Unit 3
Network security
Lecture cast

Unit 3
Network security
Lecture cast

Vulnerability assessments can be represented as a continuum from mostly paper-based, internal reviews (as exemplified by the cyber essentials process (NCSC, 2021) to a blueprint for a full attack (as discussed as part of the cyber kill chain (Hutchins et al, 2011).

CREST – independent organisation that provide formalised Pen Testing.

NIST vulnerability is defined as:
"*(a) weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."*

Therefore, an assessment involves the audit, detection and/or evaluation of such weaknesses. A penetration test (or pen test) can be seen as a specialised, often more in-depth, form of vulnerability assessment.

Public company info

Assess ID and analysis audit

- web assets
- IP address;
    - its configuration (CPU, Memory, etc);
    - the operating system details (including version);
    - any middleware and/or frameworks utilised (including version details);
    - any scripts and programming languages used (and versions);
    - the number, type and version of database systems used;
    - usernames and passwords used by the application;
    - and (if appropriate) any repositories used,
    - and passwords required to access them
    - person responsible for this task
- Human assets
- Physical assets

Detect

<table>
<tr><th>Human asset</th><th colspan="2">Web asset</th><th>Psychical asset</th></tr>
<tr><td rowspan="3">Weakest link;
Username and passwords
Password storage; hashed, is salt used? Does the system use and enforce roles for authentication?</td><td>Cloud</td><td>Type of platform, ip address, configuration, OS, scripts, programming languages</td><td rowspan="3">Routers, servers, laptops, computers, mobile devices</td></tr>
<tr><td>Shared server</td><td></td></tr>
<tr><td>Company premesis</td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
</table>

Scanning policies

Scanning policies should include assets to scan, IPs and ports to be included, and an indicative list of tools to utilise, based on advice from external bodies, plus internal priorities based on business criticality. Scans can be conducted externally (I.e. outside the network perimeter of the company) or internally (inside the network perimeter).

External scans	Internal scans
Scans carried out by external organisations, but can be executed by employees	Carried out on a regular basis by company employees

The number and frequency of scans will depend very much on the purpose of the scan (whether it is just a vulnerability check or a full pen test) and the time of the day that the scans are carried out – more care must be taken during normal business hours to avoid business disruption.

Tools

Several independent tests of various vulnerability scanners (including the ones listed) highlight the fact that each tool detected a different set of vulnerabilities on the scanned host(s) - which often leads to a recommendation of using multiple tools.

Nmap

In general, it is better to use tools that can scan at higher levels of the network stack when dealing with shared hosting sites.

Audit of underlying host itself

IDS

The most common tool deployed when scanning or auditing a host platform is a host-based intrusion detection system (HIDS). Most HIDS operate by creating a hash of key system files or objects (such as the etc/shadow or etc/passwd on Unix systems, or the registry hives such as HKEY_USERS files on Windows). If these files change unexpectedly (for example, without corresponding log entries or equivalent), the HIDS can trigger an alert. Commonly utilised applications for this function include Snort, which can act as both a HIDS and NIDS (network intrusion detection system), and Tripwire. NIDS often use externally managed databases of signatures to detect and track network intrusion attempts (Rubens, 2015). Many commercial anti-virus suites offer similar functionality.

Hardware audits

Hardware audits are often carried out by network-based tools. One of the most common is Microsoft Configuration Manager (which used to be called Microsoft SCCM – system centre configuration manager). This can often help if low-level viruses attempt to change BIOS or firmware code, or if third parties have hijacked your server(s) to use as part of their botnet farms.

Loganalysis

The final aspect of host scanning is log analysis and auditing, which will be dealt with separately in a later section.

Wireless scans

Kismet

The traditional, most flexible of the wireless scanning and auditing tools is Kismet (Kismet, 2022) which can probe wireless interfaces, 'sniff' network traffic and even act as a WIDS (wireless intrusion detection system). It is also available as part of the Kali Linux distribution (see later).

Aircrack-ng

A more focused tool is aircrack-ng (and its associated suite) which is designed to capture and extract keys and passphrases from encrypted wireless traffic. A paper by Carranza et al (2018) provides a tutorial for using Kismet, aircrack-ng and associated tools.

MS CM (SCMM)

Microsoft configuration manager (discussed previously) provides a number of services that can be used to audit and manage applications, including deployment, the enforcement of group policies, and the management of automated updates.

Apparmor

On Unix-like systems (particularly Linux), there is a tool called AppArmor which "provides MAC functionality to Linux and is used to supplement the traditional DAC (file permissions) functionality that the OS provides." (Shamim, 2016). Essentially, it provides profiles that can be used to monitor (log) or prevent applications from accessing resources and being utilised by unauthorised users. So AppArmor can be used for both auditing and management of applications.

Internet protocol Suite

PING

- PING is one of the oldest utilities that uses the IP stack. Its main purpose is to determine if a specific host is available, and to also calculate the round trip time (RTT) required to send a basic message from a source to a target address and receive a reply.
- PING uses the ICMP (Internet Control Message Protocol) message format.
- PINGs can also be used to determine the number of active nodes receiving (a so-called Ping Sweep) - which is a clue to where the name comes from (the sound made by sonar equipment scanning for other vessels). Although there is an urban legend (circulated by one of the developers) that states it is an acronym for Packet Internet Groper.

TRACEROUTE

- Traceroute is a utility that is used to display a route between two hosts, as well as calculating the transit delay caused by the routers traversed during the journey.
- On most Unix based systems traceroute uses UDP packets but most versions have an option to use other protocols (such as TCP or ICMP) instead.
- On some Windows systems the default protocol used is ICMP. Traceroute uses a function known as TTL (time to live) to count the number of routers (known as hops) between two nodes.
- Traceroute can experience problems on some modern systems because routers may refuse to respond to certain probe requests.
- It can also get confused by load balanced systems, which can result in it responding with a path not found error.

NSLOOKUP/ DIG

- NSlookup (name server lookup) is a utility used to query the DNS (domain name server) system. DNS is the service that translates URL (uniform resource locator) into IP addresses. For example, www.bbc.co.uk is translated by DNS into 151.101.128.81 (its IP address).
- It is often used in 'interactive' mode where typing the command produces a > prompt. Typing exit returns you back to you normal system. DIG (rumoured to be Domain Internet Groper) is a more modern version of nslookup, with more features.

WHOIS

- WHOIS is a Unix utility that is commonly used to query the Internet registrar databases.
- These tools are often used by attackers to try and discover information about a company that can assist with social engineering and/or denial of service attacks.
- There are some interesting examples in the Network Security Assessment book by O'Reilly (given in the list of references).

NETSTAT

- Netstat (network statistics) is a multiplatform utility used to show the active connections from a system to external hosts.
- It is deprecated on Linux systems but still provides useful information from a security perspective, with reference to the number of open channels or ports on the system.
-

Internet/web based services

- There are several third-party, web-based utilities that provide a basic system check for home-based systems – one of the oldest (but still very useful) is found at www.grc.com (then click on ShieldsUp on that page to access the scanning systems).
- This will test which ports are open on your system and also how good the security of your internet gateway/router is (for example, how much information does it expose?).

Spider

- A final tool type often used by attackers (as well as search engines) is a web spider – this tool will work its way through every page available on your website and index (or download) the HTML to reconstruct it offline.
- An invaluable tool both for attackers and search engines as it can help reveal contact information, database links and much more.
- They can also be used to launch a type of denial of service attack on a site by overloading it as it demands that it downloads certain pages.
- The robots.txt file (usually kept in the root of a website) is used to manage the level of access a typical crawler has, although some crawlers used by attackers deliberately ignore the settings specified.

Packet diagnostics

TCPDump

TCPDUMP is a Unix-style, command line tool found on most modern Unix like systems (e.g. BSD, Linux, etc). That means it is usually shipped as standard on most modern xBSD and Linux systems.

For example, it is shipped as standard as part of a modern Macintosh system. It is a command line utility that captures TCP/IP packets on a nominated interface – so it will work with both wired (ethernet) and wireless (WLAN) interfaces. It can display traffic either on the console or capture packets and write them to a file. It is controlled, like many CLI tools, by arcane combinations of command line switches. Help is available either via the '--h' CLI option or via standard Unix MAN pages. There is a Windows version available, but the next tool discussed is preferable due to ease of use.

Wireshark

WIRESHARK performs a similar function to TCPDump except it is a GUI based tool, and is available for multiple platforms including Linux, MacOS and Windows. It is an open-source packet analyser and a typical user screen is shown in figure 10.

Figure 10 - wireshark screenshot on linux

Unit 3
Network security
Lecture cast

Vulnerability and Portscanners

Nmap

Nmap is another command line-based scanning tool. It is usually used for service and OS discovery as part of a vulnerability scan. There are several GUI front ends available – the image shown in figure 11 is of the ZenMap variation.

Nessus

Nessus is a commercial vulnerability scanner, again available for multiple platforms.

OpenVAS

OpenVAS (the open vulnerability assessment system) is an open-source tool, based on the same core as Nessus. It is a server-based system, available as a downloadable image that runs within a virtual machine – as such it is a form of virtual appliance. It is designed to be controlled by the host machine – which means the VMM needs to be configured to receive network traffic both from the internet and the host machine itself. The main difference between tools like Nmap and Nessus derivatives is the presence of a data feed that contains information about known vulnerabilities and how to detect them.

Kali Linux

The final toolset on the list is Kali Linux – short for Kernel Auditing Linux it is a Linux distribution that comes pre-packaged with many testing tools including Wireshark, NMap and many others. It is available as a 'live' distribution (I.e. requires no installation) on DVD or USB and also runs within a VM. A guide to Kali is given in the references.

Portscan

Prediction to be port 80, and fingerprinting should reveal the existence of a PHP framework.

Expectation

Typically, a scan should be designed to identify the platform, its operating system, and any middleware and/or frameworks in use. It should scan for the ports expected to be in use but should also check other common (and possibly fewer common ports) and check for expected vulnerabilities based on previous research.

Assessing risk of scan

- Whilst scanning in progess, might cause pseudo DoS attack
- Have effect on IPS/IDS systems

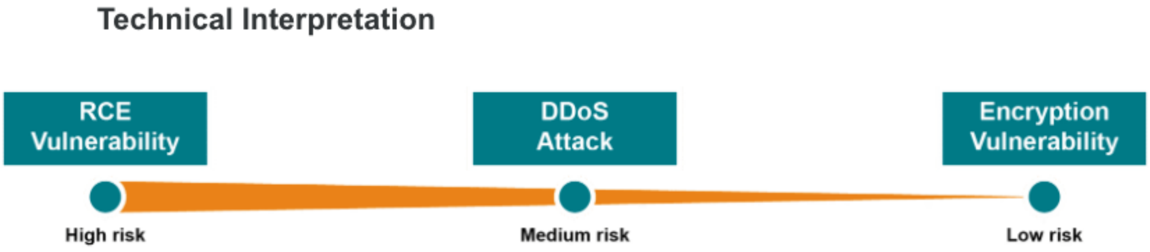
After the scan

Reports of expected outcome, actual outcome, and failures.

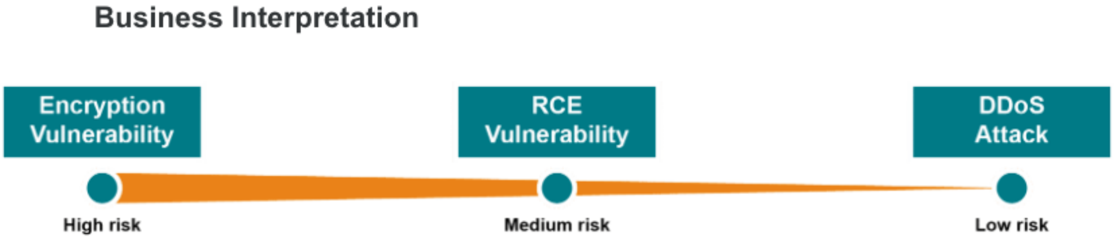
As discussed previously, failures need to be logged, investigated, and explained as often, such failures are indicative of possible unknown and/or unmanaged vulnerabilities. For example, if the scan discovers an open port that is not associated with services – or known services – the existence of that open port should be investigated and explained.

Present results

As part of the interpretation phase, results should be ranked based on both technical and business priorities. Technical priorities include the risk to the business. For example, a vulnerability that could result in remote code execution (RCE) (which could cause a system to crash, or provide a third party with remote access to, and control of, the system, would be ranked higher than a distributed denial of service (DDoS) attack which would typically result in a temporary slowdown or outage and usually requires a much more sophisticated attacker. From a technical perspective, a vulnerability that results in a lack of encryption, or decryption of certain resources may be ranked lower as it would have a limited effect on the operation of the system.



However, from a business perspective, these rankings may be very different. For example, a DDoS attack that might only cause a slowdown or temporary outage might be ranked as the lowest business priority; the RCE might be ranked as a medium priority (depending on how easy it might be to exploit) whereas the lack of encryption/decryption might be ranked as the highest priority due to the fines that could be incurred by breaching regulations such as the European GDPR.



Presentation should include:

- Discussion on the cost and ease of remediation
- Risk analysis that covers probability/possibility that a vulnerability could be excluded

Unit 3
Network security
Lecture cast

remember to make the presentation as engaging and as easy to understand as possible; use graphics where feasible; present results in ranked order (and present business priorities before technical ones); and avoid jargon, abbreviations and TLAs (three-letter acronyms) as they are not universally understood, or even agreed on.

The final step is to create a remediation/mitigation plan. This must be done carefully and judiciously, involving all stakeholders but especially in co-operation with the business IT team. Priorities should be reviewed again with an eye to look at which mitigations might be able to be included/integrated with existing plans and objectives. For example, if the IT department have a plan to upgrade all on-premises servers to the latest version of Windows, or to move to Linux, look at how that might mitigate some of the vulnerabilities discovered. Always create a fully costed plan and ensure that you get stakeholder buy-in and approval before proceeding.
When carrying out the remediation, create a deployment plan with the IT department (as they will often provide some or all of the deployment resources), and follow it. Schedule mitigations to be deployed alongside other work (for example, if a new application server is due to be installed, deploy the new security proxy/firewall at the same time.)

Firewalls

Most well-known security device in use
Available psychical, software applicated and virtual appliance

In the most simplistic definition, a firewall is a filter that sits between a trusted zone (e.g. a LAN) and an untrusted zone (e.g. the Internet) and monitors and filters the packets sent between them, based on a set of rules.

critical items to check with any firewall deployment:

1. Does it have strong password that is not the default?
2. Does it have security certificates installed and enabled for all communications – internal and external
3. Has the configuration been checked and backed up?
4. Are users prohibited from changing or disabling firewall settings?
5. Is it regularity patched?
6. Are the security bulletins from the vendor checked regular and acted upon?
7. If an external device, does it have UPS and a failure alarm?
8. Is logging enabled and either regularly checked and backed up or routered to a SIEM?