Unit 3: Vulnerability Assessments

1. **Select and explain which assessment regime to use based on the type and size of the target business.**

Conducting a vulnerability assessment is paramount in identifying, classifying, and prioritising vulnerabilities in computer systems, applications, and networks (Neagu, 2023). This comprehensive process may involve automatic and manual methods, including network-based scans, host-based assessments, database assessments, and application scans. The vulnerability assessment stages typically consist of vulnerability scanning, analysis, risk assessment, and remediation or mitigation. It is critical to regularly conduct this process to ensure that security gaps are closed and new vulnerabilities are identified.

HackerOne (N.D.) highlight that vulnerability assessment is crucial for preventing security breaches. It helps identify security vulnerabilities in operating systems, business applications, endpoint devices, and browsers. Violations can occur due to technology issues or user behaviour. Modern vulnerability assessments rely on automated scanning tools, including network-based, host-based, wireless network, application, and database scans.

The Vulnerability Assessment Process, consisting of five key steps, is an essential tool for security teams across all industries. These steps include preparing, conducting vulnerability tests, prioritising vulnerabilities, creating a report, and conducting ongoing assessments (HackerOne, N.D.). This process allows security teams to identify potential attack surfaces and vulnerabilities and craft a comprehensive remediation plan. Vulnerability management must be implemented continuously to catch any

vulnerabilities, as even a single exposure can have devastating consequences for an organisation's digital infrastructure.

Several important variables must be considered when choosing an adequate evaluation regime (OECD, 2019). These include the kind and size of the company being assessed, the sector in which it works, and its general risk tolerance. A thorough evaluation programme that best meets the unique requirements and objectives of the concerned organisation can be developed by considering these criteria. Still, the following broad principles can be adhered to:

1. **Small enterprises:** An open-source tool-based basic vulnerability assessment may be adequate for small businesses with minimal resources. Such an evaluation can pinpoint widespread weaknesses and offer suggestions for fixing them.
2. **Businesses in the medium-size range:** Companies in this size content would want to do a more thorough vulnerability assessment, including penetration testing. Automated techniques could miss more complex vulnerabilities, which penetration testing might assist in finding.
3. **Big businesses:** Big businesses with intricate IT systems want to consider employing a continuous monitoring strategy for vulnerability control. This method entails checking regularly for fresh vulnerabilities and installing updates as soon as they become available.

2. **Utilise open-source scanning and testing tools to perform vulnerability tests and scans.**

Several open-source scanning and testing tools can be used to perform vulnerability tests and scans. Here are a few examples:

1. **Nmap:** Nmap is a network scanner that can be used to identify hosts and services on a network.
2. **Nessus:** Nessus is a vulnerability scanner that can identify known vulnerabilities in systems and applications.
3. **OpenVAS:** OpenVAS is a vulnerability management tool that can be used. Several open-source scanning and testing tools can be easily used for vulnerability tests and scans.

I do want to focus on a few of the most well-known ones. To begin with, Nmap is a potent network scanner that can locate hosts and services on a network. The second is Nessus, a powerful vulnerability scanner that finds known weaknesses in programs and systems. Last but not least is OpenVAS, a feature-rich vulnerability management tool that can be used to evaluate risk, find vulnerabilities, and track the status of fixes. These tools benefit anyone trying to strengthen the security posture of their network and guard against possible threats. Monitor the status of remediation, evaluate risk, and search for vulnerabilities.

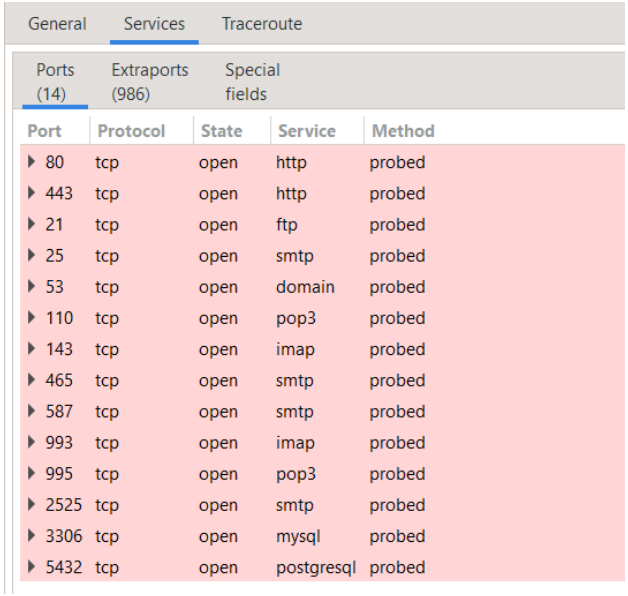
4. **Analyse scanning results and make recommendations to mitigate vulnerabilities.**

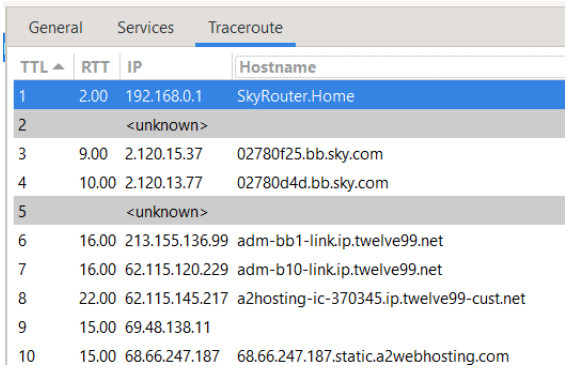
Based on the tests conducted, I have thoroughly explored the vulnerabilities and arrived at some significant results. Allow me to elaborate on the categories of these vulnerabilities and my mitigation plan.

Firstly, let's discuss the categories of vulnerabilities that I have identified. These include both software and hardware vulnerabilities, as well as network and physical security concerns. Each class has been closely examined, and I have devised specific solutions to address each.

As for the mitigation plan, I have taken a multi-faceted approach. This includes implementing new security protocols, upgrading software PHP, and providing training and education to web administrators to ensure they know potential security risks. I have also established contingency plans for a security breach and have implemented measures to ensure that any violation is detected and dealt with swiftly.

I am confident that my mitigation plan is comprehensive and practical, and I am committed to maintaining the highest level of security for the webpage and its administrators.





Vulnerabilities Detected

Title	Result	Description	Score	Info
Content Security Policy	×	CSP header is not implemented	-25	ⓘ
Cookies	×	Cookies are sent with insecure tags.	-5	ⓘ
Cross-origin Resource Sharing	✓	CORS header and files are properly implemented and only allows controlled access to resources outside the domain	10	ⓘ
Public-Key-Pins	–	HTTP Public Key Pinning (HPKP) header not implemented(optional)	0	ⓘ
Strict-Transport-Security	✓	HTTP Strict Transport Security(HSTS) header is implemented properly	10	ⓘ
Redirection	✓	Initial redirection and final redirection is to HTTPS	5	ⓘ
Referrer Policy	✓	Referrer-Policy is set to strict-origin-when-cross-origin	5	ⓘ
X-Content-Type-Options	✓	X-Content-Type-Options is set to nosniff	5	ⓘ
X-Frame-Options	✓	X-Frame-Options (XFO) header set to SAMEORIGIN	5	ⓘ
X-XSS-Protection	×	X XSS Protection is not implemented	-10	ⓘ

References:

- Neagu, C. (2023). *What Is Vulnerability Assessment?* [online] Available at: https://heimdalsecurity.com/blog/vulnerability-assessment/.
- HackerOne (N.D.). *What Is Vulnerability Assessment? Benefits, Tools, and Process | HackerOne*. [online] www.hackerone.com. Available at: https://www.hackerone.com/knowledge-center/what-vulnerability-assessment-benefits-tools-and-process.
- OECD (2019). *Corporate Governance Risk Management and Corporate Governance*. [online] Available at: https://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf.