Pentera™

Pentera Surface Detailed Report

Account name

Report created on January 15, 2023

The Pentera Surface Detailed Report summarizes the attractions, vulnerabilities, and achievements discovered on your organization's external attack surface.

PENTERA

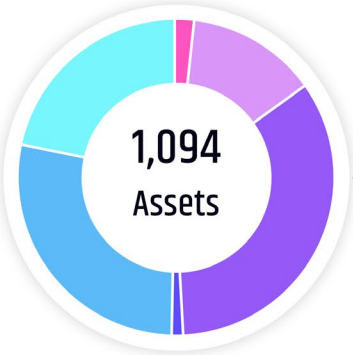
Table of Contents

Detailed Report

Executive Summary

Asset Inventory

Pentera found the following assets on your attack surface.



- 10 Domains
- 163 Subdomains
- 361 IP Addresses
- 5 Networks
- 324 Services
- 231 Websites

Findings

See the total number of attractions, vulnerabilities, and achievements found to date with a breakdown by severity.

231 Attractions	56 Extreme	175 Serious	85 Moderate	57 Minimal
324 Vulnerabilities	37 Critical	55 High	34 Medium	198 Low
121 Achievements	25 Critical	3 High	12 Medium	81 Low

Last Scan Activities

See how many activities since the last scan were successful, did not return results, or require your approval for Pentera to take action.

1,287 Total Actions

864 Successful (66.3%) **423** No results (33.6%)

100 Pending Provisioning

To enhance test coverage and accuracy, provision more activities in Pentera Surface.

Detailed Report

5 Attractions

1 Extreme | 2 Serious | 1 Moderate | 1 Minimal

See what's attractive to attackers, including open ports, exposed services, potential vulnerabilities, and more.

Extreme — Potential Log4Shell (CVE-2021-44228)

6 assets

Attackers may search for websites using technologies that are vulnerable to Log4Shell (CVE-2021-44228) to gain access to a server and execute code remotely.

199.203.240.17:6660/tcp	199.203.240.17:6662/tcp	199.203.240.17:9002/tcp
212.143.240.115:9002/tcp	212.143.240.115:6662/tcp	212.143.240.115:7001/tcp

Serious — Website using self-signed certificate

22 assets

Attackers may search for any valuable information that can help to better understand the asset, including the website certificate details. As a rule, websites with self-signed certificates are for internal use and should not be public-facing. When external-facing, a self-signed certificate attracts attention as it indicates a security flaw.

https://199.203.240.17:666	http://144.126.246.196:443	https://app.pentera-demo.io:8088
https://app.pentera-demo.io:666	https://107.180.0.147:443	https://199.203.240.17:8088
https://www.pentera-demo.io:666	https://18.197.248.23:443	https://lab.pentera.io:8088
https://support.pentera-demo.io:666	https://194.113.194.215:443	https://support.pentera-demo.io:808
https://lab.pentera.io:666	https://52.59.120.70:443	https://212.143.240.115:666
https://lab.pcysys.com:666	https://www.pentera-demo.io:8088	https://212.143.240.115:8088
https://144.126.246.196:443	https://portal.pentera-demo.io:8088	See more assets in Pentera Surface

Serious — Website using expired certificate

7 assets

Attackers may search for websites with expired certificates in order to hijack them or otherwise use them to leverage their attacks. A website with an expired certificate reflects improper security practices and attracts attackers to look for more interesting findings on the host and the organization.

http://52.38.241.177:443	https://130.211.210.150:443	https://104.16.51.111:443
http://www.pentera.io:443	https://core.pentera.io:443	https://104.16.53.111:443
http://104.16.53.111:8443		

Moderate — Website without HTTPS enforcement

3 assets

Attackers may search for websites without an HSTS response header to perform Man-In-The-Middle attacks.

https://www.pentera.io:443	https://repo.artifactory.pentera.io	https://go.pentera.io:8443

Minimal — Potential for medium-severity vulnerabilities

3 assets

Attackers can enumerate public-facing assets to detect vulnerable services and products by correlating their findings with known vulnerabilities. The higher the severity of the vulnerabilities, the more attractive the assets from the attacker's perspective.

72.14.176.210:22/tcp	212.143.240.115:5500/tcp

Detailed Report

5 Vulnerabilities

See the vulnerabilities posing risks to your organization's attack surface.

9.9 ASP.NET Insecure Deserialization

5 assets

Attackers can exploit the improper use of ASP.NET deserialization libraries and methods to inject malicious objects and potentially achieve remote code execution (RCE) capabilities

`https://199.203.240.17:8080` `https://lab.pcysys.com:8080` `http://199.203.240.17:8080`
`http://www.pentera-demo.io:80` `http://support.pentera-demo.io:80`

Remediation

The only safe architectural pattern is not to accept serialized objects from untrusted sources or to use serialization mediums that only permit primitive data types.

9.8 Oracle WebLogic RCE (CVE-2020-14882)

2 assets

Remote attackers can exploit this vulnerability by sending a specially crafted request to the vulnerable Oracle WebLogic software. Successful exploitation could allow attackers to achieve remote code execution and web interface access, potentially leading to full system compromise.

`212.143.240.115:9002/tcp` `212.143.240.115:33060/tcp`

Remediation

Update the Oracle WebLogic software to a non-vulnerable version or limit access to recognized IPs.

6.5 Citrix ADC unauthenticated access (CVE-2020-8193)

2 assets

An attacker could send a request to the NSIP address, a dedicated IP address for the management interface of Citrix devices, and thereby bypass the authorization of the administrator login to gain direct access to the device.

`199.203.240.17:8888/tcp` `212.143.240.115:8888/tcp`

Remediation

It is recommended to update the Citrix application to a non-vulnerable version.

4.6 Reflected Cross-Site Scripting (XSS)

6 assets

An attacker can inject malicious HTML or JavaScript code into the contents of a website to steal private information from visitors such session cookies/ tokens or other sensitive information retained by the browser and used by the site. The injected code executes in the victim's browser when the victim loads the infected webpage

`http://199.203.240.17:80` `http://www.pentera-demo.io:80` `http://portal.pentera-demo.io:80`
`https://lab.pentera.io:8080` `https://support.pentera-demo.io:8080` `https://212.143.240.115:8080`

Remediation

Unavailable

2.3 Discovered closed ports on the host

2 assets

Discovered closed port on the host (reachable without firewalling).

`18.66.171.9` `52.96.109.136`

Remediation

Unavailable

Detailed Report

1,963 Achievements

6 Critical	95 High	31 Medium	1831 Low

See which attack vectors Pentera exploited on your organization's attack surface.

9.8 Executed copy command

5 assets

Due to a flow in the mod_copy module, CPFR and CPTO commands are available to unauthorized users. Pentera was able to exploit this vulnerability and copy a file on the FTP server.

`https://199.203.240.17:8080` `https://lab.pcysys.com:8080` `http://199.203.240.17:8080`
`http://www.pentera-demo.io:80` `http://support.pentera-demo.io:80`

9.8 Exploited CVE-2020-1938 on Apache Tomcat

2 assets

An attacker can read the contents of configuration files and source code files of all web applications deployed on Tomcat. If uploading files is enabled, an attacker can first upload a file containing malicious JSP script code to the server, which could lead to remote code execution.

`212.143.240.115:9002/tcp` `212.143.240.115:33060/tcp`

9.4 Gathered valuable information from host

2 assets

An attacker might find sensitive information and credentials on the host that might help in further attacks

`199.203.240.17:8888/tcp` `212.143.240.115:8888/tcp`

7.2 Gained access to Oracle WebLogic Administration Console

6 assets

Unauthenticated, remote attackers can exploit this vulnerability by sending a specially crafted request to the vulnerable Oracle WebLogic software. Successful exploitation may allow attackers to access the web admin console. This can be leveraged to fetch sensitive information and perform authenticated attacks and exploit other vulnerabilities.

`http://199.203.240.17:80` `http://www.pentera-demo.io:80` `http://portal.pentera-demo.io:80`
`https://lab.pentera.io:8080` `https://support.pentera-demo.io:8080` `https://212.143.240.115:8080`

4.6 Injected XSS payload

2 assets

Attackers can inject malicious HTML or JavaScript code into the contents of a vulnerable website to steal private information from visitors such as session cookies and tokens, or other sensitive information retained by the browser and used by the site. The injected code is executed in the victim's browser when the victim loads the infected webpage, without further user interaction

`18.66.171.9` `52.96.109.136`

1 Enumerated web services anonymously

1831 assets

An attacker may enumerate exposed web services and look for confidential data, vulnerable inputs or crack web authentication pages.

`18.66.171.9`

CONFIDENTIAL AND PROPRIETY INFORMATION

Pentera provides the Pentera™ service and report "As Is", without any warranty of any kind. Pentera makes no warranty that the information contained in this report is complete or error - free.

PENTERA