Sec+ 501 Get Certified Topic 8 – Using Risk Management Tools

CH 8

- Risk: Likelihood that a threat will exploit a vulnerability
- Threat: Any condition that could cause harm, loss, damage, or compromise to our information technology systems
    - Threats are external and beyond your control
    - Malicious Human threats
        - Script kiddies, APT's, different types of system/network/malware attacks etc.
    - Accidental Human threats
        - Accidently delete or corrupt data or access data that they shouldn't be able to access. Admins can also cause system outages
    - Environmental threats
        - Long term power failure → Chemical spills, pollution.
        - Natural threats such as earthquakes, tsunamis, landslides, electrical storms, tornadoes etc.
- Threat Assessments:
    - Environmental Threat Assessment
        - Evaluates likelihood of an environmental threat occurring
    - Manmade Threat Assessment
        - Evaluates all threats from humans.
    - Internal Threat Assessment
        - Evaluates threats from within an organisation
        - E.G: Malicious Employees
    - External Threat Assessment
        - Evaluates threats from outside organisation.
        - External attackers or natural threats such as earthquakes.
- **Remember this:**
    - **A threat is a potential danger and a threat assessment evaluates potential threats. Environmental threats include natural threats such as weather events. Manmade threats**

are any potential dangers from people and can be either malicious or accidental. Internal threats typically refer to employees within an organisation, while external threats can come from any source outside an organisation.

- Vulnerability: Weaknesses in the design or implementation of a system that a threat could exploit resulting in a security breach. This is due to:
  - Lack of Updates
  - Default Configurations – Should harden system and settings/configurations instead of keeping to default
  - Lack of malware protection or updated definitions
    - E.G: Antivirus
  - Lack of firewalls
  - Lack of organisational policies
- Residual Risk
  - The risk remaining after trying to avoid, transfer, or mitigate the risk
- Risk Management:
  - The practice of identifying, monitoring and limiting risks to a manageable level. Identifies methods to limit or mitigate them.
  - Main goal: Reduce risk to a level that organization will accept.
- Risk Response Techniques:
  - Risk Avoidance
    - A strategy that requires stopping the activity that has a risk or choosing a less risky alternative
    - E.G: Use a different application for firewall, instead of opening additional firewall ports for a specific application
  - Risk Transfer
    - A strategy that passes the risk to a third party or another entity
    - E.G: Purchase Insurance
  - Risk Mitigation

        - A strategy that seeks to minimize the risk to an acceptable level. Organisation implements controls to reduce risks
        - E.G: Security guard or up to date antivirus to reduce malware threats
    - Risk Acceptance
        - A strategy that seeks to accept the current level of risk and the costs associated with it if the risk were realized
        - E.G: Instead of spending $100 in locks to secure $15 mouse, just accept the risk
- **Remember this: It isn't possible to eliminate risk, but you can take steps to manage it. An organization can avoid a risk by not providing a service or not participating in a risky activity. Insurance transfers risk to another entity. You can mitigate risk by implementing controls, but when the cost of the controls exceeds the cost of the risk, an organization accepts the remaining/residual risk.**
- Risk Assessment: Quantifies or qualifies risks based on different values or judgements. First starts by identifying assets and asset value.
    - 1. Identify Asset Values
    - 2. Identify threats and vulnerabilities and determines likelihood a threat will attempt to exploit a vulnerability
    - 3. Includes recommendations to mitigate risk
- Use quantitative measurements or qualitative measurements. Common to perform risk assessments on new systems and applications.
- Asset: Any product, system, resource, or process that an organization values
- Asset value: The worth of an asset to an organization.
    - Can be specific or subjective such as low, medium, high.
- Quantitative risk assessment:
    - Uses numerical and monetary values to calculate risk
    - Quantitative analysis can calculate a direct cost for each risk
- **SLE (Single Loss Expectancy): Cost of any single loss**

- **ARO (Annual rate of occurrence): ARO indicates how many times the loss will occur in a year. If ARO < 1, ARO is presented as a % such as once every 2 years = .5 or 50%**
- **ALE (Annual Loss Expectancy): SLE x ARO**

- Single Loss Expectancy (SLE)
  - Cost associated with the realization of each individualized threat that occurs

Asset Value x Exposure Factor

SLE = AV x EF

SLE = $10,000 x 20%

SLE = $2,000

- Annualized Rate of Occurrence (ARO)
  - Number of times per year that a threat is realized
- Annualized Loss Expectancy (ALE)
  - Expected cost of a realized threat over a given year

ALE = SLE x ARO

- **Remember this:**
  - **A quantitative risk assessment uses specific monetary amounts to identify cost and asset values. SLE identifies the amount of each loss, ARO identifies number of failures in a year, and ALE identifies the expected annual loss. You calculate ALE as SLE x ARO. A qualitative risk assessment uses judgement to categorize risks based on likelihood of occurrence and impact.**
- Qualitative Risk Assessment: Uses judgement to categorize risks based on likelihood of occurrence (probability of impact) to exploit a vulnerability.
  - E.G: Surveys, Focus groups
  - Common to assign numbers such as 1-10 and impact of each risk using low ,medium and high changing words to numbers.
  - Challenges: Gaining consensus and impact
- Report: Final Phase of Risk Assessment.
  - Identifies risks discovered and recommends controls

- Risk Registers:
  - Comprehensive document listing known information about risks. Typically includes risk scores along with recommended security controls to reduce the risks scores.
  - May include:
    - Categories
      - E.G: Hardware failures, Outages, Downtime etc.
    - Specific Risk
      - E.G: Hard Drive failure
    - Likelihood of occurrence
      - E.G: Medium
    - Impact
      - E.G: High
    - Risk Score
      - E.G: 60 out of 100
    - Security controls or mitigations
      - E.G: Implement RAID-1 to protect hard drive etc.
    - Contingencies
      - E.G: Ensure backups exist and kept up to date
    - Risk score with security controls
    - Action assigned to
      - E.G: Document who has responsibility for implementing security control
    - Action deadline
      - When security deadline should be implemented.
- Supply Chain Assessment:
  - Evaluates everything needed to produce and sell a product. Includes all raw materials and processes required to create and distribute a finished product.
- **Remember this:**
  - **A risk register is a Comprehensive document listing known information about risks. Typically includes risk scores along with recommended security controls to reduce the risks scores. A supply chain assessment evaluates everything needed to produce and sell a product. Includes all raw**

materials and processes required to create and distribute a finished product.

- Password Cracker: Attempts to discover a password
  - E.G: Cracking MD5 Hash
  - Offline Password Cracker: Attempts to discover password by analysing a file containing passwords or a database.
  - Online Password Cracker: Attempts to discover passwords by guessing them in a brute force attack. Some online password crackers collect network traffic and attempt to crack passwords sent over network.
- Network scanner: Scanner that uses various techniques to gather information about hosts within a network. E.G: Nmap/Zenmap
  - Ping scan/Ping sweep – Sends ICMP ping to a range of IP addresses in a network. If host responds, network scanner knows there is a host operational with that IP address.
    - May not work with a firewall as a firewall may block requests
  - ARP ping scan – Any host that receives an ARP packet with its IP address responds with its MAC address. If host responds, network scanner knows host Is operational with that IP address.
  - Syn Stealth Scan – TCP three-way handshake with ACK packet completion for connection. A syn stealth scan sends single SYN packet to each IP address in scan range. If host responds, scanner knows host is operational with IP address. Instead of ACK packet, scanner usually sends an RST(reset) response to close connection.
  - Port scan – Checks for open ports on a system and gives hints about what protocols or services might be running.
  - Service scan – Like a port scan but a bit more advanced. Verifies protocol or service being used.
    - E.G: Port 80 open, Get/. As the HTTP command. Will respond to Get command if used.
  - OS Detection – Analyse packets from an IP address to identify OS. Usually called TCP/IP fingerprinting.

- Remember this:
    - Password crackers attempt to discover passwords and can identify weak passwords. Network scanners can detect all hosts on a network including the OS and services or protocols running on each host.
- Network Mapping: Discovers devices on the network and how they are connected with each other. Usually done via network scan but focuses on connectivity.
- Wireless Scanners/Cracker: Can act passively or actively
    - Passive: Listens to all traffic being broadcast on known channels within 2.4GHz-5GHz frequencies.

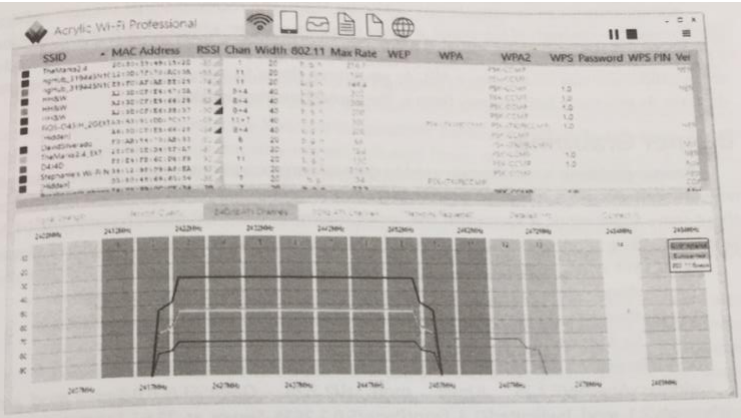


Figure 8.2: Acrylic Wi-Fi Professional

The following bullets describe some of the columns in Figure 8.2:

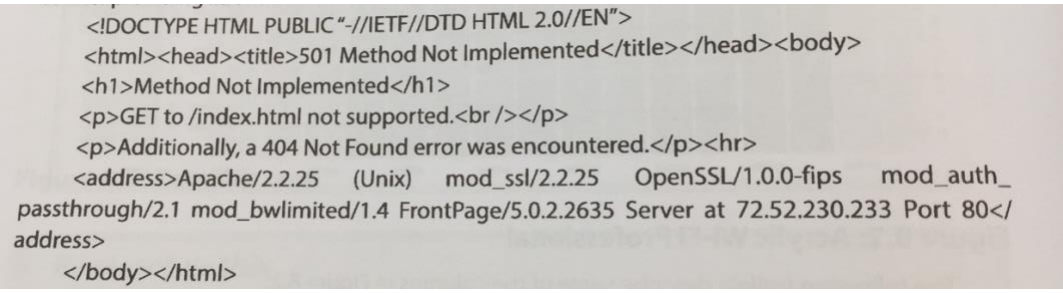
- **SSIDs.** A scanner will detect the service set identifier (***SSID***) of all access points within range of the scanner.
- **MAC addresses.** It shows the MAC, or hardware address of the AP.
- **Signal strength.** The signal strength typically identifies how near (or how far away) the AP is in relation to the computer performing the scan.
- **Channels.** This helps administrators determine if nearby APs are broadcasting on the same channel, causing interference.
- **Channel widths.** A channel is typically 20 MHz wide, but when an AP is using two channels, it is 40 MHz. The scanner will show this information.
- **Security.** The scanner will show if the AP is in Open mode or using one of the other wireless cryptographic protocols: Wi-Fi Protected Access (***WPA***) or Wi-Fi Protected Access II (***WPA2***). Chapter 4 discusses these modes in more depth.

When using an active scan, a wireless scanner acts like a scanner/cracker and can gain more information about an AP by sending queries to it. As an example, Chapter 4 discusses various attacks, including Wi-Fi Protected Setup (***WPS***) attacks. A WPS attack keeps guessing PINs until it discovers the eight-digit PIN used by an AP. It can then use this to discover the pre-shared key (PSK) used by the AP. Various wireless scanners have other capabilities, including password crackers using other methods.

Rogue System Detection

Chapter 4 discusses rogue APs, which are APs placed into service without authorization. As long as an administrator knows what APs are authorized, it's easy to discover rogue APs with a wireless scan. Administrators often perform site surveys while planning and deploying a wireless network. As an example, Figure 8.2 (the screenshot from Acrylic Wi-Fi Professional in the previous section) shows all the SSIDs it has detected.

- Admins can investigate any unknown SSIDS. Received Signal strength indicator (RSSI) shows strength of signal. A lower negative number is stronger than a higher negative number. Installing wireless scanners can detect rogue AP's.
- Banner Grabbing: Technique used to gain information about remote systems and many network scanners use it. Used to identify OS with information about some applications.
    - E.G:



```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head><title>501 Method Not Implemented</title></head><body>
<h1>Method Not Implemented</h1>
<p>GET to /index.html not supported.<br /></p>
<p>Additionally, a 404 Not Found error was encountered.</p><hr>
<address>Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.0-fips mod_auth_
passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Server at 72.52.230.233 Port 80</
address>
</body></html>
```

- **Remember this:**
    - **Wireless scanners can detect rogue AP's on a network and sometimes crack passwords used by access points. Netcat can be used for banner grabbing to identify the OS and some applications and services on remote servers.**
- Vulnerability scanner: Does not attempt to exploit vulnerabilities. Is more passive. Penetration tests are more active.
    - Identifies vulnerabilities
    - Identifies misconfigurations
    - Passively test security controls
    - Identify lack of security controls
- Some vulnerabilities and common misconfigurations discovered by vulnerability scanners include:
    - Open ports
    - Weak passwords
    - Default accounts and passwords still used
    - Sensitive Data
    - Security and configuration errors
- **Remember this:**
    - **A vulnerability scanner can identify vulnerabilities, misconfigured systems, and the lack of security controls such as up-to-date patches. Vulnerability scans are passive and have little impact on a system during a test. In contrast,**

a penetration test is intrusive and can potentially compromise a system.

- Credentialed scan: Scan uses credentials of an account
  - Allows scan to see more information and results in fewer false positives.
- Non – Credentialed scan: scan without user credentials
- Attacks usually start without credentials but then use privilege escalation techniques to gain administrative access allowing them to run a credentialed scan if desired. Although Credential scans are more accurate, admins use non-credential scans to see what an attacker might see
- **Remember this:**
  - **A false positive from a vulnerability scan indicates the scan detected a vulnerability, but the vulnerability doesn't exist. Credentialed scans run under context of a valid account and are typically more accurate than non-credentialed scans.**
- Configuration compliance scanner – verifies systems are configured correctly. Usually run as credentialed scans.
- Must obtain vulnerability testing authorization and penetration authorization before performing any testing.
- Penetration testing: Actively assesses deployed security controls within a system or network. Starts with passive reconnaissance such as a vulnerability scan, but takes it a step further and tries to exploit vulnerabilities by simulating/performing an attack.
  - Includes:
    - Passive reconnaissance
      - Collects information about a targeted system, network or organisation using open-source intelligence. Includes viewing social media and organisation's website.
    - Active reconnaissance
      - Includes tools to send data to systems and analyse responses. Usually use network and vulnerability scanners. Is Illegal when engaging with targets without authorization.
    - Initial Exploitation

        - After scanning target, testers discover vulnerabilities and try to exploit it.
    - Escalation of privilege
        - Escalate privileges to admin access
    - Pivot
        - Using various tools to gain additional information. Is the process of using an exploited system to target other systems.
    - Persistence
        - Use techniques/threats to stay hidden within a network for weeks, months, years without being detected. Usually created through backdoors such as creating alternate accounts.
- Black-box Testing
    - Occurs when a tester is not provided with any information about the system or program prior to conducting the test
    - Usually use fuzzing
- White-box Testing
    - Occurs when a tester is provided full details of a system including the source code, diagrams, and user credentials in order to conduct the test
- Grey-box testing
    - Have some knowledge of system prior to a penetration test but not all of it unlike a white box.
- Intrusive:
    - Tools that potentially disrupt operations of a system
- Non-Intrusive:
    - Tools that don't disrupt operations of a system.
- Penetration tests are more intrusive than vulnerability tests.
- **Remember this:**
    - **A vulnerability scanner is passive and non-intrusive and has little impact on a system during a test. In contrast, a penetration test is active and intrusive, and can potentially compromise a system. A penetration test is more invasive than a vulnerability scan.**

- Exploitation Frameworks:
    - Tool used to store information about security vulnerabilities. Usually used by pen testers.
        - Metasploit Framework
        - BeEF (Browser Exploitation Framework)
        - W3af (Web application attack and audit framework)

SECURITY TOOLS

- Protocol Analyzer – Capture and analyse packets on a network. Can also be referred to as a sniffer/sniffing. E.G: Wireshark
    - View IP headers and examine packets.
    - Capture data cross network in cleartext
    - Find unencrypted credentials
- PAT – Port address translation
    - Translates public and private IP addresses. If traffic goes through a device via PAT, protocol analyser only captures IP address not original IP address.
- **Remember this:**
    - **Administrators use a protocol analyser to capture, display, and analyse packets sent over an network it is useful when troubleshooting communication problems between systems. Useful to detect attacks that manipulate or fragment packets. A capture shows information show as the type of traffic (protocol), flags, source and destination IP addresses, and source and destination MAC addresses. The NIC must be configured to use promiscuous mode to capture all traffic as it is usually in non-promiscuous mode by default.**
- Command Line Tools:
    - Tcpdump
        - cmd packet/protocol analyser. Like Wireshark but in cmd.
            - -c represents count and indicates capture should stop after receiving specified no. of packets
            - -C represents file size and indicates maximum size of packet capture.

- Nmap
  - Network Scanner. Zenmap is the GUI version.
  - Identifies all active hosts and IP addresses in a network, protocols and services running on each host and OS of system.
  - E.G: nmap -T4 -A -v 192.168.0.0/24
    - -T4 refers to speed of scan. Valid switches are from T0 – T5. T0 is slower but stealthier, T5 is faster but less stealthier
    - -v stands for verbose to get more data output
    - -A indicates scan should include OS detection
- Netcat
  - Used in banner grabbing and to remotely administer systems and gather information in such remote systems. Doesn't use native encryption so its common to use SSH instead.
  - Banner Grab E.G:
    - Echo "" | nc -vv -n -w1 72.52.206.134 80
    - Nc – netcat
    - -vv for more verbose data output
    - -n to not resolve hostnames
    - -w1 to wait no more than 1 second for a reply
    - Connects to port 80 with ip 72.52.206.134
    - Echo "" sends black command to server, | pipe symbol tells netcat to send command after establishing connection
  - Netcat can also be used to scan ports and transfer files

- **Remember this:**
  - **TCPdump is a cmd protocol analyser. Can create packet captures that can then be viewed via wireshark. Nmap is a sophisticated network scanner that runs on the cmd. Netcat can be used to remotely administer systems and also gather information on remote systems.**

- Operation System Event Logs
  - Basic Logs that record events
    - Application
      - Application log record events by applications or programs running on system.
    - System
      - System log to record events related to functioning of OS such as when it starts, when it shuts down, services starting/stopping, driver loading etc.
- Firewall Router Access Logs
  - Can configure firewalls/routers to log information such as traffic that passes through. Good for troubleshooting connectivity issues and potential intrusions
- Linux logs
  - Cat /var/log/auth.log – Authentication log
  - Var/log/messages – General System Message Logs
  - Var/log/boot.log – Log entries of system boot
  - Var/log/auth.log – Authentication log contains information on successful/unsuccessful login attempts
  - Var/log/faillog – Contains information on failed login attempts
  - /var/log/kern.log – Kernel Log containing information logged by system kernel
  - /var/log/httpd – If system configured as an Apache Web server use this directory.
- **Utmp, wtmp, btmp files –**
  - Usually within /var/log folder
  - Created so administrators can answer questions such as who is currently logged in, who has logged in recently, what accounts have failed login attempts
- UTMP file – Maintains information on current state of system including who is logged in.
- WTMP file – archive of UTMP file. Shows last logged-in users

- BTMP file – Records failed login attempts. Lastb command shows last failed login attempts

- Other Logs:
  - Antivirus Logs
  - Application Logs
  - Performance Logs
- **Remember this:**
  - **Logs record what happened, when it happened, where it happened, and who did it. By monitoring logs, administrators can detect event anomalies. Additionally, by reviewing logs, security personnel can create an audit trail.**
- SIEM – Security Information and Event Management System [E.G: Splunk]
  - **Remember this: SIEM provides a centralized solution for collecting, analysing and managing data from multiple sources. Typically includes aggregation and correlation capabilities to collect and organize log data from multiple sources. Also provides continuous monitoring with automated alerts and triggers.**
  - Useful in large enterprises with massive amount of data and activity monitoring.
- SIEM uses:
  - Aggregation – Combining dissimilar items into a single item. SIEM can collect data from multiple sources such as firewalls ,IDS etc. to make it easy to search
  - Correlation Engine – Correlate/ Analyze event log data within network
  - Automated alerting.
  - Automated Triggers
  - Time Synchronization
  - Event deduplication – Removal of duplicate entries.
  - Logs/WORM – Prevent anyone from modifying log entries.
- Continuous Monitoring
  - Monitoring all relevant security controls, with goal of ensuring organization maintains strong security posture.

Periodic threat/vulnerability/risk assessments and tests are also used including vulnerability/penetration tests. Also companies routinely check via auditing reviews.

- User auditing/ User auditing review
  - Logging information on what users do and reviewing them
- Permission auditing/ review
  - Looks at rights and permissions assigned to users to help ensure principle of least privilege is enforced.
- Privilege creep/bloat: Occurs when a user gets additional permission over time as they rotate through different positions or roles
  - Privilege creep violates the principles of least privilege
- **Remember this:**
  - **Usage auditing records user activity in logs. A usage auditing review looks at logs to see what users are doing and it can be used to recreate an audit trail. Permission auditing reviews help ensure that users have only the access they need and no more and can detect privilege creep issues.**