

Non-Technology Controls

Question	Possible Answers
List some principles for good security architecture.	The approach includes redundancy and layers of defenses.
Discuss basic information and systems classification principles for a risk assessment.	The architecture is actually designed – as opposed to resulting from reactions to threats and vulnerabilities over time. The architecture is periodically reviewed and revised. Sensitivity of information (e.g., personal privacy or intellectual ownership). Criticality of information to the organization's mission. Prioritization of information systems and network infrastructure components for protection as well as for recovery.
What are some important elements in a security policy pertaining to personnel?	Definition of roles and responsibilities. Expectation of compliance. Expectation to meet standards of reasonable care and due diligence. Enumeration of penalties and consequences for failure to follow policies.
What role can Purchasing play in security?	Requiring security standards as part of any purchase of information technology products and/or services. Requiring evaluation of vendors for their security capabilities.
List some best practices for security procedures, guidelines and standards.	They are documented. They are reviewed and updated as needed. They are audited or tested as needed.
What are some best practices for connecting or exchanging data with external parties?	Formal agreements are required. External parties are evaluated for their security capabilities.
What general things should users learn in information security training?	What the organizational policies are. Types of threats and how to identify and/or avoid them. Who to report suspected incidents to.
List some best practices for patches and upgrades.	Both vendors and public sources are monitored for information on vulnerabilities and availability of patches. Security patches and upgrades are prioritized and installed in a timely manner. Security patches and upgrades are tested prior to installation.

Question	Possible Answers
Name some best practices regarding Configuration Management.	<p>Configuration management policy and procedures are documented.</p> <p>Inventories of hardware and software are complete, accurate, and up to date.</p> <p>Configurations are reviewed and audited periodically.</p> <p>Default settings and default passwords are changed when systems and software are installed.</p>
What are some ways to protect physical access to sensitive areas?	<p>Doors have locks.</p> <p>The doors are tested regularly.</p> <p>Cameras and/or sensors are used for surveillance.</p>
List some best practices for backups.	<p>Systems are backed up regularly.</p> <p>Backups are stored off site.</p> <p>Restores from backups are tested periodically.</p>
List different objectives for system auditing and monitoring.	<p>Systems scanning periodically and after changes for vulnerabilities such as default configurations, misconfigurations, or unpatched systems.</p> <p>System monitoring to ensure that only allowed processes are running.</p> <p>Review of firewall rules for accuracy and completeness.</p> <p>Password cracking tests to identify weak or easily guessed passwords.</p>
How should information be disposed of?	<p>Disks (electromagnetic and optical) are properly wiped or destroyed.</p> <p>Paper records with sensitive information (e.g., including security settings) are shredded rather than thrown out.</p>
What are some good personnel policies for information security?	<p>Conducting background checks for employees, temporary workers, and contract workers who handle sensitive data or administer critical systems.</p> <p>Requiring separation of duties.</p> <p>Having standards for termination and, in handling termination situations, cooperation between Human Resources and information technology departments.</p>
For incident response, what internal parties besides technical staff may have a role to play?	<p>Legal counsel.</p> <p>Human resources.</p> <p>Senior management.</p> <p>Public relations.</p>
For incident response, what external parties may have a role to play?	<p>ISPs.</p> <p>Information security associations.</p> <p>Law enforcement agencies.</p> <p>Interconnected partners.</p>
What actions should take place after an incident is over?	<p>Capture lessons learned.</p> <p>Apply other needed patches or configuration changes.</p> <p>Update plans and procedures to correct deficiencies.</p>

Question	Possible Answers
List some environmental controls.	Emergency power and lighting. Fire protection. Sensors for temperature and humidity. Protections against water damage (e.g., plastic sheeting). Emergency shutdown controls. Monitoring of environmental controls. Procedures for responding to alarms. Periodic testing of environmental controls.
What are some good policies or requirements for fault and problem management?	Testing for system defects and errors for both in-house and purchased systems. Use of a test lab to test changes and restore procedures. Procedures for backing out changes as part of the installation process. Logging and tracking of defects and errors. Plans to correct defects and errors in an appropriate timeframe.

Technology-Based Controls

Question	Possible Answers
Describe when encryption should be used.	For sensitive and personal identification information. For data in transmission (e.g., email). For Web sessions using HTTPS. For stored records or files. For log files. For remote sys admin logins using SSH instead of telnet. For VoIP call content.
List some session controls.	Lock a session after it has been idle for a period of time. Terminated a session upon disconnect.
What would you audit in firewall logs for a VoIP system?	To determine types of calls. To see whether calls are changing type during the call.
For a wireless network, what kinds of things should be reviewed in an audit?	Unauthorized wireless access points. Wireless access points that are not properly configured. Wireless packets, to verify that they are using the standard authentication protocol.
List some protections against malicious code and hackers.	Anti-virus software that is kept up to date. Anti-spam / anti-spyware software that is kept up to date. Properly configured firewalls. Intrusion detection system with up to date signatures. A file integrity checking tool.

Question	Possible Answers
List some best practices for network design.	Use layers of defense; e.g., network and host intrusion detection. Have multiple network paths and 2 or more ISPs. Employ a split DNS technique (external DNS only for publicly accessible hosts, separate internal DNS). Use network address translation (NAT) to protect internal network addresses.
What are some protocols or methods for securing wireless LANs?	RADIUS – authentication. 802.1x (EAP) – authentication.. 802.11i (WPA2). Turn off DHCP for wireless access points; use static addresses.
Name some best practices regarding DNS servers.	Do not include HINFO or TXT records. Restrict zone transfers to the secondary DNS only. On firewall filtering rules, limit TCP port 53 to the secondary DNS only.
What are some best practices for account management?	Unused and idle accounts are tracked and shut down. Temporary accounts are prohibited or closely controlled. Administrator, root, or super user access is limited to only the few people who have those responsibilities.
What should be done with unsuccessful logons?	Lock the account after the threshold for unsuccessful attempts has been exceeded.
List some best practices regarding audit and logging trails.	Track unsuccessful logon attempts. Logging and audit trails are enabled. Logs and audit trails are reviewed for anomalies promptly and regularly. Traffic analysis is done regularly. Audit information is protected.
For voice communications systems, where could you find evidence of abuse and fraud?	Phone bills. Call detail records. Voicemail box access. Interactive Voice Response (IVR) system.
Name some risky practices regarding user or device identification and authentication.	Trunk to trunk transfers. Shared or group accounts are allowed. Use of guest and anonymous accounts or access. Not requiring users to provide identification and authentication (e.g., account name and password or PIN) before accessing resources. Not requiring strong passwords. Not requiring regular password changes. Not authenticating devices (e.g., with a MAC address) when attaching to the network.

Attacks

Question	Possible Answers
How would you conduct physical reconnaissance of a target to get network access?	Walk around trying to open or find unlocked network closet doors. Find unguarded reception areas or offices left open, or conference rooms with voice and data jacks.
How would you as an outsider get physical access to the target?	Follow someone into restricted areas (piggybacking). Get a job as a janitor or maintenance person to gain access to offices and PCs. Hire on as an employee or a temp or pose as a supplier or vendor.
List some social engineering methods of attackers.	Pose as a new employee, system administrator, vendor, etc. Use pretexts to obtain contact name and number, passwords, sensitive documents, information about systems and network architecture. Use pretexts to get the target to do something such as go to a Web page that downloads malware, establish a voicemail box or computer account. Participate in newsgroups to provide advice and get information from employees of the target. Become friends with disgruntled or naïve employees and enlist them to launch an attack or help you launch an attack. Spoof the email address of a system administrator, then request users to provide passwords.
What could you find out from using a search engine and/or searching public Web sites about a target?	Employee contact information; phone numbers; business locations; identities of business partners; technologies in use; events that can be exploited; general information about the culture of the target. Linking web sites associated with the target (link:www.target-name.com) Unencrypted data such as backup files, source code, database schemas, embedded comments on passwords, etc.
What can the InterNIC Registrar and sources such as ARIN tell you about the target?	IP addresses of Web servers and DNS. Possibly also the type of servers the target is running. Names of technical staff.
How can employees expose confidential and sensitive information to attackers?	Asking questions or sharing information in a newsgroup or listserv. Blogging. Sending an email to an unauthorized person, whether intentionally or by accident.

Question	Possible Answers
What kinds of systems are apt to have lax or weak security controls?	<p>Employees' home systems with remote access.</p> <p>Test systems.</p> <p>Windows backup domain controller.</p> <p>VoIP systems.</p> <p>Wireless LANs.</p>
What kinds of things can scanning tools reveal about a target?	<p>Default configurations.</p> <p>Older versions of operating systems / unpatched systems.</p> <p>Commonly open TCP or UDP ports, particularly ones that should be closed.</p> <p>Unprotected wireless network.</p>
What can traceroute tell you about a target?	<p>Network topology, including which devices are routers, firewalls, servers, etc.</p> <p>The TTL field of traceroute can help identify the path to the host via routers.</p>
What are some ways to attack a wireless network?	<p>Set up a PC to act as a wireless access point, so it answers other PCs seeking a wireless network. Then, authenticate the victim's request and gain access to the victim's PC.</p> <p>Cause a power outage, so low-end wireless access points revert to their default settings and can be compromised.</p>
What are some ways to avoid or minimize detection at the network level?	<p>Attack at night or over a weekend or holiday, because it may take longer for someone to notice or respond.</p> <p>Modify traffic so it doesn't match IDS signatures; this works well if target administrators do not update their IDS regularly.</p>
What are some ways to avoid or minimize detection at the operating system or application level?	<p>Send packet fragments, a flood of fragments, or packets fragmented in unusual ways to confuse the IDS.</p> <p>Hide attack tools or data in another file such as a graphics or audio file.</p> <p>Use a rootkit to establish a backdoor.</p> <p>Tunnel back out with HTTP or SMTP to avoid detection at the firewall.</p> <p>In Windows, hide attack tools or data in an alternative data stream behind a commonly used program or file such as notepad.exe or readme.txt.</p> <p>In Unix, hide files by using a name that starts with one or two periods.</p>
How would you conduct an SQL attack on a Web form?	<p>Try filling in a field with a delimiter (such as ;) or an extra-long string. Observe the URL of the page that displays the error message. (Even better if the application displays the SQL when returning the error message!) Then modify the SQL to query other data (e.g., another account) or to update the database (modify existing data or add a new record).</p>

Question	Possible Answers
What can make a Web login page vulnerable to account harvesting?	The error response for a failed login distinguishes between a failed User ID and a failed password. The error may be distinguished in the URL, in a cookie, or in a hidden form element on the Web page with the error message.
How does session hijacking work?	Find Web sites that do not properly protect session IDs. Then analyze how they are generated, to determine if future session IDs are predictable. If so, then login in and then modify the session ID to take over some else's session.
What could an attacker do with an intercepted or guessed VoIP user ID and password?	Prevent the user from placing calls by changing the password. Place phone calls at the victim's expense. Capture voice conversation packets, either to eavesdrop or to corrupt the conversation (alter the contents, inject noise or silence). Delete voicemail messages. Change a call forwarding number. Change the calling plan. Send a SIP control packet to direct a call to a different device that is under attacker control. For example, someone calling the victim will end up talking to the attacker. Or, the victim making an outbound call will talk to the attacker rather than the intended recipient.
In what ways can a program exhaust a server's resources?	A recursive program won't stop running. A program that generates massive output to fill up disk space. A program that creates enormous amounts of network traffic.

Challenge Security Extra Questions

Management

Policy and Planning – Planning

Are security plans required for all systems, including networks?

Are regular reviews and updates to plans required?

Risk Assessment – Policy

Do you require risk to be managed, including performance of risk assessment and planning for mitigation activities?

Is periodic review and update of assessments and plans required?

Security Assessments and Audits – Policy

How frequently should they be performed?

What scope is needed?

Does an independent third party evaluate your security architecture and controls?

Systems and Services Management – Policy

Is information security required to be considered for all IT systems and services, whether purchased or developed in-house?

Is compliance with all laws and regulations required? For example, are laws with respect to copyright or child pornography referenced?

Operational

Configuration Management – Telecommunications

Do you block access to outside dial tone for trunks connecting the voice system and the voicemail system?

Are unused voicemail boxes removed promptly?

Do you disallow trunk to trunk transfers?

Do you disallow call forwarding to off-premises numbers?

Configuration Management – VoIP

Do you limit the ability to log in remotely to VoIP phones, servers, and gateways?

Are direct connections to the Internet blocked?

Incident Response – Policy

Is there a policy that establishes incident response planning and other capabilities?

Does the policy require incidents, including losses, to be reported?

Is the plan reviewed and updated periodically?

Are components of the plan tested regularly?

Are staff members trained for incident response?

Incident Response -- Handling

Are standards for investigating incidents set?

Do standards address involvement of law enforcement?

Do they include procedural protections for suspects?

Business Continuity – Policy	<p>Is a business continuity plan required?</p> <p>Is the plan updated regularly?</p> <p>Is testing of the business continuity plan required?</p> <p>Are appropriate people trained to follow the business continuity plan?</p>
Business Continuity – Alternatives	<p>Is there route diversity and redundancy in your network configuration?</p> <p>Do you have an alternative site for processing?</p>
Physical security – Network	<p>Is cabling sufficiently protected?</p>
Physical security -- Alarms	<p>Are alarms in place?</p> <p>Are alarms monitored?</p> <p>Are there procedures for responding to alarms?</p> <p>Are alarms and monitoring procedures tested?</p>
Security awareness and training	<p>Does a policy require security training and awareness programs?</p> <p>Do you ensure that users are fully trained in security awareness and risks associated with information technology?</p> <p>Are users required to take security training annually?</p> <p>Do technical staff receive appropriate quality security training?</p>
Configuration Management – Change control	<p>Are change management procedures required?</p> <p>Are changes to systems reviewed and authorized?</p> <p>Are only authorized personnel allowed to install or change equipment or software?</p> <p>Are emergency change procedures available but used only rarely?</p>
Security Operations and Maintenance – Network and System Administration	<p>Unused ports are closed.</p> <p>Use of FTP is limited.</p>

Technical

Access Controls -- Authorization for use	<p>Are access control measures required by policy to protect information and systems?</p> <p>Who may use data and information systems?</p> <p>What purposes may they use them for?</p> <p>What activities are prohibited?</p> <p>Who may operate or administer systems?</p>
---------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------