.

**CPE** - **Common Platform Enumeration** provides standards for describing product names and versions.

**CVE** - **Common Vulnerabilities and Exposures** provides a standard for describing security-related software flaws.

**CVSS** - **Common Vulnerability Scoring System** provides standards for measuring severity of flaws.

**XCCDF** - **Extensible Configuration Checklist Description Format** is a language for specifying checklists and their results.

**OVAL** - **Open Vulnerability and Assessment Language** is the language for specifying low-level test procedures used by checklists.

**Reading CVSSv2 Scores**:

Example: **CVSS2**#**AV**:N/**AC**:M/**Au**:N/**C**:P/**I**:N/**A**:N

**AV** - **Access Vector**

* **L - Local. Attacker** must have physical or logical access to the system.
* **A - Adjacent Network**. Attacker must have access to the local network
* **N - Network**. An attacker can exploit remotely over a network.

**AC - Access Complexity**

* **H - High**. Exploitation requires special conditions that would be hard to find.
* **M - Medium**. Exploitation requires somewhat special conditions
* **L - Low**. Exploitation doesn’t require any special conditions.

**Au - Authentication**

* **M - Multiple.** Attacker needs to authenticate two or more times
* **S - Single**. Attacker needs to authenticate once
* **N - None**. No authentication required.

**C - Confidentiality**

* **N - None**. No confidentiality impact.
* **P - Partial.** Access to some information is possible. No control over what information.
* **C - Complete**. All information on the system is compromised.

**I - Integrity**

* **N - None**. No integrity impact.
* **P - Partial**. Modification of some info is possible, but no control over which.
* **C - Complete**. Integrity is completely compromised.

**A - Availability**

* **N - None.** No availability impact.
* **P - Partial**. Performance of the system is degraded.
* **C - Complete**. System is completely shut down.

**CVSS Risk Categories:**

* Below 4 - **Low**
* 4 to 6 - **Medium**
* 6 to 9 - **High**
* 10 - **Critical**

**Incident Response**

Adverse event - Any event that has negative consequences.

Security Incident - violation or imminent threat of violation of security policies and practices.

CSIRT - Computer Security Incident Response Team.

**Scope of impact** - determination of whether an event is enough of a deviation from normal operations to be called an incident and the degree to which services were affected.

**MTD** - Maximum Tolerable Downtime. Maximum acceptable downtime.

**KPI** - Key Performance Indicators

**RTO** - Recovery Time Objective. Acceptable Downtime.

**Phases of Incident Response NIST 800-61**

1. Preparation
2. Detection & Analysis
3. Containment, Eradication and Recovery
4. Post-Incident activity

**NIST Recommends to have the following for incident response:**

* Digital Forensics Workstation
* Backup Device
* Laptops for collection, analysis and reporting
* Spare server and networking equipment
* Blank removable media
* Portable printer
* Forensic and packet capture software
* Bootable USB with trusted copies of tools
* Office supplies and evidence collection materials

**NIST 800--61 Classifies 4 major categories of security event indicators:**

* Alerts from IPS, IDS, SIEM, Antivirus and other monitoring software
* Logs from systems and applications
* Publicly available info about new exploits and vulnerabilities
* People who report suspicious activity

**Containment, Eradication, Recovery**

1. Select appropriate containment strategy
2. Implement containment strategy
3. Gather additional evidence
4. Identify attackers and attacking systems
5. Eradicate effects of the incident

**US Federal Agencies** must retain all incident handling records for 3 years.

**Threat Classification**

* External/Removable Media
* Attrition - brute-force methods to degrade, compromise or destroy systems, network or services
* Web - executed from a web application
* Email
* Impersonation
* Improper Usage
* Loss or theft
* Unknown
* Other

**Functional Severity Classification**

* **None** - no effect.
* **Low** - minimal effect. Organization can still provide all critical services to all users but with less efficiency.
* **Medium** - organization lost the ability to provide a critical service to a subset of users.
* **High** - organization is no longer able to provide some critical services to any users.

**Economic Impact Classification**

* **None** - no financial impact
* **Low** - loss of $10,000 or less
* **Medium** - loss of $10,000 to $500,000
* **High** - loss in excess of $500,000

**Recoverability Effort**

* **Regular** - Time to recovery is predictable with existing resources
* **Supplemented** - time to recovery is predictable with additional resources
* **Extended** - time to recovery is unpredictable, additional resources and outside help needed
* **Not Recoverable** - recovery is impossible

**Data Type Impact Categories**

* **None** - no info exfiltrated, changed, deleted or compromised.
* **Privacy Breach** - PII was accessed or exfiltrated.
* **Proprietary Breach** - unclassified proprietary information was accessed or exfiltrated.
* **Integrity Loss** - Sensitive or proprietary information changed or deleted.

**Information Impact Categories**

* **None** - nothing exfilled, changed, deleted or compromised.
* **Regulated Information Breach** - information regulated by an external compliance obligation was accessed or exfiltrated.
* **Intellectual Property Breach** - sensitive intellectual property was accessed or exfiltrated.

**Incident Analysis**

**Router-Based Monitoring**

* **Netflow, sFlow, J-Flow** - traffic flow protocols.
* **RMON** - monitors LAN layers 1-4. Uses probes to gather data and is implemented as a management information base.
* **SNMP** - Simple Network Management Protocol. Provides information about the devices.

**SNMPv1 and v2** should not be used. **SNMPv3** added authentication, encryption and users.

**iPerf** - tool that measures max bandwidth that a network can handle.

**PRTG** - **Paessler Router Traffic Grapher**. Provides server, network and bandwidth monitoring. It combines 4 types of monitoring:

* **Packet sniffing**. Looks at headers
* **Network Flows**
* **SNMP traps**
* **WMI** - Windows Management Instrumentation. Provides access of management data for the OS and to its reports

**Solar Winds**

* **Netflow Traffic Analyzer** - designed to handle network bandwidth analysis using flows
* **Network Performance Monitor** - network fault detection and availability management. Displays stats and performance as well as network health.

**Nagios** - network and system log monitoring tool. Nagios Core is a free and open source version. Nagios XI is commercial.

**Cacti** - open source tool that uses SNMP polling to poll network devices for status info and provides graphical views of network and device status. Uses RRDTool for graphing and analysis.

**Host-Based Monitoring**

**SCOM** - System Center Operations Manager. Centralized Windows monitoring and management system.

**SCCM** - System Center Configuration Manager can provide info about disk usage.

**Resmon** - **Resource Monitor**. Windows monitor for CPU, memory, disk and network utilization. Shows which TCP connections are open, which processes have network activity and what services are associated with open ports.

**Perfmon** - **Performance Monitor**. Shows energy usage, disk, network activity, etc. Used for detailed data collection

**Sysinternals** - bundle of tools for Windows monitoring.

**Linux:**

* **ps** - provides info about CPU and memory usage, the time processes were started and how long it has run
* **top** - provides CPU and memory usage as well as details about running processes.
* **df** - reports disk usage.
* **w** - shows who is logged in.
* **service --status-all** shows the state of all services running.

**Performing Forensic Analysis**

**Forensic Toolkit Components:**

* **Digital Forensics Workstation** - needs a powerful multicore CPU, a lot of RAM and fast, reliable storage.
* **Forensic investigation suite of software like**: FTKK, EnCase, SIFT (Sans Investigative Forensic Kit) or Sleuth Kit (TSK).
* **Write Blockers** - ensure that drives connected to a forensic system cannot be written to.
* **Forensic drive duplicators** - copy drives for forensic investigations and then provide validation.
* **Wiped drives and wiped removable media**
* **Cables and drive adapters**
* **Camera**
* **Label maker and documentation tools**
* **Notebooks and document forms**

**Windows System Artifacts:**

|  |  |
| --- | --- |
| **Location** | **Usage** |
| Windows Registry | Info about files and services, locations of deleted files, evidence of applications being run |
| Autorun Keys | Programs set to run at startup |
| Master File Table (MFT) | Details of Inactive/Removed Records |
| Event Logs | Logins, service start/stop, evidence of applications being run |
| INDX Files and Change Logs | Evidence of deleted files, MAC timestamps |
| Volume Shadow Copies | Point-in-time info from prior actions |
| User directories and files | Logged-in user artifacts |
| Recycle Bin contents | Files that were intended to be deleted |
| Hibernation files and memory dumps | Memory artifacts of commands run |
| Temporary directories | Artifacts of software installation, user temporary file storage, limited lifespan data |
| Application Logs | Application-specific data |
| Removable Drives | Evidence when relevant to the analysis |

**Linux Imaging with DD:**

***dd*** clones drives in RAW format, bit by bit. It supports the following options:

* Setting block size with the ***bs*** flag in bytes
* Operator ***if*** sets the input file
* Operator ***of*** sets the output file

**FTK** Suite provides **Imager Lite** for cloning drives.

**USB Historian** is software that displays removable storage that was used with a given Windows machine. Displays the manufacturer and serial number of the USB.

**Software for memory capture:**

* ***fmem*** and **LiME** - Linux kernel modules that allow access to physical memory. ***fmem*** uses dd and **LiME** directly copies.
* **DumpIt** - Windows memory capture tool that copies physical memory to the folder where it is.
* **Volatility Framework** - tools to extract encryption keys, passphrases, analyze user activity and rootkit activity.
* **EnCase** and **FTK** have built-in memory capture and analysis capabilities.

**Recovery and Post-Incident Response**

**Timestomping -** threat actors modifying timestamps to conceal the sequence of their actions.

**NIST Containment Strategy Criteria:**

* Potential Damage to and theft of resources
* Need for evidence preservation
* Service availability
* Time and resources needed to implement the strategy
* Effectiveness of the strategy
* Duration of the solution

**Eradication:**

* Sanitization
* Reconstruction/reimaging
* Secure disposal

**Validation:**

* Patching
* Permissions
* Scanning
* Verifying logging and monitoring

**Sanitization and Secure Disposal according to NIST SP 800-88:**

* **Clearing** - rewriting data.
* **Purging** - overwriting, block erasing, cryptographic erasing. Degaussing purges hard drives with magnets.
* **Destroying** - renders data recovery through physical destruction.

**Sanitization and Disposition Decision Making:**

* **Low Security Category:** if leaving org control, purge, otherwise clear.
* **Moderate Security Category:** if not to be reused, destroy. If leaving org control, purge, otherwise clear.
* **High Security Category:** if not to be reused, destroy. If leaving org control, destroy, otherwise purge.

**Policy and Compliance**

**PCI DSS Compensating control criteria:**

1. Must meet the intent and rigor of the original requirement
2. Must provide a similar level of defense as the original requirement
3. Must be above and beyond other requirements

**Major US Regulations:**

* Health Insurance Portability and Accountability Act (**HIPAA**) includes security and privacy rules that affect healthcare providers
* Payment Card Industry Data Security Standard (**PCI DSS**) provides detailed rules about storing, processing and transmitting credit and debit cards.
* Gramm-Leach-Bliley Act (**GLBA**) - covers financial institutions and requires they have a security program and a person in charge of it.
* Sarbanes-Oxley (**SOX**) - applies to financial records of publicly traded companies.
* Family Education Rights and Privacy Act (**FERPA**) - requires that educational institutions implement security and privacy controls

**NIST Cybersecurity Framework:**

**Framework Core** consists of 5 security functions that apply across all industries:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

**Framework Implementation Tiers:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tier** | **Risk Management Process** | **Integrated Risk Management Program** | **External Participation** |
| **Tier 1: Partial** | Reactive, no formal practices | Limited Awareness | No processes to participate |
| **Tier 2: Risk Informed** | Processes are established, but not org-wide | There is awareness, but not org-wide | No formalized processes |
| **Tier 3: Repeatable** | Formally approved and are policy | Org-wide approach to managing risk | Collaborates with partners |
| **Tier 4: Adaptive** | Org adapts its practices through lessons learned and predictive indicators | Org-wide approach to managing risk that uses risk informed policies, processes and procedures | Shares and collaborates to make sure to stay up to date |

**ISO 27001 is a set of standards from the International Organization for Standardization (ISO) that covers the following 14 categories:**

* Information Security Policies
* Organization of information security
* Human resource security
* Asset management
* Access Control
* Cryptography
* Physical and Environmental Security
* Operations Security
* Communications Security
* Systems acquisition, development, and maintenance
* Supplier relationships
* Information security incident management
* Information security aspects of business continuity management
* Compliance with internal and external requirements

Control Objectives for Information and Related Technologies (**COBIT**) is a set of best practices for IT developed by Information Systems Audit and Control Association (**ISACA**) that divides activities into **4 domains**:

* Plan and Organize
* Acquire and Implement
* Deliver and Support
* Monitor and Evaluate

Sherwood Applied Business Security Architecture (**SABSA**) offers a model for approaching security from different perspectives:

|  |  |
| --- | --- |
| **View** | **Architecture Layer** |
| **Business View** | Contextual Security architecture |
| **Architect’s View** | Conceptual Security architecture |
| **Designer’s View** | Logical Security architecture |
| **Builder’s View** | Physical Security architecture |
| **Tradesman’s View** | Component Security architecture |
| **Service Manager’s view** | Security Service Management architecture |

The Open Group Architecture Framework (**TOGAF**) divides architecture into 4 domains:

* **Business architecture** - explains interactions between enterprise architecture and business strategy
* **Applications architecture** - explains interactions between applications and business processes
* **Data architecture** - describes the org’s approach to storing and managing information assets
* **Technical architecture** - describes the infrastructure needed for other domains

**TOGAF Architecture Development Method (ADM):**

1. Prelim: Framework and Principles
2. A: Architecture Vision
3. B: Business Architecture
4. C: Information System Architecture
5. D: Technology Architecture
6. E: Opportunities and Solutions
7. F: Migration Planning
8. G: Implementation Governance
9. H: Architecture Change Management

Information Technology Infrastructure Library (**ITIL**) is a framework for IT service management that covers **five core activities**:

* Service Strategy
* Service Design
* Service Transition
* Service Operation
* Continual Service Improvement

|  |  |
| --- | --- |
| **Goals** | **PCI DSS Requirements** |
| Build and Maintain a Security Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 1. Protect stored cardholder data 2. Encrypt transmissions of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 1. Protect all systems against malware and regularly update anti-virus software or programs 2. Develop and maintain security system and applications |
| Implement Strong Access Control Measures | 1. Restrict access to cardholder data by business need to know 2. Identify and authenticate access to system components 3. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 1. Track and monitor all access to network resources and cardholder data 2. Regularly test security systems and processes |
| Maintain an Information Security Policy | 1. Maintain a policy that addresses information security for all personnel |

**Defense in Depth**

Defense in Depth **security designs**:

* **Uniform Protection** - same level of protection to all systems and networks.
* **Protected enclaves** - some network segments, systems or physical locations have additional controls.
* **Risk/Threat Analysis-based** - only controls that are needed for anticipated threat vectors are implemented.
* **Information Classification-based** - controls are mapped to information classes.

**Types of security controls**:

* **Physical** controls - security controls that impact the physical world
* **Logical** controls are technical controls that enforce the CIA triad in the digital space
* **Administrative** Controls - procedural mechanisms that an organisation follows
* **Preventive** Control - intended to stop an incident from occurring with proactive measures
* **Detective** Controls - detect an incident and capture information about it
* **Corrective** Controls - remediate an incident or act to limit how much damage it causes

**Firewall Placements**

* **Single Firewall** Network has its DMZ sitting between the border router and the firewall protecting internal network.
* **Service-leg DMZ** (Multiple interface network design) use the firewall’s interfaces to separate out the network into parts.
* **Multi-Firewall** Design puts the DMZ in between of 2 firewalls.

**Trusted Platform Module**

* Remote attestation allowing configurations to be verified
* Binding which encrypts data
* Sealing, which encrypts data and sets requirements for the state of the TPM chip before decryption

**Reviewing Security Architecture**

* **Operational view** describes how a function is performed and what it accomplishes.
* **Technical view** describes technologies, settings and configurations used in an architecture.
* **Logical view** describes how systems interconnect.

**Identity and Access Management**

**AAA -** Authentication, Authorization, Accounting.

IAM - Identity and Access Management.

**LDAP** - Lightweight Directory Access Protocol

**OU** - Organizational Unit

**CN** - Common Name

**Common Authentication Protocols**

**TACACS+** - Cisco’s TACAS over TCP. Insecure and should be isolated.

**RADIUS** - Remote Authentication Dial-in User Service. Uses IPsec and MD5.

**Kerberos** - designed to work in untrusted networks. Principals are composed of primary (usernames), instance and realm (group). Realms have different KDC (Key Distribution Centers).

**Shared Authentication** - allow an identity to be reused on multiple sites while authenticating with a single identity provider.

**CAS** - Central Authentication Service

**OpenID** - open source decentralized authentication.

**OAuth** - open authorization standard that relies on authentication tokens.

**OpenID Connect** - authentication layer built using OAuth.

**Security Issues with Identities:**

* Personnel-based
* Endpoints
* Server-based exploits
* Applications and services
* Roles, rights and permissions

**LDAP Attacks:**

**Insecure Binding** - attacks unencrypted LDAP connections.

**Improper Access Control** - allows harvesting or modifying information.

**LDAP Injection** - exploits web applications that build LDAP queries.

**Denial Of Service** - disrupts authentication services

**Kerberos Attacks:**

* Admin account attacks
* Ticket Reuse that includes pass-the-ticket, pass-the-key and impersonation.
* Ticket Granting Server (TGT) attacks. Golden tickets grant access to everything under Kerberos control

**Radius Attacks:**

* Session replay
* Attacks on the shared secret
* Denial-of-Service
* Credentials-based Attacks

**Active Directory Attacks:**

* Malware
* Credentials theft
* Privilege escalation
* Service account use
* Unnecessary Admin rights
* Usage of old protocols like NTLM

**Account Life Cycle:**

* Create and set password
* Provision services and set rights and roles
* Modify and maintain
* Disable
* Retire and deprovision

**Federated Identity**

* **IDP** - Identity Provider
* **RP** - Relying Party
* **SP** - Service Provider

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **SAML** | **OpenID** | **OAuth2** | **ADFS** |
| **Authorization** | Yes | No | Yes | Yes |
| **Authentication** | Yes | Yes | Partial | Yes |
| **Potential Security Risks** | Confidentiality, denial of service, processing risks | Redirect manipulation, confidentiality, replay attacks, CSRF/XSS, Phishing | Redirect Manipulation, Confidentiality  impersonation | Token attacks |
| **Common Uses** | Enterprise authentication and authorization | Authentication | API and service authorization | Enterprise authentication and authorization in Windows |

**ADFS** - Active Directory Federation Services. Provides authentication and identity info as **claims** to third-parties. Partners use **trust policies** to match claims to claims supported by a service and then to make decisions.

**ADFS Process:**

1. User attempts to access an application
2. ADFS agent checks for ADFS cookie. If it’s not there, the user is sent to the ADFS server.
3. ADFS checks for a SAML token, if not, does home realm discovery.
4. Home realm discovery identifies the server associated with the user and then authentications via that realm.
5. Account partner provides a security token with identity info in the form of claims and sends the user back.
6. Validation occurs normally and uses its trust policy to map the account partner claims to claims they support.
7. New SAML token is created and stored. User is redirected back to the application.

**OAuth:**

* **Clients** - applications that users want to access
* **Resource Owners** - end users
* **Resource servers** - servers provided by a service that the resource owner wants the app to use
* **Authorization Server** - server owned by the identity provider

**Federation Incident Response:**

* Identity Providers are typically responsible for notifying account owners and may be responsible for notifying relying parties.
* Service Providers need to determine what they response would be if the identity provider was compromised.

**Software Development Security**

**SDLC -** Software Development Life Cycle.

**General SDLC steps:**

1. Feasibility phase determines whether the effort should occur.
2. Analysis and requirements phase determines what is needed to the application.
3. Design Phase - includes design for functionality, architecture, etc.
4. Development Phase - where the actual coding happens.
5. Testing and integration phase
6. Training and transition
7. Ongoing operations and maintenance
8. Disposition phase shuts down old services.

**CMMI** - Capability Maturity Model Integration.

**CMMI model:**

1. **Initial**. Process is chaotic. No effective plans and procedures are made. Inconsistent.
2. **Repeatable**. Change control, formal management structure. Can repeat processes from project to project.
3. **Defined**. Formal procedures are in place and define processes. Quantitative process improvement is utilized.
4. **Managed**. Formal processes in place to collect and analyze quantitative data and metrics.
5. **Optimizing**. Company has budgeted and integrated plans for continuous process improvement.

**Software Development Models:**

* Waterfall
* Spiral
* Agile
* RAD
* V model - Waterfall with a test phase attached to each step
* Big Bang - no planning or process

**Waterfall**:

1. Gather Requirements
2. Design
3. Implement
4. Test/Validate
5. Deploy
6. Maintain

**Spiral:**

* Identification
* Design
* Build
* Evaluation

**Agile**:

* Spring Planning
* Development
* Testing
* Demonstration

**Backlog** - list of features required to complete a project.

**RAD**:

* Business Modeling
* Data Modeling
* Process Modeling
* Application Generation
* Testing and turnover

**Code Review Methods:**

* **Pair Programming** - two developers working at the same time. One writes, one reviews.
* **Over-the-shoulder** - developer explains the code to the other developer.
* **Pass-around** - complete code is sent to reviewers to check.
* **Tool-assisted** - done using software.
* **Fagan inspection** - formal code review.

**Fagan Code Review:**

1. Planning
2. Overview
3. Preparation
4. Meeting
5. Rework
6. Follow-up

**Testing:**

* **Fault injection** inserts faults into error handling paths.
* **Mutation** testing modifies the program slightly.
* **Regression** testing checks that changes don’t introduce new issues.

**Cybersecurity Toolkit**

**Endpoint Protection**

**EMET -** Enhanced Mitigation Experience Toolkit

* Includes **DEP** - Data Execution Prevention to prevent the execution of malware from memory
* Includes **ASLR** - address space layout randomization to prevent buffer overflows

**Sysinternals Suite:**

1. **AccessEnum** - enumerates permissions
2. **AutoRuns** - shows what starts at system boot or login
3. **Process Explorer** - details about each running process
4. **PsTools** - set of command line utilities
5. **SDelete** - secure file deletion
6. **ShareEnum** - analyzes shares and their permissions
7. **Sysmon** - monitors processes and their activity
8. **ProcDump** - process dumping for memory and error analysis
9. **TCPView** - shows the socket-level of network-connected services

**Syslog** - standard for logging.

* Kiwi Syslog from SolarWinds
* Syslog-ng - open source
* Rsyslog - open source

**Windows login failure** ID 4625

**Windows login success** ID 4624

**Security Event and Information Management**

**Popular SIEM’s:**

* ArcSight
* QRadar
* Splunk
* AlienVault
* OSSIM

**USM** - Universal Security Manager provides:

* Asset Discovery
* Vulnerability Scanning
* IDS
* Behavior Analysis
* SIEM

**OSSIM** - Open Source SIEM includes:

* **OpenVAS** for vulnerability scanning
* **Suricata** for IDS
* **Nagios** for monitoring
* **OSSEC** for host-based IDS
* **Munin** for traffic analysis
* **FProbe** for NetFlow

**Network Monitoring**

**Cacti** - network graphing tool running on top of RRDtool. Collects data frequently and supports SNMP.

**SolarWinds Orion** - centralized monitoring platform for flows, system, network, application, virtualization and storage monitoring.

**ManageEngine’s NetFlow Analyzer** - graphical view of network bandwidth and other flow info.

**Nagios Core** - open source monitoring tool for services, systems, resources and other things through plugins.

**Multi Router Traffic Grapher (MRTG)** - open source network monitoring tool that uses SNMP.

**Vulnerability Scanning**

**Tenable Nessus**

* Port 8834
* Has a scanning server and a client
* Has a safe checks option for destructive attacks
* Has **NASL** - Nessus Attack Scripting Language for plugins

**Qualys QualysGuard** - SaaS.

**Rapid7 Nexpose**

**OpenVAS**

* Port 9392
* Has Manager and Scanner
* Uses a collection of 47000 Network Vulnerability Tests (NVT’s)
* Shows vulnerability score and confidence level

**Nikto**

**DISA -** Defense Information Systems Agency

**STIG -** Security Technical Implementation Guide

**Potential Inhibitors to Remediation:**

* **MOU -** Memorandum Of Understanding
* **ROE -** Rules of Engagement
* **SLA -** Service Level Agreement
* **Corporate Governance** - system of processes and rules an organization uses to direct and control its operations.

**Password Tools**

**Password Recovery Tools:**

* Fgdump
* Pwdump
* SAMdump2

**Password Cracking Tools:**

* **John the Ripper** - popular Linux tool
* **Cain and Abel** - for Windows only
* **Ophcrack** - open source tool that uses rainbow tables
* **Passware Kit Forensic** - breaks protected files.

**Network Security Tools**

**Popular Firewall Manufacturers:**

* Check Point
* Palo Alto
* Cisco
* Juniper

**Popular Host Intrusion Detection Systems:**

* Snort - has a community curated set of rules to identify malicious activity.
* Bro - utilizes protocol analysis.

**Popular Web Application Firewalls:**

* Akamai Kona Site Defender
* CloudFlare’s Cloud WAF
* F5 ASM
* Fortinet FortiWeb
* Impreva SecureSphere and Incapsula
* Radware AppWall
* NAXSI
* ModSecurity

**Web App Fuzzers:**

* Untidy fuzzer
* Peach Fuzzer
* Microsoft Security Development Lifecycle MiniFuzz and Regex Fuzzer

**Hashing Tools:**

* Md5sum
* Shasum

**Forensic Suites:**

* FTK
* EnCase
* Sans Sift
* Sleuth Kit
* Helix 3 Enterprise and Pro
* Cellebrite UFED - mobile