Crowe Horwath.

April 2014

The Pros and Cons of Vulnerability Assessments and Penetration Tests

By Raj Chaudhary, PE, CGEIT and Christopher R. Wilkinson, CISSP

Identifying vulnerabilities in a timely manner is a function critical to the risk management process for all organizations. Vulnerability assessments and penetration tests provide similar services but offer very different types of value to a organization. Often this value is not fully understood by the risk management function. Ultimately, the organization, based on its risk assessment as well as its IT infrastructure and management's input, needs to determine what assessment or combination of assessments best fits its IT security strategy.

Typically, a combination of both types of assessments is necessary for a robust vulnerability management program. That said, each type has particular benefits and disadvantages.

Vulnerability Assessments

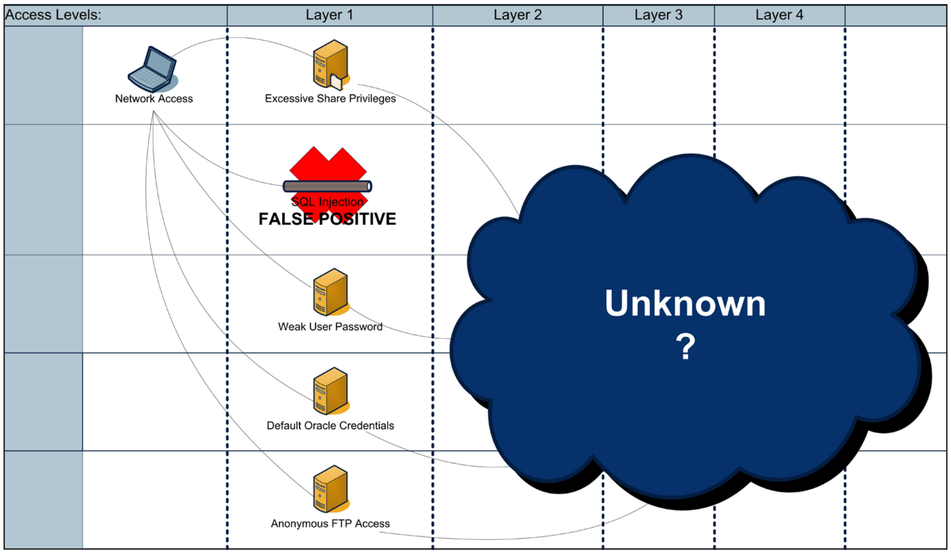
A vulnerability assessment typically involves using an automated tool to scan an information technology infrastructure and report the results. The tool's job is to identify all systems and the associated applications and services they are running. Based on this information, the tool attempts to identify issues such as missing patches, default passwords, and known exploits. All problems identified by the tool are then presented in a vulnerability assessment report. It should be noted that a typical vulnerability assessment does not include confirmation or validation of identified issues, which would verify that the tool's findings are accurate. In short, false positives usually are not removed, but instead are left as a potential issue for IT administrators to confirm if it is an issue or determine if it is a false positive.

In addition, a vulnerability assessment does not explore the purported issue's impact outside of rudimentary factors often based on tool output. For example, a vulnerability scanning tool will identify a weak password in a database and rank this as a high risk vulnerability. However, the vulnerability scanning tool fails to take into account that the database might not contain sensitive information and that the default password allows no one to gain additional access to the underlying operating system or escalate privileges to that of a server administrator.

Overall, vulnerability assessments and the tools used to perform them identify the first step an attacker might take to gain access to systems and data but are not able to quantify the potential impact of findings in a comprehensive manner and what the real priority of remediating any issues should be for the organization.

Vulnerability scanners provide identification and insight to only the first layer of the layered security model and do not take into account mitigating controls or the resulting impact on data.[1] Exhibit 1 shows the extent a vulnerability scanner can reach in truly assessing the risk an organization faces.

Exhibit 1: Vulnerability Assessment



Vulnerability Assessment Pros

- Thousands of security checks can be performed in automated fashion.
- The entire network can be assessed relatively quickly.
- Vulnerability assessments typically can be integrated into the organization's threat and vulnerability management program.
- Vulnerability assessments are useful for layer-one remediation testing.
- Vulnerability assessments identify easy targets.

Vulnerability Assessment Cons

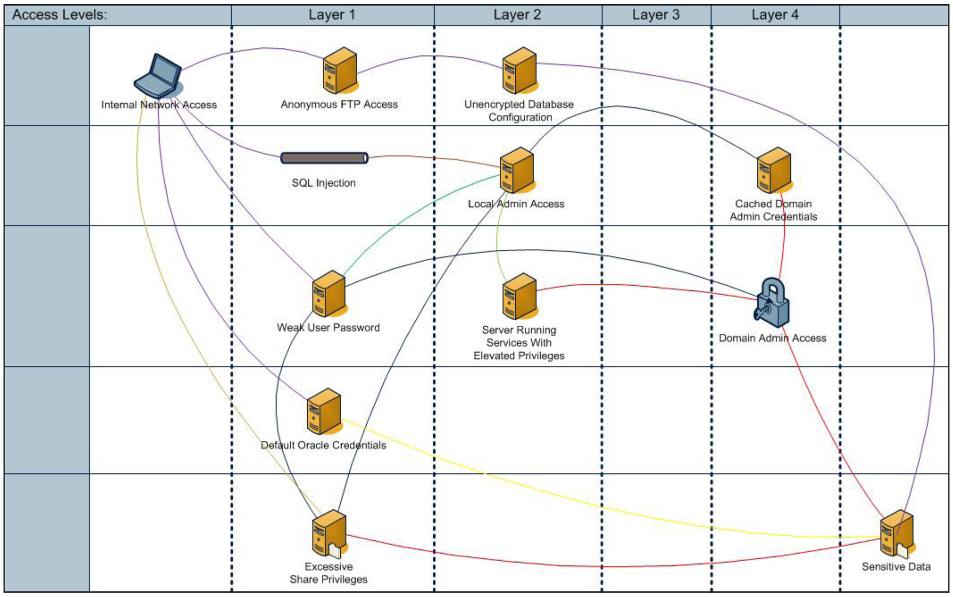
- Vulnerability assessments can provide an overwhelming, incoherent amount of data.
- They typically contain numerous false positives, especially for areas such as patch management and secure application development.
- Due to lack of impact analysis, they have inadequate risk rankings often based on tool suggestions.
- They are unable to chain together vulnerabilities to determine overall impact to the business.
- They fail to identify logical attack vectors such as password reuse and application logic flaws.
- Recommendations for remediation are often generic and based on tool output.

Penetration Tests

Penetration tests, often referred to as “pentests,” mimic a real-world attacker attempting to access systems and data by identifying vulnerabilities and combining (chaining) them to get unauthorized access to information or gain administrative control of the environment. Penetration testing typically uses vulnerability scanning software to efficiently get a fundamental picture of the corporation’s security in the allotted test time and to identify initial attack vectors into the organization.

Unlike vulnerability assessments, penetration tests can take into account mitigating controls and the issue’s impact by evaluating the confidentiality, integrity, and availability of the supporting environment. Penetration testing involves the human factor, which is required to chain together identified vulnerabilities to understand the organizational impact of the issues and to dive deeper into the environment, well past layer one. Exhibit 2 is a visual example of the layered testing that penetration tests can provide.

Exhibit 2: Penetration Test



Pentest Pros

- Mitigating controls are taken into account when risk-ranking vulnerabilities during penetrating testing.
- A proper business impact analysis can be performed for each issue identified.
- The human factor is used, and therefore process and logic security flaws can be identified.
- Vulnerabilities are chained together to discover the full impact of all discovered issues.
- False positives are removed from all layers of the security model.
- Logical, realistic recommendations that fit the organization are provided.

Pentest Cons

- Penetration testing’s value is highly dependent on the skills of the delivery team.
- Depth of coverage includes time and effort in addition to a vulnerability assessment.

Results of Pentesting: Example of a Layered Security Analysis

Layer 1:
Leveraging an internal network connection, a default database administrator account (DBA) password was identified. A vulnerability assessment would also identify this but then would go no further.

Layer 2:
Using the DBA, the local administrative password for the underlying operating system was obtained by exploiting a weak database configuration.

Layer 3:
A network scan with the local administrative credentials identified several servers using the same password for the account – revealing a lack of appropriate password zones.

Layer 4:
A user with domain administrative rights was logged in to one of the servers. Hijacking this account gave access to all network folders.

Conclusion

Vulnerability assessments and penetration tests are similar services in that they are both necessary tools in a organization's threat and vulnerability management program. However, they differ greatly with regard to providing value in their analysis, as depicted in Exhibit 3. This differentiation lies in the following:

1. Depth of analysis in the layered security model, with penetration tests targeting beyond layer one security controls
2. Performance of an impact assessment that attempts to place a practical risk ranking on noted issues
3. Removal of false positives to enable efficient remediation efforts

Exhibit 3: Typical Scope for Assessments

	Vulnerability Assessment	Penetration Test
Target identification	X	X
Layer one vulnerability identification	X	X
Removal of false positives		X
Vulnerability exploitation and compromise		X
Password strength analysis		X
File-share authorization analysis		X
User-rights examination		X
Egress traffic analysis		X
Password reuse analysis		X
Voice and data traffic segmentation		X
Service or application account privilege analysis		X

Typically, organizations structure their vulnerability management program to incorporate both vulnerability assessments and penetration tests as critical components to manage risk. For example, annual penetration testing is performed often in conjunction with either quarterly or monthly vulnerability assessments to track remediation efforts and identify vulnerabilities introduced by changes in the environment.

Chief information officers (CIOs), audit personnel, and information security officers need to be aware of these services and their corresponding value. The better CIOs and risk managers understand both types of assessments, the better an organization's comprehensive security strategy will fit the business's overall goals.

Contact Information

Raj Chaudhary is a principal with Crowe Horwath LLP in the Chicago office. He can be reached at 312.899.7008 or raj.chaudhary@crowehorwath.com.

Chris Wilkinson is with Crowe in the Dallas office. He can be reached at 219.308.8980 or christopher.wilkinson@crowehorwath.com.

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.