Chapter 8

Risk management tools

horizontal line

**Risk assessment**

**Quantitative risk assessment**

Measures the risk using monetary value. A commonly used quantitative model uses the following values to determine risks:

* Single loss expectancy (SLE): The cost of any single loss
* Annual rate of occurrence (ARO): How many times the loss will occur in a year, e.g. once every two years is 0.5%
* Annual loss expectancy (ALE): SLE\*ALO

**Qualitative risk assessment**

A probability and impact level is assigned to the risk. One challenge of this approach is gaining consensus on the probability and impact level of each risk.

**Assessment documentation**

This identifies the risks discovered, and the recommended controls. However, if an attacker gains access to this report, they will be able to see all the vulnerabilities. Any controls highlighted in the report will take time to implement, giving an attacker plenty of vulnerabilities to exploit.

**Risk registers**

A repository of all identified risks, which may have the following columns: category, Specific Risk, likelihood of occurrence, impact, Risk Score, Security Controls, Contingencies, Risk Score with Contingency Controls, Action Assigned To and Action Deadline.

**Supply chain assessment**

Provides an assessment of the elements needed for an operation, and the processes required. It also examines processes and identify any steps that would be a single point of failure.

**Checking for vulnerabilities**

**Password crackers**

Attempt to discover a password. Admins can use them in a vulnerability assessment.

**Network scanners**

Use various techniques to gather info on hosts in a network. Popular tools include:

* **Ping scan**: sends ICMP pings to IP addresses on a network, to check host responsivity.
* **ARP ping scan**: ARP packets are sent to obtain a system’s MAC address, to check that the host is operational
* **SYN stealth scan**: Sends SYN packets to each IP address in the scan range, expecting a SYN/ACK packet in return, to test responsivity. The scanner sends RST (reset) packet instead of ACK.
* **Port scan**: Checks for open ports on a system
* **Service scan**: Like the port scan, but can identify what protocols/services it may be running
* **OS detection**: Analyse packets from an IP address to identify the OS (TCP/IP fingerprinting)

**Network mapping**

Done as part of a network scan, and identifies devices on a network and how they are connected with each other

**Wireless scanners**

* **Passive scans**: Scanner listens to all traffic being broadcast on known channels within 2.4-5ghz range
* **Active scans**: Scanner acts like a scanner/cracker to gain more info about an AP by sending queries to it.

**Rogue system detection**

If an admin knows which APs are authorized, a wireless scan can reveal rogue APs by revealing unknown SSIDs. Received Signal Strength Indicator (RSSI) shows strength of signal. The closer a number is to zero, the stronger the signal.

**Banner grabbing**

Used to gain info about remote systems, and to identify the OS along with app info. It returns a HTML banner with all the info

**Vulnerability scanning - a passive test**

Vulnerability scanners utilise a database of known vulnerabilities, such as Common Vulnerabilities and Exploits (CVE) and test systems against this database. Vulnerabilities can include:

* **Open ports:** Only relevant ports should be open
* **Weak passwords**
* **Default accounts and passwords**: Basic hardening of systems should remove these accounts
* **Sensitive data**
* **Security and config errors**

**Credentialed vs non credentialed**

Credentialed scans run using the credentials of an account, or as non credentialed without any user credentials (which is how attackers perform their attacks, so is more appropriate)

However, credentialed attacks with admin credentials perform scans at a much deeper level, so are more accurate

**Configuration compliance scans**

Verifies that systems are configured correctly, using configuration files. This is configuration validation. Nessus can perform such a scan, and these scans need to be credentialed.

**Testing**

**Pentesting**

Strict boundaries need to be laid out for this kind of testing, because it can result in outages. It can involve the following processes:

* **Passive reconnaissance**: Collecting info using open source intelligence
* **Active reconnaissance**: Using tools to send data to a system, and analysing response. It can also include network scanners
* **Initial exploitation**: Vulnerability scanners can reveal vulnerabilities to an attacker, which the attacker can exploit
* **Privilege escalation**
* **Pivot**: Using various tools to gain additional information
* **Persistence**: Techniques such as creating a backdoor allow attackers to stay in a system for longer.

**Types of testing**

**Black box**: Testers have 0 knowledge of the environment or app, and approach it with the same knowledge as an attacker. They often use fuzzing.

**White box**: Testers have full knowledge of the environment and app and all related docs

**Gray box**: Testers have some knowledge

**Exploitation frameworks**

**Metasploit**: Open source project on Linux, and has data on over 1600 exploits. It also includes tools to test, develop and exploit code.

**BeEF**: Browser exploitation framework, focuses on identifying browser vulnerabilities

**W3af**: Web app attack and audit framework, goal is to find and exploit vulnerabilities and share these with others.

**Security tools**

**Sniffing with protocol analyser**

Can be used to view IP headers and examine packets to troubleshoot or identify attacks using manipulated or fragmented packets.

Attackers can view unencrypted data by connecting a switch within the network to redirect packets to a protocol analyser such as Wireshark.

When using a protocol analyser, the NIC should be configured to use promiscuous mode, where it processes all packets regardless of IP address. This allows it to capture all packets that reach the NIC.

**Command line tools**

**tcpdump**

Command-line packet analyser, which has switches:

* -c: Count, which is the amount of packets it should capture before it stops
* -C: Filesize, which is the max size of packet capture that can be stored in a file. When this is reached, tcpdump is closed and it starts storing packets in a new file.

**Nmap**

A network scanner, that can identify active hosts and their IP addresses, protocols they are running and the host OS. it has these switches:

* T4: Speed of the scan
* A: Indicates that the scan should include OS detection
* -v: Indicates verbosity level. You can get more data output by using -vv or -vvv

**Netcat**

**Echo “” | nc -vv -n -w1 [ip] [port]**

Used to access remote systems, using SSH for encryption. Can be used for banner grabbing. It has these switches:

* -vv for verbose output
* -n to not resolve host names
* -w1 to not wait for more than 1 second
* Echo “” sends a blank command to the server
* | Tells netcat to send command after establishing connection

You can also use netcat for:

* Transferring files
* Port scanner, running against an IP address to specify range of ports it is using

**Monitoring logs for event anomalies**

**OS logs**

Windows systems have event viewer, which lets users view successful and unsuccessful events. Application logs are recorded by apps or programs running on the system, and system logs record events related to the functioning of the OS.

**Firewall and router access logs**

They log traffic that passed through, as well as traffic that was blocked. It also includes packet info

**Linux logs**

Viewable on system log viewer or by using the cat command form the terminal, cat /var/log/auth.log. These logs include:

* var/log/messages: General system activity
* var/log/boot.log: Log entries when system boots
* var/log/auth.log: Contains entries related to successful/unsuccessful logins
* var/log/faillog: Failed login attempts
* /var/log/kern.log: Info logged by system kernel
* var/log/httpd: you can view access and error logs for a system configured as an apache server.

There are also the following files:

* Utmp: Current status, who is logged in
* Wtmp: Archive of utmp file
* Btmp: failed login attempts

**Other logs**

Antivirus logs: All antivirus activity

Application logs: logs to record performance and user activity

Performance logs: monitor system performance

**SIEM**

Security information and event management system, combining security info management (SIM) and security event management (SEM). Features are:

* **Aggregation**: Store and aggregate data in a format that is easy to analyse
* **Correlation engine**: Collects and analyses log data to detect patterns
* **Automated alerting**
* **Automated triggers**: An action in response to a predefined event.
* **Time synchronisation**: All data should be in the same time zone, which makes analysing easier
* **Event deduplication**: Removes duplicate entries
* **Logs/WORM**: Write once read many, prevents users from modifying log entries

**Continuous monitoring**

**User auditing**

Logs info on what users do. Logon attempt logging must be correctly configured, so that logon, as well as resource access, is recorded as a logon action.

**Permission auditing**

Identifies and compares user privileges, privilege escalation and privilege creep, where a user’s privileges change due to a role change, but previous privileges are never removed.

**ACRONYMS**

SLE: Single loss expectancy, the cost of any single loss

ARO: Annual rate of occurrence, how many times the loss will occur in a year

ALE: Annual loss expectancy, SLE \* ALO