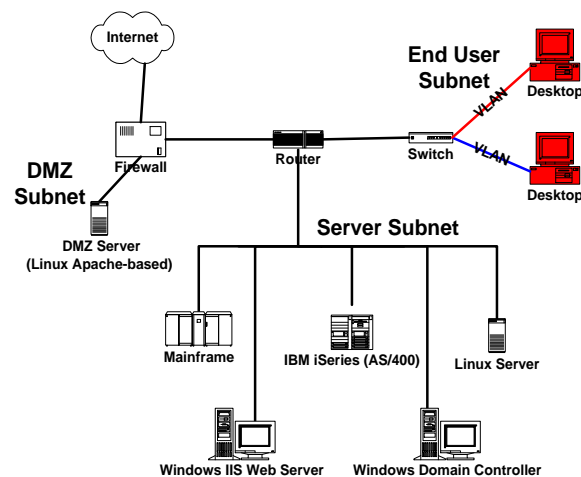


Assessing other devices / Scanning

- Other devices
 - Desktop Systems
 - Cisco routers
 - Firewalls
- Intro to general purpose vulnerability scanners

Class 8

Desktop Systems



Class 8

Windows XP Desktop

- Use MBSA to review local configuration
 - Many of the tests are the same as servers
- End user systems differ from servers in significant ways:
 - Network accessible services should be minimized
 - Typical users should not have administrator rights
 - Methods for software installation should be controlled

Class 8

Windows XP Desktop

- Are the desktop systems part of a Windows 2000/2003 domain?
 - If so, then reviewing applicable group policies and their enforcement is relevant
 - If not, then this method for enforcing common security standards is not available

Class 8

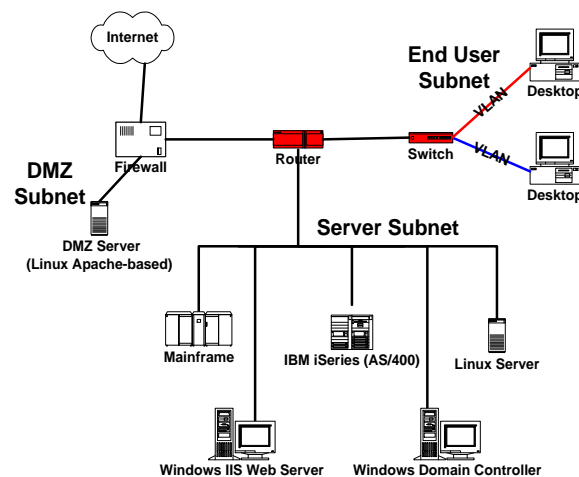
Windows XP Desktop

- Additional checks:
 - Anti-virus software current
 - Software firewall
 - Screen saver timeout with password
 - Disk/directory/file encryption
 - Malware or unauthorized software present?

Class 8

Network Devices

Cisco Routers used as an example



Class 8

Cisco Routers

- Organizational policy compliance vs. inherent vulnerabilities
 - Inherent vulnerabilities are factors which present a risk regardless of how the network is configured. These are general to any site
 - Organizational compliance is how well the router enforces rules for managing traffic. These are specific to the organization.

Class 8

Cisco Routers

- Inherent vulnerabilities are limited in number but important:
 - Security patches
 - Use encrypted passwords
 - Assign strong passwords
 - Configuration change control
 - Physical security

Class 8

Cisco Routers

- Organizational compliance checks can be numerous and the impacts subtle:
 - Access control lists
 - Separation of traffic into VLANs (actually a switch issue)
 - Use of management services (SNMP, CDP, etc.)

Class 8

Cisco Routers

- CIS provides a tool for reviewing router configuration
 - Router Audit Tool (RAT)
 - Runs from a Windows command prompt (“MS/DOS”)
 - Input is text file from “show config”
 - Output is assessment results as HTML file

Class 8

Firewalls

- Very similar to routers and other network devices:
 - Vulnerabilities patched?
 - Remote access restricted?
 - Only secure administrative communication allowed, from authenticated administrators
 - Event logging for exceptions?

Class 8

Firewalls

- Firewalls play a key role in enforcing security policies, and policy-based audits are very important:
 - Are rules configured properly?
 - Are firewall exceptions properly documented, and subject to change control?
 - Event logging for traffic violating rules and administrative actions

Class 8

Firewalls

- Common problems:
 - Too many exceptions
 - Rules configured incorrectly
 - Lack of change control
 - Network access around the firewall
 - Firewall can be fooled by anomalous traffic (a firewall design flaw)

Class 8

Firewalls

- Assessment involves:
 - Review documented management processes
 - Examine rules, ensure exceptions are documented
 - Test firewall rules with sample traffic
 - Use scanning tools to see if any visible flaws
 - Confirm version release to ensure properly patched

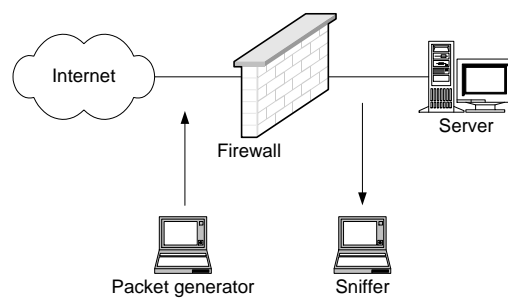
Class 8

Firewalls

- Note that PCI assessments require detailed review of firewalls:
 - Stateful inspection: test with SYN-ACK and SYN-RST scans
 - Scan all ports (0 – 65535)
 - Test from a variety of ports
 - Scan outbound and inbound

Class 8

Firewalls



Class 8

Vulnerability Scans

Class 8

Vulnerability Scans

- Similar in intent to a security assessment
- Broad and shallow rather than narrow and deep:
 - Review all systems on a network
- Focus on network-facing services and what can be inferred from these

Class 8

Vulnerability Scans

- Types of scanning tools:
 - Port scanners
 - Service enumerators
 - War dialers
 - Wireless access tools
 - Sniffers
 - Password cracking tools
 - Integrated vulnerability scanners

Class 8

Vulnerability Scans

- Port scanners:
 - What systems are visible from the network?
 - What IP ports and protocols are open on the target?
 - What else can we find out from how the target responds to basic IP-based network queries?

Class 8

Vulnerability Scans

- Service enumerators:
 - What applications are provided via network services?
 - What versions of these applications are provided?
 - How are the applications configured?

Class 8

Vulnerability Scans

- War dialers:
 - For a range of phone numbers, which ones are modems?
 - How does the modem respond?
 - Can we guess the target system or service behind the modem?

Class 8

Vulnerability Scans

- Wireless access tools:
 - Listen to wireless communications over the airwaves.
 - What access points and networks are accessible?
 - Are communications encrypted?
 - Can the encryption be broken?

Class 8

Vulnerability Scans

- Sniffers:
 - Listen to traffic on wired networks
 - What hosts are present?
 - How do they communicate?
 - What software are hosts running?
 - Are passwords being sent over the network?

Class 8

Vulnerability Scans

- Password cracking tools:
 - Most systems encrypt passwords
 - Encrypted passwords must be stored somewhere
 - Encrypted passwords travel over the network and can be sniffed
 - Cracking tools try to “guess” the passwords by encrypting common words and word variations, and comparing to the captured encrypted passwords

Class 8

Vulnerability Scans

- Integrated vulnerability scanners:
 - Try to combine many of the previously mentioned functions into a single integrated tool
 - Automate the tasks involved in gathering security vulnerability information
 - Combine with standard vulnerability databases
 - Create nifty automated reports

Class 8

Vulnerability Scans

- “Gotchas”:
 - Scans can crash unstable servers and network devices
 - A scan looks like a network attack and can cause panic
 - Keeping scans within defined subnets can be difficult; scanning unauthorized subnets can be a “career limiting move”
 - False positives
 - Make the client look bad
 - Make you look like an idiot

Class 8

Managing the Vulnerability Scan

- Real-time communication between scanners and technical administrators
- “Get out of jail free” card
- Special considerations when scanning critical servers
- Other points described for a security assessment are also valid

Class 8