Resources

PENETRATION TESTING

Exploring Weaknesses to Strengthen Defenses

WHAT'S THE DIFFERENCE BETWEEN A VULNERABILITY ASSESSMENT AND PENETRATION TESTING?

It's surprising how often individuals are confused with the terms vulnerability assessment, penetration testing and cybersecurity. Some individuals use these terms interchangeably, but they have specific meanings. Cybersecurity is an overarching term defining "art of protecting networks, devices and data from unauthorized access" (CISA, n.d.). Practitioners in the cybersecurity field perform vulnerability assessments and penetration testing as part of their practice; the differences are explained next.

PENETRATION TESTING

According to the SANS Institute, a vulnerability assessment is defined as follows in the context of vulnerabilities and exploits:
"Vulnerabilities are the gateways by which threats are manifested; a system compromisecan occur through a weakness; a vulnerability assessment is a search for these weaknesses/exposures in order to apply a patch or fix to prevent a compromise" (Cima, 2001).

A vulnerability assessment involves the process of scanning digital assets for any potential vulnerabilities, flaws or weaknesses that could leave it open to exploitation. At a minimum, all organisations should scan their digital assets for vulnerabilities; this includes websites, servers, laptops, firewalls, switches, access points and all other IP accessable devices.

VULNERABILITY ASSESSMENT

There is often confusion between penetration testing and vulnerability assessments, because the terms are related but different.
The SANS Institute provides the following clarification: "Penetration testing has more of an emphasis on gaining as much access as possible while vulnerability assessments place the emphasis on identifying areas that are vulnerable to a computer attack. An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem. A vulnerability assessor will stop just before compromising a system, whereas a penetration tester will go as far as they can within the scope of the contract." (Northcutt, et al., 2006) The penetration testing process involves enumeration and scanning for any technical flaws or vulnerabilities. After such flaws are found, attempts are then made to penetrate inside the network and gain a foothold. Once this has been established, attempts are then made to utilise trusts and relationships to gain further ingress into the domain.

QUESTIONS ABOUT PENETRATION TESTING

An Introduction to Penetration Testing

Individuals are often confused regarding the difference between vulnerability scanning and penetration testing. Both activities are part of cybersecurity best practices, and vulnerability scanning always comes before penetration testing.

Vulnerability scanning searches for weaknesses in an asset or system that could, potentially, be exploited by a bad actor. As an analogy, vulnerability scanning is akin to seeing if a window or door is unlocked on a house, but not entering the house. It is a passive activity.

Penetration testing exploits the potential weakness (identified during vulnerability scanning) to determine the degree to which a malicious attacker could gain access to an asset or system. Using the analogy of a house, a penetration tester attempts to open the unlocked window or door and take a step into the house.

When to Perform Vulnerability Scanning Vs. Penetration Testing?

Performing both vulnerability scanning and penetration testing is the most robust and assured way to insure an environment is properly configured to safeguard against malicious attackers. Performing vulnerability scanning routinely (monthly, weekly, daily) is a best practice, and performing penetration testing annually, at a minimum, is prudent.

Can Penetration Testing Help with Regulatory Compliance?

In a single word, yes. For many organisations, contractual requirements and statutory obligations compel organisations to perform penetration tests periodically by an independent entity such as Allendevaux & Company. Regulations such as the General Data Protection Regulation or California's Consumer Privacy Act require enterprises to demonstrate due care and due diligence in terms of validating data protection best practices, and penetration testing is the ultimate form of assurance. Many sector-specific domains also require penetration testing by statutory obligation, including PCI DSS, healthcare, finance and banking.

My Data is Contained in AWS or Azure. Why is Penetration Needed?

While Amazon Web Services or Microsoft Azure hosts a company's data, it is usually the software running within AWS or Azure that is vulnerable to attack. It is necessary to vulnerability scan and penetration test any new release of software in order to provide "sufficient guarantees" that the system does not contain an unknown security hole or weakness that could be exploited by a malicious attacker.

What Types of Assets or Systems Should be Penetration Tested?

Any asset or system that collects, stores, processes and transmits confidential and sensitive information such as company secrets or personal information should be tested. Cloud service providers should test cloud environments and systems supporting operations. Financial institutions should test banking and financial services systems, including the portals that customers and partners access. Hospitals should test all internal and external systems associated with critical hospital operations and functionality, including any systems that store and process patient data. The practitioners at Allendevaux & Company can help your organisation identify and prioritise your approach.

QUESTIONS ABOUT PENETRATION TESTING

What approach does the Allendevaux & Company take for penetration planning and testing?

The cybersecurity practitioners at Allendevaux & Company approach cybersecurity assurance by using the NIST Cybersecurity Framework or ISO/IEC 27032 best practices. Both are highly recognized standards, and often NIST is used for United States centric activity whilst ISO/IEC 27032 is employed for international engagements.

What certifications does the team at Allendevaux & Company hold and maintain?

The cybersecurity team is comprised of a diverse team of highly experienced professionals, holding industry recognized certifications in security and compliance, white hacking, data analytics and auditing. Education and certifications including OSCP, CIPP/US, CIPT, HCISPP, CIS LI, CIS LA, CIPM and others.

More Questions

Will penetration testing break services and systems?

While vulnerability scanning is passive, penetration testing is active, exploiting discovered weaknesses but stopping short of causing damage. Still, unexpected outcomes have happened during penetration testing, though it is rare, such as a service locking-up or a system's performance slowing. Due to this, it is recommended that penetration testing be scheduled during less active times.

Is penetration testing needed if vulnerability scanning has been performed?

Vulnerability scanning is the starting point, identifying the weaknesses a system may possess that could be exploited by a bad actor. Penetration testing is active, challenging a system to determine if weaknesses exist that a malicious attacker would otherwise exploit. Vulnerability scanning always precedes penetration testing, and the latter provides the best proactive methodology to assure information is sufficient protected from threats.

Is Allendevaux & Company an Experienced Penetration Testing Firm?

The cybersecurity team has thousands of hours of penetration testing experience across all types of industries, including healthcare, communications, finance and banking, pharmaceutical, corporate, government, defense contractors, and manufacturing.

Is penetration testing needed if vulnerability scanning has been performed?

Vulnerability scanning is the starting point, identifying the weaknesses a system may possess that could be exploited by a bad actor. Penetration testing is active, challenging a system to determine if weaknesses exist that a malicious attacker would otherwise exploit. Vulnerability scanning always precedes penetration testing, and the latter provides the best proactive methodology to assure information is sufficient protected from threats

More Questions

Is Allendevaux & Company an Experienced Penetration Testing Firm?

The cybersecurity team has thousands of hours of penetration testing experience across all types of industries, including healthcare, communications, finance and banking, pharmaceutical, corporate, government, defense contractors, and manufacturing

Your price is higher than others, or your price is lower than others. Why the variation?

The most costly component of any PEN testing engagement is the certified and experienced expertise assigned to the scope, as well as and the senior management providing peer-review and oversight. While some vendors use automated systems and promote it as a PEN test, and others outsource the scope to an offshore resource, the PEN testers at Allendevaux & Company follow best practices underwritten in the industry today. Background checks are performed on every individual before they're permitted to work in production engagements.

It is also important to note that certifications alone do not result in the most successful penetration testers, but it helps. Yet true expertise also comes from industry experience and skills developed from thousands of hours of professional engagement and working in teams. Those are the types of individuals the firm employs on every penetration test. Quality is our first goal, and we are usually competitive. But if there's a lower price by a competitor, remember this is not the domain to go cheap with the cheapest bidder. Data breaches bring reputational damage, amass legal costs, attrition customers and incur agency sanctions.

Outputs

WHAT IS THE OUTPUT OF A PENETRATION TEST REPORT?

Executive Summary:

This serves as a high-level view of risks discovered and the potential business impact. This is a succinctly written section of the report portrayed in non-technical parlance. The section often contains graphs, charts and tables helpful to convey the findings to an executive reader that needs to understand the salient points to make informed decisions for the organisation.

Technical Risks:

This section identifies the risks and criticality of each finding. But to simply state a risk is “dangerous” does not convey the totality of any risk; that’s why the business impact is often tied to the risk when relevant.

Potential Impact of Vulnerability:

Most reports contain higher-level descriptions regarding how to address the problems discovered. When possible, guidance will be provided regarding how to properly configure and harden a firewall, how to filter SQL injections, and how to bring swift resolutions of many findings. But there is an assumption thatthe IT staff will have a good understanding of how to take the specific findings and make intelligent decisions to address the bulk of the issues.

Methodology:

It is important to understand the methodology employed by the PEN testers, and this section details those details.

Potential Impact of Vulnerability:

The likelihood and potential impact of the risks are important criteria to be noted in a PEN test report. In this section, reviewers of the report are able to dig into the details of what is affecting the organisation. Factoring the likelihood and potential impact of an exploitation rounds-out the report with detail for better decision-making.

Presentation:

A live presentation concludes the engagement, enabling an organisation to ask questions to the PEN testers and receive helpful commentary regarding findings and clarifications to the report.

WHAT PENETRATION TESTING TOOLS DO YOU USE?

All penetration testing starts with a comprehensive scan to validate the network perimeter and inventory assets such as ip addresses, ports and services). This process is normally accomplished using tools such as Nmap, Angry IP Scanner, Dipiscan, Masscan, NetCrunch and ZMap.

Once data has been compiled from perimeter mapping, the next step in the process involves conducting a vulnerability scan to find exploitable weakness that will be targeted during penetration testing. Vulnerability scanning is conducted using tools such as Nessus, Qualys, AlienVault and Zenmap from both external and internal vectors (as relevant).

The penetration testing team reviews the results of the vulnerability scan, prioriting the effort and planning the attack. An array of tools are used depending upon the weaknesses found, including but not limited to any of the following:

Qualys
Vulnerability Scanning

Kali Linux
Hacking Tools

Metasploit
Network Exploitation

Feroxbuster/Gobuster/Ffuf
Brute Forcing

SQLmap
SQL Injection (Database Hacks)

Nmap
Network Mapping

Cewl
Targeted Password Cracking

John/Hydra/Ncrack
Password Cracking

Burp Suite Pro
Traffic/Vulnerability Scanner

WPScan
WordPress Security

Wireshark
Network Traffic Analysis

SIPVicious
VoIP Security

Nikto/W3af/Skipfish/ZAP
Web Application Analysis

If onsite wireless penetration testing is performed, then Aircrack-ng is also utilised.

CONTACT US

✉ Email: **Info@allendevaux.com**

Web: **www.allendevaux.com**

☎ US: +1 (213) 279-1055

☎ UK: +44 2038 802 321

☎ CH: +41 44 585 92 15

WORKS CITED

- Cima, S. (2001, July 6). Vulnerability Assessment. SANS Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/basics/vulnerability-assessment-421

- CISA. (n.d.). What is Cybersecurity? Department of Homeland Security. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-001

- Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Silas, R., & Mancini, S. (2006, June). Penetration Testing: Assessing Your Overall Security Before Attackers Do. SANS Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-securityattackers-34635

- Janardhanudu, G., & van Wyk, K. (2013, July 5). White Box Testing. US-CERT. Retrieved from https://www.us-cert.gov/bsi/articles/best-practices/white-box-testing/whitebox-testing

- Wolfram, B. (2013, August 26). Difference Between Blackbox Testing and Double Blind Test. Professional Groups. Retrieved from http://www.isaca.org/Groups/Professional-English/cisa-exam-study-community-2013/Pages/ViewDiscussion.aspx