What is a security assessment?

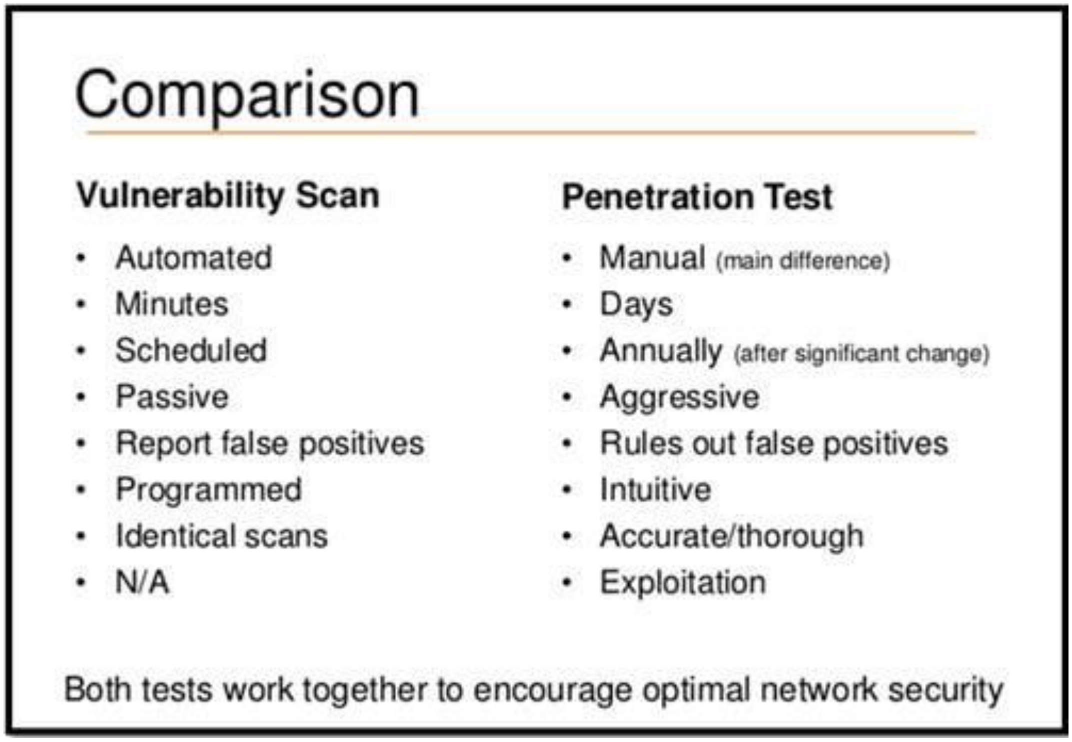
Security assessments are periodic exercises that test your organization's **security** preparedness. They include checks for vulnerabilities in your IT systems and business processes, as well as recommending steps to lower the risk of future attack

Vulnerability Assessment ?

A vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system

Penetration testing,

also called **pen testing** or ethical hacking, is the practice of **testing** a computer system, network or web application to find security vulnerabilities that an attacker could exploit. **Penetration testing** can be automated with software applications or performed manually.



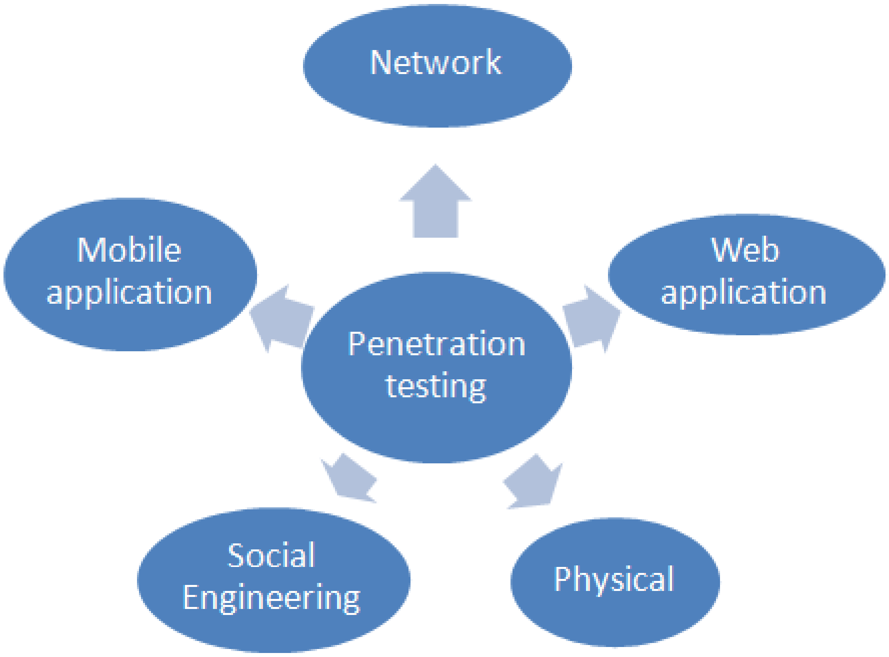
Comparison

Vulnerability Scan	Penetration Test
Automated	Manual (main difference)
Minutes	Days
Scheduled	Annually (after significant change)
Passive	Aggressive
Report false positives	Rules out false positives
Programmed	Intuitive
Identical scans	Accurate/thorough
N/A	Exploitation

Both tests work together to encourage optimal network security

Vulnerability Assessment	Penetration Testing
This is the process of finding and measuring the vulnerability of a system	Penetration testing finds the vulnerabilities and exploits it to take advantage of the system
The end result is a list of vulnerabilities which is often prioritized by its potency	A penetration test is more goal oriented. It helps in charting the path which will be taken by the attacker to take over the system.
Vulnerability assessment is recommended when the system already has known security issues or the organization has no security measures and wants to get started in that area.	Penetration test, on the other hand, is recommended when the company has a good level of security and they want to search for some hidden vulnerabilities.
Emphasizes “breadth over depth”. Meaning it is more concerned about finding more vulnerabilities instead of understanding the true severity of each.	Emphasizes “depth over breadth”. They discover vulnerabilities with specific goals in mind. They want to know how a potential hacker can exploit the situation to take over the system.

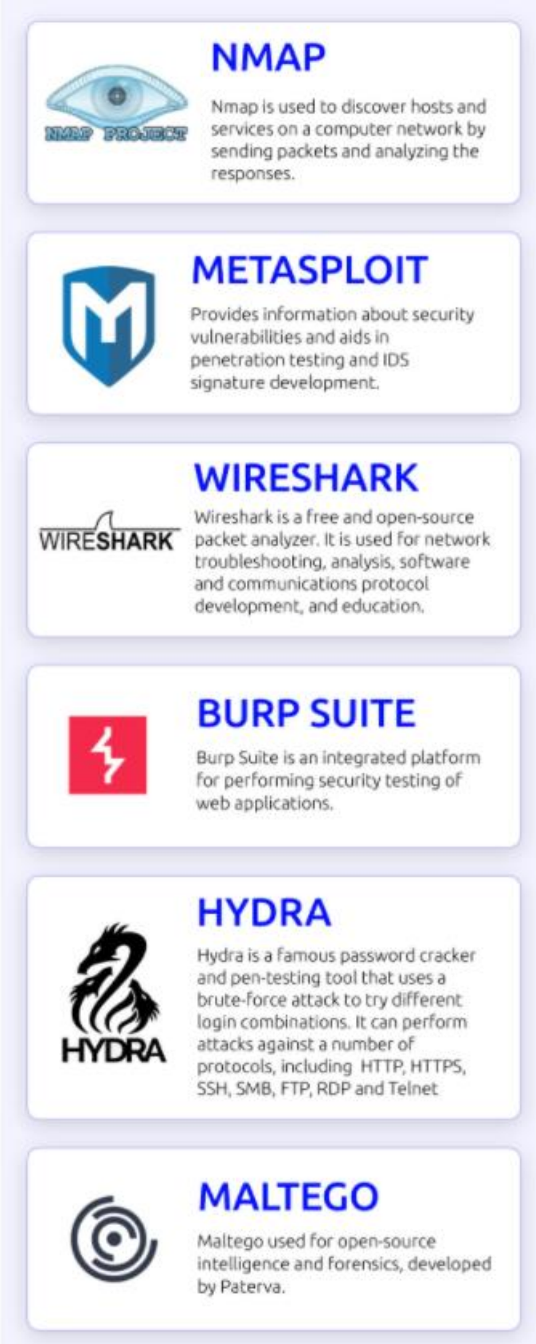
Types of Pen Testing



Manual vs Automated Pentesting

Manual Testing	Automated Testing
You should not expect accuracy when you opt for manual testing. Human errors will be there, so you cannot entirely rely on it.	Automated testing gives you accurate results since engineers perform it with the intended tools and/or scripts.
It consumes more time.	It is faster as compared to manual testing.
You need to invest on human resources.	You need to invest on testing tools.
Frequent repetition is not required in manual testing.	Engineers repeat automated testing process for longer time.
Human observation is a must.	Since it involves use of tools, human observation is not mandatory.

Pentesting tools



NMAP

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

METASPLOIT

Provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

WIRESHARK

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

BURP SUITE

Burp Suite is an integrated platform for performing security testing of web applications.

HYDRA

Hydra is a famous password cracker and pen-testing tool that uses a brute-force attack to try different login combinations. It can perform attacks against a number of protocols, including HTTP, HTTPS, SSH, SMB, FTP, RDP and Telnet

MALTEGO

Maltego used for open-source intelligence and forensics, developed by Paterva.