PRELIMINARY

PENETRATION SCAN REPORT

Generated on

30 May 2024

Prepared for

COMPANY
SLOGAN HERE

TABLE OF CONTENT

COMPANY
SLOGAN HERE

pngtree.com

ABOUT

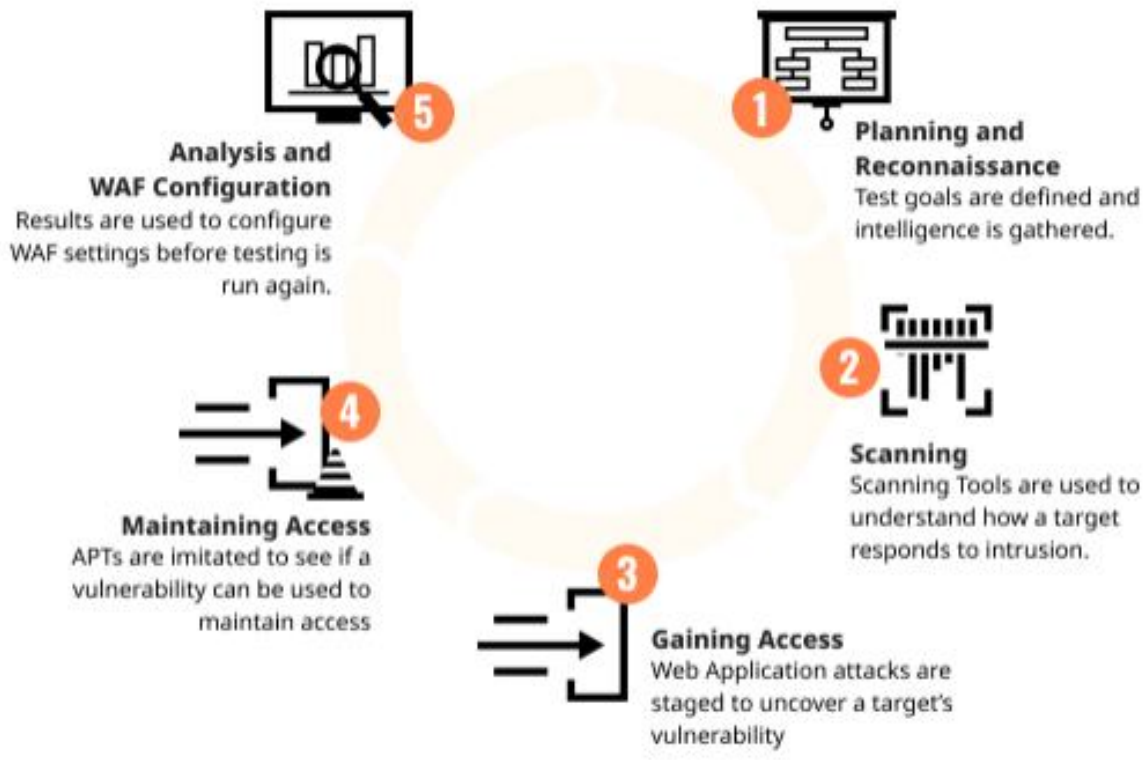
WHAT IS PENETRATION TESTING?

A penetration test, also known as a pen test, is a simulated cyberattack against your computer system to check for exploitable Susceptibilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., Application protocol interfaces (APIs), frontend/backend servers) to uncover Susceptibilities, such as unsanitized inputs that are susceptible to code injection attacks

Insights Provided By The Penetration Test Can Be Used To Fine-Tune Your WAF Security Policies And Patch Detected Susceptibilities

PENETRATION TESTING STAGES



Penetration Testing Stages

WHY IS PEN TESTING IMPORTANT?

COMPANY
SLOGAN HERE

Penetration Tests Let Companies Evaluate The Overall Security Of Their IT Infrastructure. A Company May Have Robust Security Protocols In One Area, But Be Lacking In Another. The High Cost Of A Successful Cyberattack Means No Company Should Wait For A Real-World Scenario To Play Out Before Going On Offense. Using Penetration Testing Tools To Expose Holes In A Business's Security Layer Allows Security Experts And Pen Testers To Address Any Shortcomings Before They Become Critical Liabilities.

Test Security Controls - Gain insights into the overall health of your application, network, and physical security layers.

Find Real-World Susceptibilities - Expose endpoints in your computer systems most susceptible to attacks from adversaries.

Ensure Compliance - Companies can maintain information security in compliance with industry standards for penetration testing.

Reinforce Security Posture - Penetration testing assists businesses in prioritizing and addressing their Susceptibility with a security program.

WHEN SHOULD YOU PEN TEST?

Some Companies Make The Mistake Of Starting A Pen Test Too Early On A Network Or System Deployment.

When A System Or Network Is Being Deployed, Changes Are Constantly Occurring, And If A Pen Test Is Undertaken Too Early In That Process, It Might Not Be Able To Catch Possible Future Security Holes.

In General, A Pen Test Should Be Done Right Before A System Is Put Into Production, Once The System Is No Longer In A State Of Constant Change.

It Is Ideal To Test Any System Or Software Before It Is Put Into Production.

Most Companies Do Not Adhere To This Recommendation Because They Are Eager To Get Their Return On Investment (ROI) Quickly.

Companies Might Also Fail To Follow This Best Practice Because A Project Has Exceeded Its Deadline Or Budget.

These Factors Make Companies Enthusiastic To Push Their New Services Live Without Having Conducted The Proper Security Assessments.

This Is A Risk That Needs To Be Evaluated And Put In Perspective When Deploying New Systems.

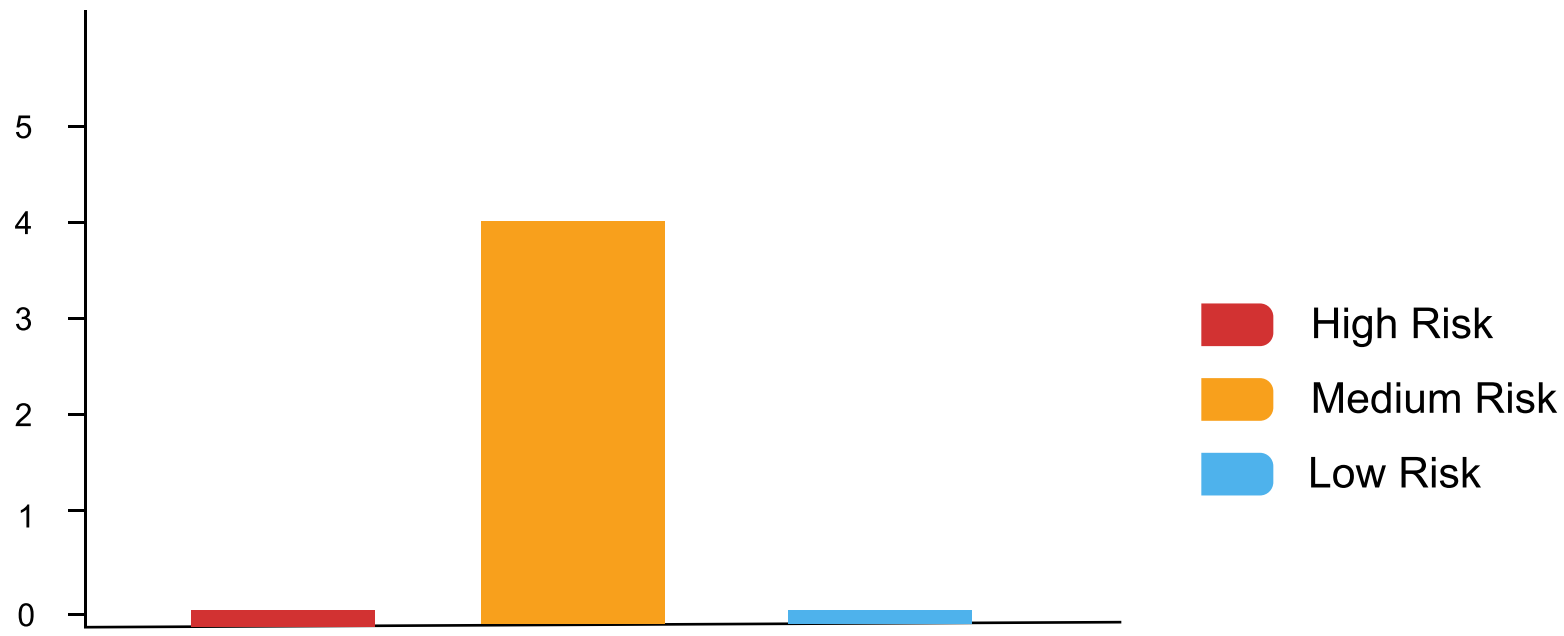
Regular Comprehensive Network Scans Are Essential For Keeping Your Network Secure And Resilient. By Routinely Scanning For Vulnerabilities, You Can Identify And Address Potential Security Risks Before They Are Exploited By Attackers, Ensuring The Continuous Protection Of Your Systems And Data.

TARGET
DETAILS

WE PERFORMED PENETRATION SCANS ON THE FOLLOWING TARGETS:

Https://Sample2.Com
Http://Sample.Com
192.168.100.1
192.169.1.45
Https://Example1.Com
Https://Example2.Com
10.1.1.1

SUMMARY
FINDINGS



The Pen Test That Was Conducted Discovered A Total Of 411 Severity. The Vertical Section Is For The Risk And The Horizontal Section Is The Confidence With Which It Reports The Risk Probability. The Following Table Summarizes The Risk And Confidence Of The Findings Identified During This Penetration Testing:

	Risk	High	Medium	Low	Informational	Total
Confidence	High	0	106	26	0	132
	Medium	0	51	19	123	193
	Low	2	24	0	60	86
	Total	2	181	45	183	411

TOP 10
RISK DISCOVERED

COMPANY
SLOGAN HERE

The Following Table Contains The Top 10 Web Application Security Risk

Sr. No.	Application Security Risk	Vulnerability Status
1	Broken Access Control	Vulnerabilities Identified
2	Cryptographic Failures	No Vulnerabilities Identified
3	Injection	No Vulnerabilities Identified
4	Insecure Design	No Vulnerabilities Identified
5	Security Misconfiguration	Vulnerabilities Identified
6	Vulnerable And Outdated Components	No Vulnerabilities Identified
7	Identification And Authentication Failures	No Vulnerabilities Identified
8	Software And Data Integrity Failures	Vulnerabilities Identified
9	Security Logging And Monitoring Failures	No Vulnerabilities Identified
10	Server-Side Request Forgery (SSRF)	No Vulnerabilities Identified

COMPANY
SLOGAN HERE

pngtree.com

SEVERITY
CHARACTERISTICS

When categorized into high, medium, and low levels, Severity characteristics are often used to prioritize issues or incidents based on their impact, urgency, and criticality. Here's a breakdown of the characteristics typically associated with high, medium, and low severity levels:

High Severity

Impact

Critical impact on system functionality or data integrity.
Affects a large number of users or critical business processes.

Urgency

Requires immediate attention and resolution.
Rapid response and intervention are essential

Characteristics

Critical errors or failures that significantly impair system functionality.
Security breaches or Susceptibilities that pose a severe threat.
Outages or disruptions affecting core services.

Medium Severity

Impact

Moderate impact on system functionality or data integrity.
Affects a subset of users or non-critical business processes.

Urgency

Requires attention and resolution within a reasonable timeframe.
A timely response is necessary, but immediate action may not be critical.

Characteristics

Errors or issues that impact specific functionalities but not the entire system.
Performance degradation that affects user experience.
Security Susceptibilities with a moderate level of risk.

Low Severity

Impact

Low impact on system functionality or data integrity.
Affects a small number of users or has minimal business impact.

Urgency

Requires attention, but resolution may not be time-sensitive.
Can be addressed during regular maintenance or planned updates.

Characteristics

Minor errors or warnings that do not significantly impact overall system performance.
Cosmetic issues or non-critical functionalities experiencing glitches.
Low-risk security findings or Susceptibilities

NOTES

State classifications for ports include open, closed, filtered, unfiltered, open | filtered, and closed | filtered.

Open	An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. An open port is an avenue for attack. Attackers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non security scans because they show services available for use on the network.
Closed	A closed port is accessible (it receives probing packets and responds to them), but no service is actively using it. They can be useful for OS detection as well as for verifying that a host is up on that IP address. Since closed ports can still be accessed, it could be wo rthwhile to search later in case any do. Administrators might wish to think about using a firewall to block certain ports.
Filtered	Due to packet filtering, Susceptibility scanner is unable to detect whether the port is open because its probes cannot access the port. A dedicated firewall device, router rules, or host-based firewall software may be used for the filtering. Hackers are frustrated by these ports since they offer scant information. Filters that just drop probes without responding are much more prevalent than those that occasionally answer with ICMP error signals, such as type 3 code 13 (destination unreachable: communication administratively banned). As a result, Penetration testing is compelled to retry numerous times in case the probe was dropped due to network congestion and not filtering.

Unfiltered	An accessible port is in the unfiltered state when Susceptibility scanner cannot tell whether it is open or closed. This state is only assigned to ports by the ACK scan, which is used to map firewall rulesets. It may be possible to determine whether a port is open by scanning unfiltered ports with other scan types like Window scan.
Open/ Filtered	When Susceptibility scanner is unable to detect whether a port is open or filtered, it places ports in this state. This happens with scan kinds where open ports don't respond. A packet filter may have blocked the probe or the responses it generated, which would explain why there was no answer. Susceptibility scanner therefore cannot be certain if the port is open or being filtered. Ports are categorized in this fashion by the UDP, IP protocol.
Closed? Filtered	When Susceptibility scanner is unable to detect whether a port is closed or filtered, this status is utilised. Only the IP ID idle scan is utilised with it.