Penetration Testing Vs. Vulnerability Scanning

What is the difference?

For businesses seeking to understand their cyber risk, it is extremely important to understand the difference between penetration testing and vulnerability scanning. Both endeavors can provide a business with valuable information, but they are quite different in terms of scope, cost, and outcome. This article will seek to explain the differences and when and how a small business might choose to conduct one versus the other.

Small businesses often pay consultants to conduct assessments in the form of vulnerability scanning and/or penetration testing to determine if they are vulnerable to a cyber-attack and if so, by what method. The reason for conducting either is to help a business figure out what they can do to better protect the business from cyber-attacks. Both types of assessments can help to identify weaknesses but neither, on its own, will provide a complete picture of a business' weaknesses.

Network Vulnerability Scanning

Network vulnerability scanning is the process of identifying known vulnerabilities that exist in defined systems connected to a network via an IP (Internet Protocol) address. Vulnerability scans are conducted using a device and/or software to look at a network and compare the state of the network, and more specifically all the hosts/systems on the network, to a library of known vulnerabilities. The outcome of the vulnerability scan should be a list of known vulnerabilities, some indication as to the severity or nature of the vulnerability, and actions required to remediate or close the vulnerability.

Network Vulnerability Scans

Two types of network vulnerability scans are typically conducted by small businesses. Internal vulnerability scans (IVS) and external vulnerability scans (EVS). The distinction between and IVS and EVS is simply the location from which the can is run. An IVS is run inside a network (behind the firewall) against all the devices on the inside of the network (i.e., servers, workstations, printers, switches, storage devices, security cameras, phone systems, phone

handsets, door access controls, wireless access points…). An EVS is run from outside the network, typically from the public Internet to determine weaknesses known vulnerabilities that are exposed to the public Internet.

The vulnerability scanner, typically a laptop running scan software, will scan each IP address on the defined network or subnet and seek to identify all hosts or systems on the network. Next, the scanner seeks to identify known vulnerabilities for each open port on the IP addresses. Each IP address may have as many as 65,000+ ports. one vulnerability scan might be set to only review a specific number or range of ports to include those most often used for typically network services (i.e., port 443, port 25, port 80, port 3389…). The scanned ports should be defined in the scope of work and the vulnerability scan reports.

It is important to understand that a vulnerability scan will only identify known vulnerabilities that have made their way into the scanning vendor's database. For this reason, it is important to leverage a vulnerability scanner from a reputable scan vendor and it is equally important that the person conducting the scan updates the vulnerability definitions list immediately prior to conducting the scan to make sure that the most up to date definitions are used when conducting the scan.

A vulnerability scan deliverable should include a list of the network(s) that were scanned, IP addresses in use at the time of the scan, and a list of vulnerabilities identified on each IP address and ports. Most good vulnerability scan reports will also provide some indication as to the severity/criticality of a particular vulnerability along with remediation suggestions.

It is common for a vulnerability scanner to identify tens of thousands of vulnerabilities. Many vulnerabilities can be remediated by simply updating software or firmware on a given host (i.e., server, printer, IP phone, laptop…) and running updates for hosts(s) might simultaneously remediate hundreds or thousands of the vulnerabilities on the list. Remediating other vulnerabilities might require configuration changes to hardware or software.

It is highly likely that fully remediating some vulnerabilities will negatively impact the functionality of a system or host. For example, open FTP (File Transfer Protocol) ports are frequently identified on a vulnerability scan because the FTP protocol sends the FTP username and password across the network in clear text and this vulnerability is easily exploited. Shutting down port 21 (File Transfer Protocol) or disabling the FTP protocol on a scanner may break the scan to file function on a network scanner. In these instances, a decision must be made regarding the relative risk and other risk mitigation strategies that

might be employed to reduce risk without formally remediating the specific vulnerability identified by the scan. Other, more secure, scanning protocols might be available for use on a good network scanner or additional controls might be established to help mitigate the risk of continuing to use FTP inside a network.

Perhaps the single most important consideration for conducting a vulnerability scan is making sure your business has the expertise or can engage with an outside vendor to provide the expertise necessary to take the results of the scan to produce a remediation plan. The plan will often prioritize the most critical risks and work down through the vulnerability list in an organized manner and will include documenting what vulnerabilities cannot be remediate, why they cannot be remediated, and what mitigating controls are to be used to reduce the remaining risk.

Patching or remediating vulnerabilities is critical to prevent the likelihood and severity of a network breach. Each remediated vulnerability may end up being the one that prevents a threat actor from gaining access to systems and inflicting harm on a business and its customers. This is the value of conducting and using a vulnerability scan.

Vulnerability scan pricing will range from $500 - $10,000 depending on the number and size of networks being scanned. Vulnerability scans require the use of software that typically costs between $2,500 - $5,000 per year.

Penetration Testing

Penetration testing is the process of attempting to identify and exploit vulnerabilities in processes, systems, software, and people. A penetration test should be conducted by an independent party with no control of the systems to be tested, no influence over the design of the systems to be tested, and no stake in the outcome of the penetration test. The effectiveness of a penetration test is highly dependent on the skill and expertise of the tester.

The penetration testing firm will seek to gain access to a defined system or set of data. The purpose of a penetration test is to identify vulnerabilities and how exploitation of vulnerabilities, often in combination, might result in a breach of systems or data. The rules of engagement for a penetration test will typically contain limits as to the types of methods used, scope of systems to be included, extent to which vulnerabilities may be exploited, and how the penetration tester will conduct the test. The rules of engagement will also cover with whom and when the penetration tester should communicate regarding issues, success, and failure. A penetration test may also include a scope of work that will define the cost of the

test, duration of the test, deliverables, proof of execution, and definition of the amount of effort and resources to be expended to conduct the test.

Penetration tests are typically limited in scope for the purpose of cost containment and for the purpose of focusing the effort of the test on the most valuable assets (systems and data). However, penetration tests can be designed to cover any breadth or depth desired. Businesses should carefully consider what they hope to accomplish with a penetration test and work with the third-party penetration tester to design a test to meet the objectives.

Common penetration testing objectives include:

- Gaining access to sensitive data shares
- Gaining remote access to systems (workstations, servers, Network Attached Storage, printers…)
- Gathering or hacking Domain Admin credentials
- Gathering or hacking user credentials
- Gaining access to sensitive areas (i.e., server rooms, network closets, file rooms, office, unattended workstations…)
- Gaining access to a user's email
- Gaining access to accounting or ERP platforms
- Gaining access to Software as a Service applications
- Gaining access to cloud storage

Following are the most common penetration testing methods used to achieve the objectives:

- Social Engineering to gain sensitive information and/or access to systems.
    - Vishing (voice/phone calls to employees)
    - Phishing (targeted emails to employees)
    - In person visits to physical locations, often posing as vendors, delivery companies, utilities, customers, prospective customers, employees…
    - Chat/Instant messaging
    - Social media
- Attempting to gain physical access to sensitive areas by bypassing physical security controls (door locks, security cameras, fencing, alarms…)
- Taking advantage of network gateway (firewall) vulnerabilities exposed to the public Internet

- Taking advantage of network vulnerabilities behind the firewall. This method typically requires connecting a device to the network that is owned and managed by the penetration tester.
- Deployment of malware, often through social engineering.
- Wireless network hacking.

- Taking advantage of firewall/gateway vulnerabilities.
- Running a vulnerability scan to identify known vulnerabilities for the purpose of exploiting the same.

Success in achieving penetration test objectives often requires exploiting multiple vulnerabilities, and very frequently involves social engineering and human error. In this respect, penetration testing best mimics the nature of a real-world attack by a threat actor. Penetration testing does not expose all vulnerabilities but a path or multiple paths to obtain a specific objective. The completion of a penetration test does not eliminate the possibility that additional, and potentially more serious vulnerabilities may still exist. This is because penetration testers, like threat actors, often take the path of least resistance to obtain the objective.

The deliverable for a penetration test should include a description of methods, identification of success and failure achieving objectives, and proof of having obtained the objectives. Proof may come in many forms including photos, copies of documents, screen shots, credentials, and log files. The deliverable often also includes recommendations for remediating vulnerabilities.

Like with a vulnerability scan, if a business chooses to invest in a penetration test, it is important to have or engage with experts who can take action to remediate the issues identified by the penetration test.

Comparison of Vulnerability Scans and Penetration Tests

	Vulnerability Scan	Penetration Test
Only reveals vulnerabilities as of a specific point in time.	Yes	Yes
Determines all attack vectors and vulnerabilities	No	No
Reveals all known vulnerabilities for a particular host (IP address)	Yes	No
Can be conducted by an internal IT resource or vendor with responsibility for managing IT systems.	Yes	No
Provides recommendations for remediating discovered vulnerabilities	Yes	Sometimes
Ranks discovered vulnerabilities by severity	Yes	Sometimes
Proves that a particular vulnerability can be exploited to the detriment of the company	No	Sometimes
Determines if multiple vulnerabilities can be exploited to the detriment of the company	No	Sometimes
May help to identify weaknesses with SaaS applications	No	Yes
May help to identify vulnerabilities related to process	No	Yes
May help to identify social engineering vulnerabilities	No	Yes

Penetration testing pricing varies widely depending on the scope of the test. Most small – medium sized businesses start with narrowly scoped penetration tests to cover some or all the methods and objectives listed above. Penetration tests of this type will typically run from $12,000 - $20,000.

Summary

Vulnerability scans and penetration tests are important tools for businesses who are seeking to identify blind spots on their cybersecurity posture. These tools are best and most often used by businesses that have already endeavored to implement procedures, controls, and policies to address the most common types of risks. Neither a clean vulnerability scan or an unsuccessful penetration test is an indicator that a business is secure. Rather, they are an additional piece of information from a specific point in time to help gauge overall effectiveness of existing cybersecurity procedures, controls, and policies.