



Pentera Security Validation Report

The Pentera™ automated penetration test report summarizes the vulnerabilities, exploit achievements, and remediation action items recommended in your network based on the latest ethical hacking pentesting techniques.

Disclaimer:

For security reasons, this report is anonymized and excludes sensitive data

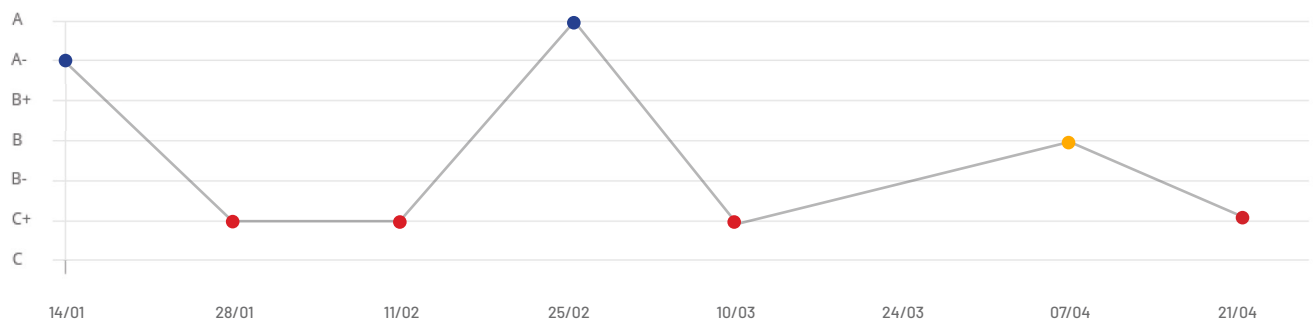
Executive Summary

Cyber Resilience Score & Settings



Name:	Black Box - Data Center C
Description:	Black Box Test - Stealthy Attacker - Bi-weekly
Type:	Penetration Testing (Black Box)
Time & Duration:	Apr 21 2025 20:12 - Apr 22 2025 02:06, 05h:54m:05s
Included IP Range(s):	192.168.90.0 - 192.168.90.9, 192... 2 Ranges
Action Approval Score:	100% - 126/126
User Input:	2 - IP Range(s)

Resilience Score Over Last 8 Tasks



Resilience Score Card

! Critical Assets Congratulations! Pentera wasn't able to compromise any critical assets in your network	Low
👤 Credentials and Account Takeover Pentera gained access to 12 privileged accounts out of 1134 using 2 techniques (password spray and post exploitation)	Critical
👤 Sniffing Sniffed 1 credentials and performed 11 relay attacks	Medium
🔒 Password Strength 8% of your passwords were cracked in under 30 minutes, a total of 111 accounts were cracked in 5 hours	High
🔑 Lateral Movement Performed lateral movement to 1 Windows Workstation(s), 1 Windows Server(s) and 1 Unix/Linux host(s)	Medium
📁 Accessible Data Gained access to 358660 File(s), 11 Hosts (with complete access) and 1 Network service(s)	Critical
🖨️ Host Takeover Pentera was able to takeover 8 out of 15 hosts (53%): 5 Windows Servers, 3 Windows Workstations	Critical
🛡️ AV/EDR Bypass Pentera bypassed 2 AV/EDR vendors and opened remote command session on 5 hosts	Low

126 Total Action Approvals



● 126 Approved (100%)
 ● 0 Not Approved (0%)

6868 Total Actions

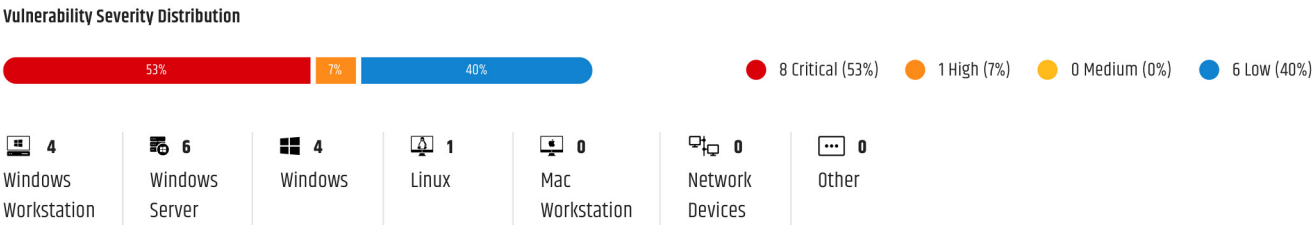


● 1554 Successful (23%)
 ● 5314 No-results (77%)

Target Network Key Findings

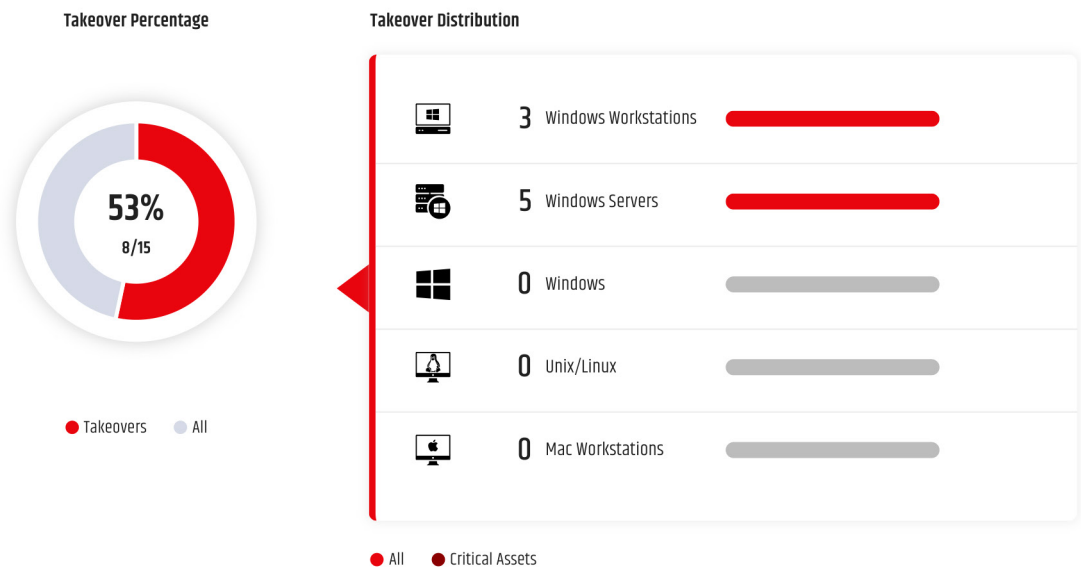
15 Discovered Hosts

Pentera identified 15 live hosts across 4 device categories, 8 were affected by critical vulnerabilities



53% Host Takeover¹

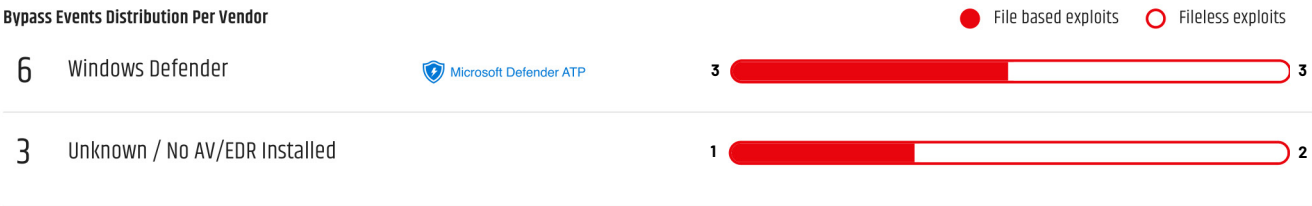
Out of 15 live hosts, Pentera took over 8 hosts



¹ Host Takeover refers to the state when an attacker achieves complete control of a remote host's operating system, installed software, hardware and files

9 Antivirus/EDR Bypass Events

Bypassed 2 AV/EDR vendors and opened remote command session on 5 hosts

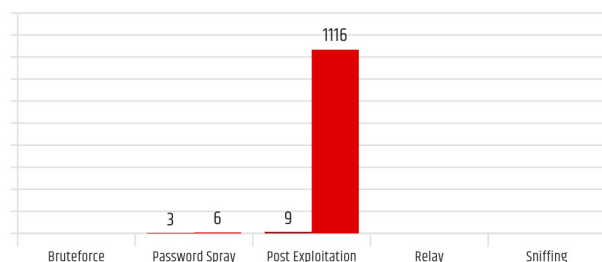


Credentials & Passwords

1134 Compromised Accounts¹

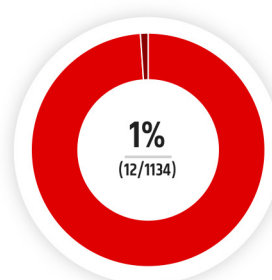
Pentera 'obtained access' to 12 privileged accounts out of 1134 using 2 techniques

Obtaining Techniques



● Non-privileged ● Privileged

Privileged Account Distribution



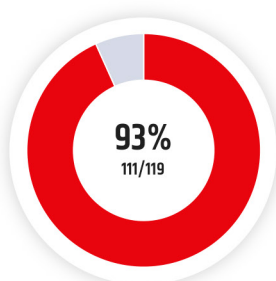
● 1122 Non-privileged (98%) ● 12 Privileged (1%)

¹ Refers to the state when Pentera was able to access an account's plaintext password, password hash (that can be used without cracking) or credentials successfully used in a relay attack.

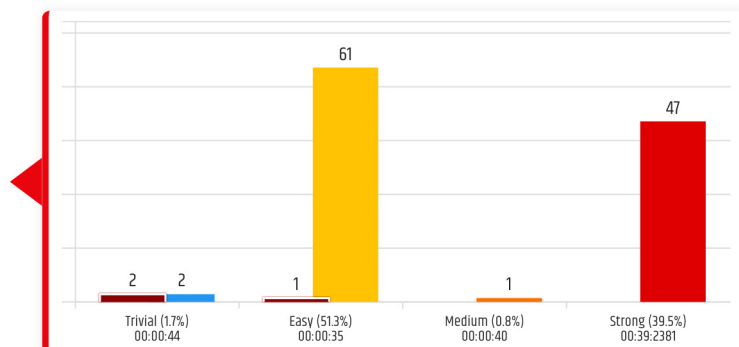
111 Passwords Cracked

8% of your passwords were cracked in under 30 minutes, a total of 111 accounts were cracked by Pentera in 5 hours.

Cracking Success Rate



Cracking Difficulty



Non-privileged Users: ● trivial ● easy ● medium ● strong ● privileged users

Compromised Accounts Table

Listing 50 of 1134 items¹.

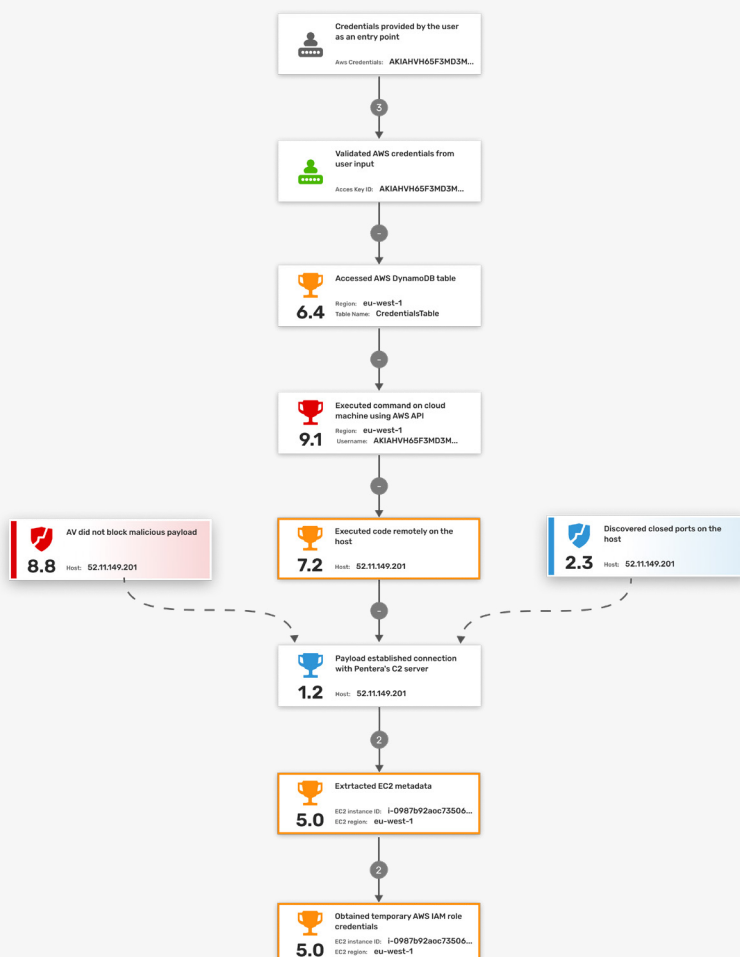
Username	Account Type	Privileged	Compromised By	Cleartext Password Obtained	Host / Domain Name
acurry	Domain User Account	No	Post exploitation	No	PENTERA.LOCAL
adanvers	Domain User Account	No	Post exploitation	No	PENTERA.LOCAL
administrator	Local User Account	No	Password spraying	No	192.168.120.4
administrator	Local User Account	No	Post exploitation	No	192.168.120.5
administrator	Local User Account	No	Post exploitation	No	192.168.120.6

Attack Kill Chain



5.0

Obtained temporary AWS IAM role credentials



Achievements

Pentera accomplished 31 achievements in total. Every achievement represents a discrete successful action performed by Pentera.

9.1

Severity

Executed command on cloud machine using AWS API

An attacker may use AWS API to remotely execute command over a cloud machine

7.2

Severity

Executed code remotely on the host

5.0

Severity

Extracted EC2 metadata

Instance metadata is used to configure and manage a running EC2 instance, and may be used to facilitate attacks if obtained by attackers. Instance metadata may include sensitive data such as identity credentials, IAM roles, public keys, and security groups.

5.0

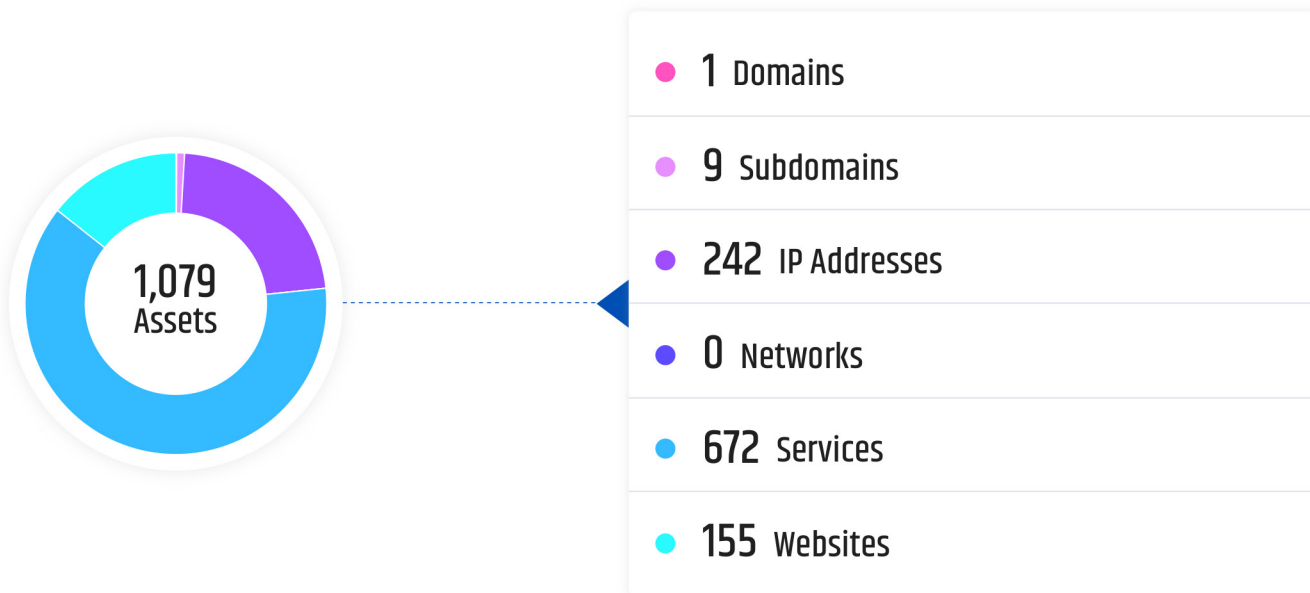
Severity

Obtained temporary AWS IAM role credentials

Attackers may find IAM role credentials attached to an EC2 instance and leverage them for cloud asset discovery and lateral movement.

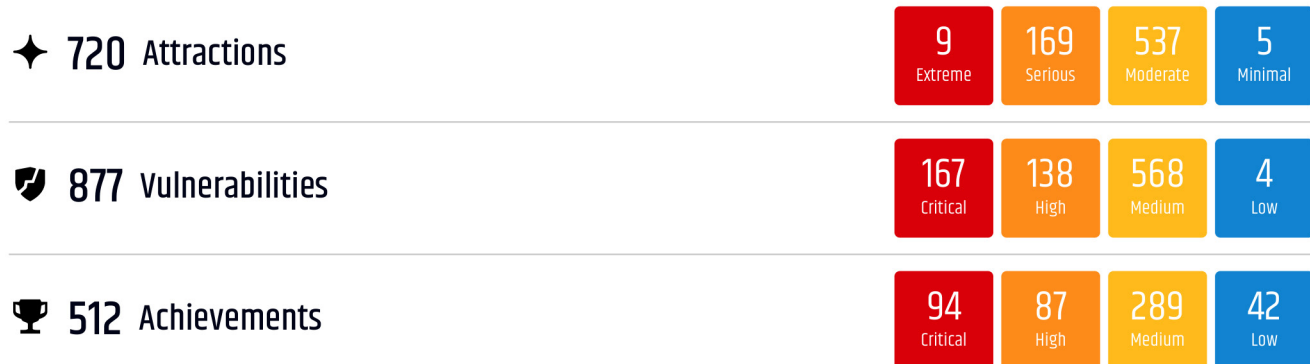
Asset Inventory

Pentera found the following assets on your attack surface.



Impacting Findings

See a breakdown by the severity of attraction, vulnerability, and achievement occurrences currently impacting your attack surface.



Past Findings

Vulnerability and achievement occurrences that were found in the past and currently do not pose a threat to your attack surface.



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.



Top Actions

Track which of Pentera's key validation actions exposed vulnerable assets in your environment. This summary highlights where real risk exists (**Found**) – and where validation confirmed no current exposure (**Not Found**).

Risk	Action	Vulnerable Assets	Status
Critical	Log4Shell (CVE-2021-44228)	4 of 133 (4%)	Found
Critical	ASP.NET Insecure Deserialization	10 of 157 (7%)	Found
Critical	Exploited Java Insecure Deserialization	10 of 157 (7%)	Found
Critical	Exploited F5 BIG-IP unauthenticated remote code execution (CVE-2022-1388)	1 of 627 (<1%)	Found
Critical	Exploited Oracle WebLogic RCE (CVE-2020-14882)	5 of 5 (100%)	Found
Critical	Exploited SQL injection	4 of 154 (3%)	Found
Critical	Fortinet Authentication Bypass (CVE-2022-40684)	1 of 98 (2%)	Found
Critical	Scanned Citrix host for CVE-2019-19781 vulnerability	1 of 116 (<1%)	Found
Critical	Scanned F5 BigIP vulnerability (CVE-2020-5902)	1 of 2 (50%)	Found
Critical	Text4Shell (CVE-2022-42889)	0 of 127 (0%)	Not found
Critical	Validated Apache Tomcat vulnerability CVE-2020-1938	2 of 2 (100%)	Found
Critical	Validated ProFTPD vulnerability CVE-2019-12815	2 of 2 (100%)	Found
Critical	Validated Sophos unauthenticated remote code execution (CVE-2022-1040)	0 of 627 (0%)	Not found
Critical	Forwarded request to arbitrary server to confirm Apache HTTP Server SSRF (CVE-2021-40438)	1 of 627 (<1%)	Found
Critical	Validated leaked credentials for SSH service	2 of 69 (3%)	Found
Critical	Local File Inclusion (LFI)	4 of 132 (4%)	Found
Critical	Exploited XML External Entity (XXE)	4 of 132 (4%)	Found
Critical	Validated leaked credentials for MySQL database	1 of 4 (25%)	Found
Critical	Validated leaked credentials for web application	4 of 37 (11%)	Found
Critical	Validated subdomain takeover using Amazon S3 bucket	1 of 10 (10%)	Found
High	Gained access to Oracle WebLogic Administration Console using authentication bypass (CVE-2020-14883)	5 of 628 (<1%)	Found
High	Scan for Citrix CVE-2020-8193	1 of 627 (<1%)	Found
High	Detected Cisco ASA/FTD vulnerability (CVE-2020-3580)	1 of 627 (<1%)	Found
High	Exploited Open Redirect vulnerability	4 of 132 (4%)	Found
High	Enumerated web directory listing	9 of 157 (6%)	Found
High	Search for enabled Remote MySQL connection	1 of 1 (100%)	Found
High	Search for enabled remote PostgreSQL connection	2 of 3 (67%)	Found
Medium	Exploited Reflected Cross-Site Scripting (XSS)	6 of 148 (5%)	Found

Ransomware Readiness



Percentage of hosts that proved resilient to ransomware. Excludes hosts with no files to test

Type	Maze Ransomware Emulation
Time	Apr 21 2025 20:12 - Apr 22 2025 02:45
Test Name	Automated_Maze
Description	Advanced Targeted Testing
IP Ranges	172.20.3.0 - 172.20.3.255, 172.21.5.0... 2 Ranges
Data Exfiltration to	Designated C2
Targeted Hosts of Testing Candidates*	80% (80 / 100)

Action Success Rate

55% (6 of 11)

	Payload Launch	55%
	File Enumeration	100%
	Process Manipulation	0%
	Encryption	100%
	Data Exfiltration	100%
	Host Modification	100%

AV / EDR Bypass
65 Hosts

Encrypted files while bypassing endpoint security controls

Ransomware Completed
60 Hosts

Performed all campaign-related actions

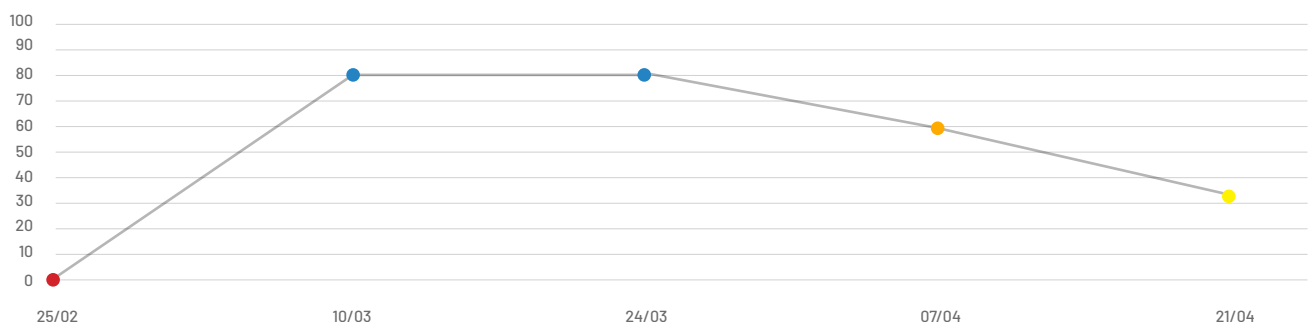
Ransomware Interrupted
15 Hosts

Interrupted by security controls or network connectivity issues

Found No Files To Encrypt
5 Hosts

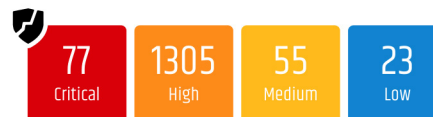
Targeted standard user-related files

Resilience Score over the last 5 runs



1460 Vulnerabilities

Pentera identified a total of 1460 vulnerability occurrences across 4 severity levels



#1

4.7

Remediation Priority

severity

Host can be forced to authenticate by a rogue server

1 occurrences

In cases where the DNS server fails in name resolution queries, the LLMNR, NetBIOS-NS and mDNS services attempt to resolve them. Since those are a broadcast protocols, anyone can respond to the query. An attacker may refer the request to a machine in his control using a man-in-the-middle attack, And obtain sensitive data such as username and password hash.

PENTERA.LOCAL

#2

8.7

Remediation Priority

severity

Password can easily be cracked leveraging leaked password

2 occurrences

Attackers can leverage leaked passwords found or sold on the darknet to gain initial access into the organization. Leaked passwords pose a risk even if they are outdated, because they can be leveraged in dictionary attacks and enhance password cracking techniques.

bbanner

nromanoff

#3

8.1

Remediation Priority

severity

Local File Inclusion (LFI)

1 occurrences

A Local File Inclusion (LFI) vulnerability exposes a path to executable code using an attacker-controlled variable, thereby allowing attackers to control which file is executed at runtime. For more details on the different types of LFI flaws, see: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

192.168.121.6

#4

8.8

Remediation Priority

severity

AV/EDR Did not block Crypto mining payload

2 occurrences

A crypto mining (Cryptojacking) payload refers to malware or unwanted software that uses a victim's computing resources to mine cryptocurrency without their consent. This type of malware runs in the background of infected computers or even web browsers, leveraging the processing power of these devices to solve complex mathematical problems that validate transactions on a blockchain network. Successful validation rewards the attacker with cryptocurrency, directly deposited into their digital wallet. Crypto mining payloads consume significant amounts of processing power and electricity, often resulting in noticeable system slowdowns, reduced performance, and higher energy bills for the unsuspecting victim.

192.168.123.2 (ENVBNEW-PDC.pentera.local)

192.168.124.6 (ENVBNEW-2012SRV.PENTERA.LOCAL)

#5

8.8

Remediation Priority

severity

PrintNightmare (CVE-2021-34527)

9 occurrences

A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

192.168.124.3 (ENVBNEW-FILESRV.pentera.local)

192.168.123.20 (WIN10A.pentera.local)

192.168.123.21 (WIN10B.pentera.local)

192.168.124.5 (ENVBNEW-2016SRV.pentera.local)

192.168.123.22 (WIN10C.pentera.local)

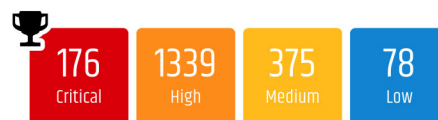
192.168.124.4 (ENVBNEW-DC-CA.PENTERA.LOCAL)

192.168.123.2 (ENVBNEW-PDC.pentera.local)

192.168.124.6 (ENVBNEW-2012SRV.PENTERA.LOCAL)

192.168.121.2 (ENVBNEW-PDC.pentera.local)

1968 Achievements



Pentera accomplished 1968 achievements in total. Every achievement represents a discrete successful action performed by Pentera.

10

(2) Completed ransomware attack kill chain on the host

Severity

Pentera was able to execute an end-to-end attack of the selected ransomware family without being blocked.

9.7

(2) Executed crypto mining payload on host

Severity

An attacker successfully executing a crypto mining payload on a host bypasses security protocols, turning the compromised machine into a source of income by mining cryptocurrency. This unauthorized use of computing resources not only indicates the presence of malware within the network but also serves as a precursor to potentially more damaging activities. The execution of such payloads can severely degrade system performance, increase energy consumption, and disrupt business operations.

9.4

(3) Gathered valuable information from host

Severity

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

9.2

(1) Accessed sensitive system file

Severity

Attackers can retrieve the shadow file from a host

9.1

(12) Executed command on cloud asset using AWS API

Severity

An attacker may use AWS API to remotely execute command over a cloud machine

8.8

(1) Obtained EKS credentials from AWS credentials

Severity

Attackers with token to EKS can use it to attack to Kubernetes platform in the organization.

✨ Black Box – Data Center C

Jan 15, 2025 – Mar 15, 2025

Security Insights are based on this test and 4 successfully completed tests that preceded it.

Recent findings show clear progress in reducing high-impact exposures and disrupting attacker movement across the environment. However, newly surfaced risks and critical regressions—like compromised credentials and remote code execution—underscore the need for continuous testing and focused remediation.

Vulnerability Trend Analysis

Total # of Vulnerabilities
24% ↓
139 fewer vulnerabilities

Critical Vulnerabilities
77% ↓
17 fewer critical vulnerabilities

Achievement Trend Analysis

Total # of Achievements
3% ↑
17 additional achievements

Critical Achievements
19% ↓
4 fewer critical achievements

Notable Improvements

Spring4Shell 25 ↓
API secrets exposed in web page content 2 ↓
Local File Inclusion (LFI) 1 ↓

Notable Improvements

Injected probing payload 12 ↓
Accessed sensitive system file 1 ↓

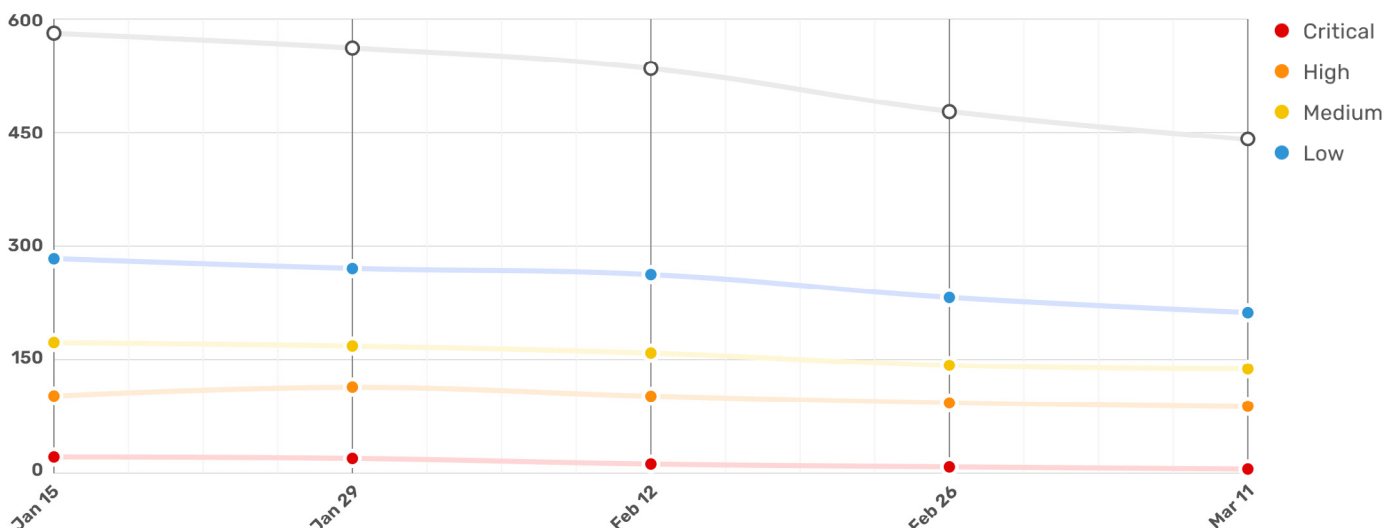
Key Regressions

Rejto HTTP File Server RCE (CVE-2024-23692) 2 ↑
Password can be easily cracked 7 ↑
Insecure SNMPv2 5 ↑

Key Regressions

Gathered valuable information from host 5 ↑
Extracted SCCM NAA credentials 2 ↑
Rejto HTTP File Server RCE (CVE-2024-23692) 2 ↑

Vulnerability trend analysis



Black Box – Data Center C

Jan 15, 2025 – Mar 15, 2025

Security Insights are based on this test and 4 successfully completed tests that preceded it.

What should we remediate first?

Rejetto HTTP File Server RCE (CVE-2024-23692)

9.8

Severity

2

Occurrences

Risk: Allows remote code execution via shared libraries
Action: Restrict access to exposed SMB services and disable writable shares where unnecessary

Host can be forced to authenticate by a rogue server

4.7

Severity

1

Occurrences

Risk: Enables man-in-the-middle attacks & data theft
Action: Disable LLMNR protocol in group policy settings

Local file inclusion (LFI)

8.1

Severity

1

Occurrences

Risk: Allows execution of arbitrary files on the server through poorly sanitized input
Action: Use allowlists for file access, and disable unnecessary file-handling functions

Security posture improvement – key areas

Network Security

Secure protocols (SNMPv3), disable unnecessary services (LLMNR), and monitor network traffic for unauthorized access attempts

Why it requires attention

Attackers often exploit insecure protocols and legacy services to gain initial access or move laterally inside the network

Web Application Security

Validate user input, sanitize outputs, and keep software up-to-date to prevent LFI attacks

Why it requires attention

Attackers exploit such web application exposures to inject malicious input and access sensitive data such as logs and credentials

Identity Strength

Strengthen password policies, enforce MFA

Why it requires attention

Weak credentials and access controls provide an easy way for attackers to extend their reach inside the network and escalate privileges

MITRE ATT&CK Matrix for Enterprise - Heat Map

MITRE ATT&CK®	Total Patterns	Most Common Technique
	3373	Execution / System Services

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning T1595 ^	Exploit Public-Facing Application T1190	Exploitation for Client Execution T1203	Create Account T1136 ^	Access Token Manipulation T1134 ^	Indicator Removal T1070 v
Scanning IP Blocks T1595.001	Valid Accounts T1078 ^	Windows Management Instrumentation T1047	Domain Account T1136.002	Make and Impersonate Token T1134.003	Access Token Manipulation T1134 v
Vulnerability Scanning T1595.002	Domain Accounts T1078.002	System Services T1569 ^	Account Manipulation T1098	Token Impersonation/Theft T1134.001	System Services T1569 v
Gather Victim Network Information T1590 ^		Service Execution T1569.002		Create or Modify System Process T1543 ^	Software Deployment Tools T1072
DNS T1590.002		Command and Scripting Interpreter T1059 ^		Windows Service T1543.003	Obfuscated Files or Information T1027 v
Search Open Technical Databases T1596 ^		PowerShell T1059.001		Exploitation for Privilege Escalation T1068	Trusted Developer Utilities Proxy Execution T1127 v
DNS/Passive DNS T1596.001		Scheduled Task/Job T1053 ^			System Binary Proxy Execution T1218
Network Service Discovery T1046		Scheduled Task T1053.005			Process Injection T1055 v
					Reflective Code Loading T1620
					Rogue Domain Controller T1207

LLMNR - Multicast Name Resolution

MITRE

LLMNR/NBT-NS Poisoning and Relay (T1171)

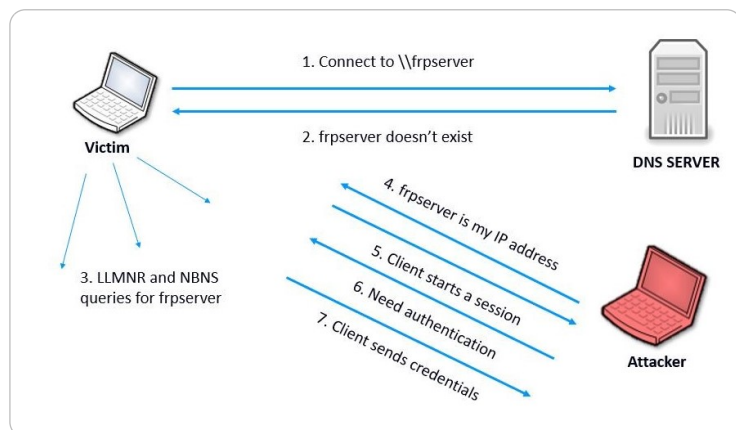
Insight

LLMNR (Link-Local Multicast Name Resolution), NBNS (Netbios Name Service) and mDNS (Multicast Domain Name Service) are Microsoft Windows protocols which serve as alternate methods of Name Resolution. If a machine tries to resolve a particular host, but DNS resolution fails, the machine will then attempt to ask all other machines on the local network for the correct address via LLMNR, NBNS or mDNS. Since this operation is performed using broadcast or multicast queries with no means of validation, it is susceptible to malicious answers distributed by an attacker, effectively poisoning the network.

Impact

An attacker can listen on a network for these LLMNR (UDP/5355) or NBNS (UDP/137) broadcasts and respond to them, pretending that the location of the requested host is at the attacker's machine.

Let's look at an example in the diagram below:



1. The victim machine wants to go the print server at \\ftpserver, but mistakenly types in \\frpsrvr
2. The DNS server responds to the victim that no dns record was found
3. The victim turn to the network and asks by using LLMNR or NBNS if there is anyone knows the location of \\pntserver
4. The attacker responds to the victim that \\pntserver is his own IP address
5. The victim believes the attacker and starts a session with him
6. The attacker asks the victim to authenticate
7. The client sends its credentials (NTLMv1 / NTLMv2)
8. The attacker can now crack the hash to discover the password

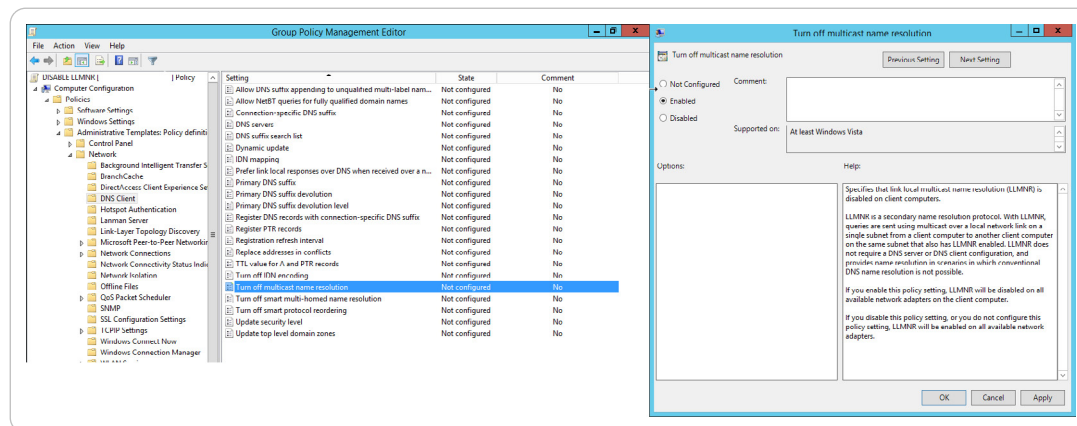
Recommendations

Disable the protocols: mDNS, LLMNR, and NBNS.

Disable mDNS

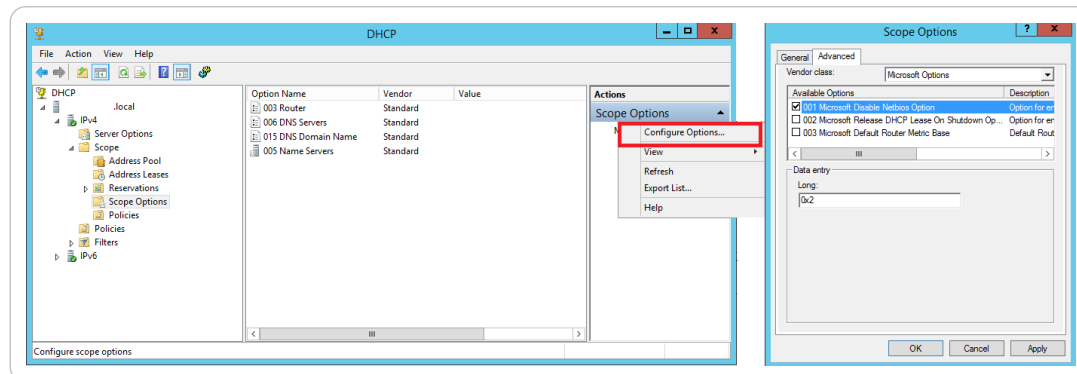
There is a `mDNSResponder.exe` process that belongs to the `Bonjour Service` in Windows, which is Apple's "Zero Configuration Networking" application, typically installed automatically by iTunes, Skype and others. It can be disabled by using GPO.

Disable LLMNR via GPO



1. Create a new GPO record for all computers in the environment.
2. Navigate to **Local Computer Policy / Computer Configuration / Administrative Templates / Network / DNS Client**.
3. Set **Turn Off Multicast Name Resolution** to **Enabled**.

Disable NBNS in a DHCP environment



1. Go to DHCP Management
2. Go to "scope options" for the network you are changing
3. Right click and Configure Options
4. Select Advanced tab and change "Vendor class" to "Microsoft Options"
5. In the "Available Options" frame, select and check the box "001 Microsoft Disable Netbios Option"
6. In the "Data Entry" frame, change the data entry to 0x2
7. Click "OK". The new settings will take affect when the clients renew their addresses.

Disable NBNS on a single host

1. Open the **Control Panel > Network and Sharing Center**.
2. Select **Change adapter settings**.

