ABACUS

PENETRATION TESTING REPORT

CONFIDENTIAL // ABACUSTECHNOLOGY.COM

CLIENT [redacted]

ASSESSMENT DATE

REPORT VERSION

CLASSIFICATION

[redacted]

External and Internal Network Penetration Testing Report

2026Q2 / 1

Project Objective

Abacus was contracted by [redacted] ([redacted]) to perform an external and Internal penetration test between the dates of 4/8/2026, and 5/1/2026, on [redacted] internal and external infrastructure.

Objectives of this Exercise:

- Replicate the vantage point and attack vectors of a malicious actor whose objective is to gain access to [redacted] information systems by breaching the external network perimeter.
- Identify high-risk security gaps in [redacted] internal information systems and technical security controls.
- Replicate the vantage point and attack vectors of a malicious actor who has breached [redacted] externally facing perimeter and is trying to laterally move across [redacted] internal information systems.
- Bring attention to the weakest areas of [redacted] security posture by exploiting the highest risk security gaps and attack vectors present across [redacted] internal and external network.
- Provide full due diligence information to [redacted] such as vulnerability details, risk mitigation recommendations, reconnaissance processes, exploitation methods, information system statistics, any compromised credentials, any acquired system configuration files, kill-chain diagrams, network diagrams, and more.

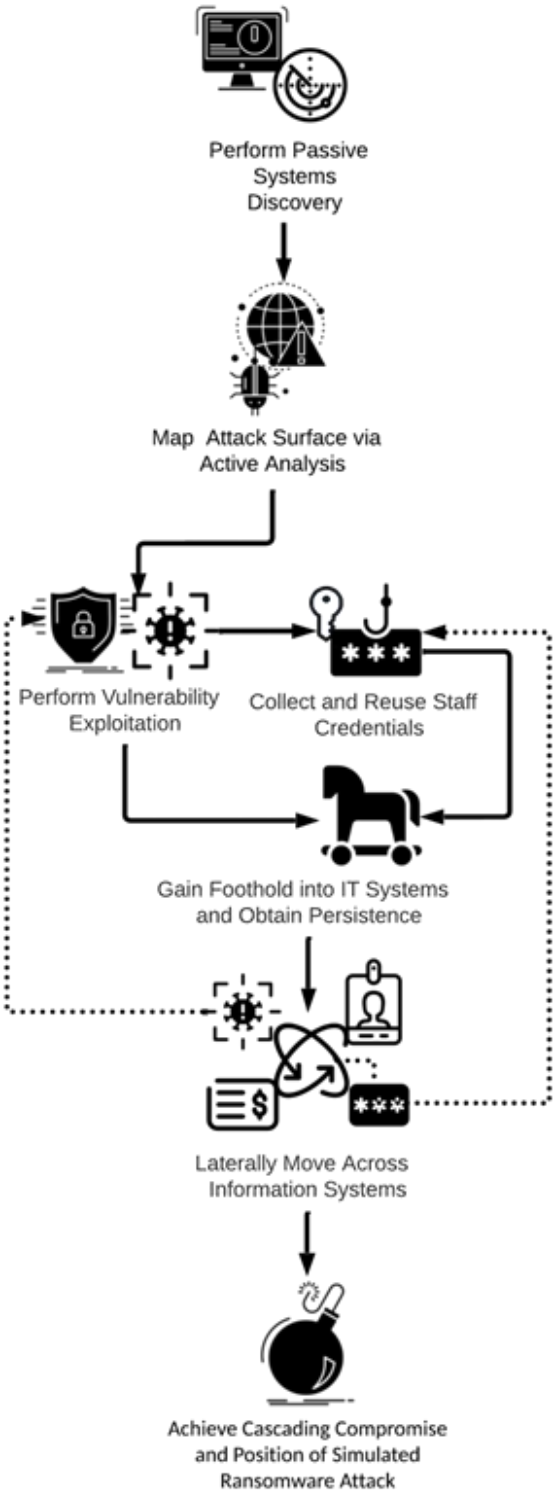
Abacus performed testing in accordance with NIST SP800-115 (Technical Guide to Information Security Testing and Assessment), PTES (Penetration Testing Execution Standard), and the MITRE ATT&CK framework. The findings in this report are not necessarily exhaustive; they are limited to IT system targets within the signed Rules of Engagement (RoE) scope or directly approved by [redacted] point of contact during the engagement. Furthermore, resource restrictions and the need to avoid disrupting business operations limit the testing that may be performed.

This report reflects [redacted] security posture, as seen during the dates in which the penetration testing was conducted. Future changes to any applications or infrastructure will alter the security position of the environment from its current state. Additionally, as time passes, new attacks may arise that were previously unknown to the security industry. Considering this, Abacus always recommends that all information systems undergo recurring security testing within a reasonable timeframe.

Table of Contents

Project Objective 2
Table of Contents 3
Penetration Testing Methodology 4
Risk Scoring 5
Risk Results Key 6
Penetration Testing Summary 8
External Network Penetration Testing Narrative 10
Internal Network Penetration Testing Narrative 31
Risk Details 46
Conclusion 72
About the Security Testers: 73
Appendix A - MITRE ATT&CK Tactic Definitions 74

Penetration Testing Methodology

Pentesting Phases	MITRE ATT&CK Tactics	Abacus Group's Standard Kill Chain
Conduct Organizational Reconnaissance	Reconnaissance TA0043	
Conduct Intelligence Gathering	Resource Development TA0042	
Analyze the Attack Surface		
Conduct Initial Exploitation	Initial Access TA0001	
Establish a Foothold	Execution TA0002	
	Persistence TA0003	
	Defense Evasion TA005	
Conduct Lateral Movement	Lateral Movement TA0008	
Privilege Escalation	Privilege Escalation TA0004	
	Discovery TA0007	
	Collection TA0009	
Establish Command and Control	Command and Control TA0011	
Demonstrate the Practical Impact	Impact TA0040	

Risk Scoring

To present the findings in a manner easily digested and prioritized, Abacus uses the traditional aspects of Magnitude of Impact and Ease of Exploitation to determine the Level of Risk associated with individual findings identified in this security assessment.

Magnitude of Impact

The Magnitude of Impact rating is a measure of the damage each weakness could inflict on the organization and is based on access, data, etc., obtained through exploitation (i.e., level of access gained, types of information accessed, the strength of security measures bypassed)

Rating	Definition
HIGH	Exploitation could seriously affect system confidentiality, availability, integrity, or authentication. Resources to mitigate high risks should receive priority.
MODERATE	Exploitation could moderately affect system confidentiality, availability, integrity, or authentication.
LOW	Exploitation could minimally affect system confidentiality, availability, integrity, or authentication. The presence of multiple low impact findings could result in a finding with a higher impact rating.

Ease of Exploitation

The Ease of Exploitation rating measures the degree of difficulty for exploiting each finding. The higher the rating, the easier it is to exploit the finding and, therefore, the more likely it is to be exploited

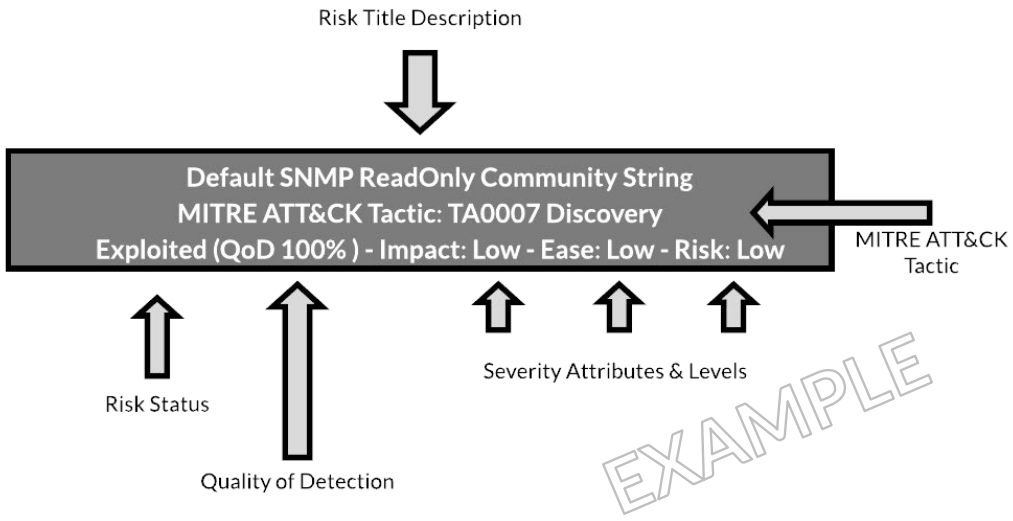
Rating	Definition
HIGH	Exploitation is easily accomplished using freely and readily available tools, techniques, and exploits.
MODERATE	Exploitation is moderately accomplished using a combination of freely available and custom tools, techniques, and exploits.
LOW	Exploitation is difficult to accomplish and requires a significant investment of time to develop custom tools, techniques, and exploits.

Level of Risk

		MAGNITUDE OF IMPACT		
		HIGH	MODERATE	LOW
EASE OF EXPLOITATION	HIGH	HIGH	MODERATE	MODERATE
	MODERATE	MODERATE	MODERATE	LOW
	LOW	MODERATE	LOW	LOW

Security Findings that are noteworthy but do not have an associated risk are labeled as Informational. Informational Security Findings are not inherently usable as attack vectors but may have associated operational excellence recommendations for implementing additional technical safeguards and controls.

Risk Results Key

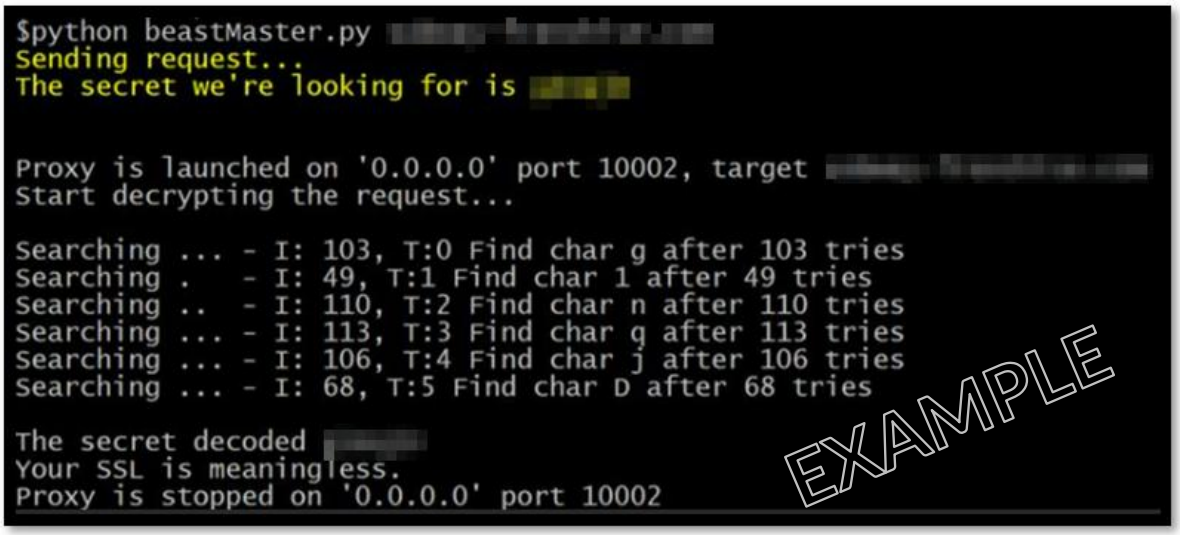


- **Risk Title Bar**
  - ***Risk Title Description***
    - Contains a brief description of the pertinent risk.
  - ***MITRE ATT&CK Tactic***
    - Defines the MITRE ATT&CK Tactic category to which the risk is most closely associated to.
  - ***Risk Status***
    - Specifies if the risk was detected or exploited. In many situations, a high-severity risk is detected but not exploited due to the potential service impact to a production system and subsequent violation of the project Rules of Engagement (RoE).
    - In some cases of a service-impactful risk, a proof-of-concept exploit can be safely performed.
  - ***QoD (Quality of Detection)***
    - For "*Detected*" but not exploited risks, QoD is a value between 0% and 100% (i.e., confidence) that ranks the reliability of the executed network vulnerability test or fingerprinted information system.
  - ***Impact***
    - The Impact rating is a measure of the damage each weakness could inflict on the organization and is based on access, data, etc., obtained through exploitation.
  - ***Ease***
    - The Ease rating measures the degree of difficulty for exploiting each finding. The higher the rating, the easier it is to exploit the finding and, therefore, the more likely it is to be exploited.
  - ***Risk***
    - The Risk rating is based largely upon the potential negative impact to the pertinent environment combined with the ease of exploitation as illustrated in the matrix on the previous page.

Insecure TLS Protocols and Cipher Suites Susceptible to BEAST Attack
MITRE ATT&CK Tactic: TA0001-Initial Access
Exploited – **Impact:** Moderate – **Ease:** Moderate – **Risk:** Moderate

Summary:
The affected endpoints supported outdated TLS versions 1.0 and 1.1, along with weak cipher suites with known attacks. This may allow a malicious actor to sniff webserver traffic and decrypt the content of an encrypted session, gaining access to potentially sensitive information. TLSv1.0 is considered obsolete, and TLSv1.1 is rapidly being retired from production. It was possible to leverage the Browser Exploit Against SSL/TLS (BEAST) attack to defeat TLS on the affected endpoints.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Update TLS configurations for modern or intermediate compatibility. Intermediate is the recommended configuration for the vast majority of services that do not need compatibility with legacy clients, such as Windows XP or old versions of OpenSSL, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

- **Risk Body**
  - ***Summary***
    - Contains a high-level overview of the risk description.
  - ***Risk Detection Result(s)***
    - Demonstrates evidence that the risk exists, showcases exploitation if exploitation was performed.
  - ***Risk Mitigation Recommendation(s)***
    - Gives recommendations on how to best mitigate this risk.
  - ***Reference(s)***
    - Lists useful outside references that elaborate on the risk and/or provide additional mitigation recommendations.
  - ***Affected Endpoint(s)***
    - Lists every endpoint detected as being affected by this risk.

Penetration Testing Summary

[redacted]

Organization	[redacted]		
Point of Contact Name	[redacted]	Security Testing Timeframe	April 8th, 2026 - May 1st, 2026
Point of Contact Phone	N/A	Point of Contact Email	[redacted]

Total Count of Security Findings: 16

2	7	5	2
High	Moderate	Low	Informational

Summary of Risk Results	
Risk Title Description	**Affected Endpoint(s)**
PDU with Default Credentials [Internal]	[redacted]
ASREP Roasting – User Accounts With Kerberos Pre-Authentication Disabled [Internal]	[redacted]
OpenSSH Susceptible to CVE-2024-6387 [Internal]	[redacted]
Externally Exposed NTLM Authentication [External]	[redacted]
Subdomain Takeover via Dangling DNS [redacted] [External]	[redacted]
SMB Signing Not Required and Enforced [Internal]	[redacted]

	[redacted]
Missing HTTP Security Headers [External]	[redacted]
Unauthenticated Internal Web Portal [Internal]	[redacted]
End of Support Exchange Server [External]	[redacted]
Vulnerable and Outdated Web Technologies [External]	[redacted]
SMB Null Session Allowed [Internal]	[redacted]
Expired and Untrusted TLS/SSL Certificates [External]	[redacted]
Missing or Misconfigured SPF and DMARC [redacted] [External]	[redacted]
Insecure TLS 1.2 Cipher Suites [External]	[redacted]
Outdated OpenSSH With Known Vulnerabilities [Internal]	[redacted]
Missing SPF Hard Fail and DMARC Reject [External]	[redacted]

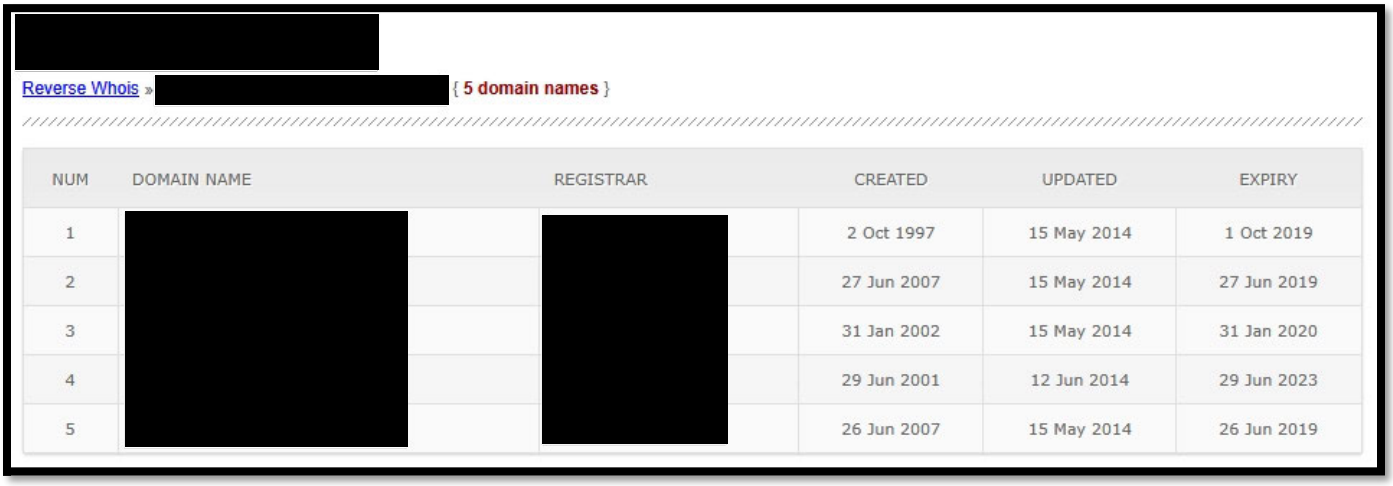
External Network Penetration Testing Narrative

Abacus's role was to replicate the vantage point of a malicious actor with no access or prior information about [redacted] information systems. This engagement was a full-scope external network penetration test designed to assess how well [redacted] networks could withstand an attack from a sophisticated, real-world adversary. All penetration testing activities performed by Abacus came from the source subnets of [redacted] as defined in the RoE. All automated penetration testing activities performed by NodeZero were manually reviewed by Abacus and originated from the source address of [redacted]

Abacus approached the engagement from a fully black-box perspective. The engagement began by performing passive reconnaissance and information gathering to gain an understanding of [redacted] online footprint and external attack surface.

Abacus began the assessment by performing reconnaissance to identify domain registrar information, alternate company names, other owned domain names, and to check for information disclosures. This analysis identified additional registered domain names for the company. A total of 18 domains were identified registered to [redacted] Group Services.

WHOXY – identified a privacy redaction service and no pertinent registrant information



WHOXY – identified additional domains registered to the company (1 of 2)

[redacted]

Reverse Whois » NAME [redacted] { 12 domain names }

NUM	DOMAIN NAME	REGISTRAR	CREATED	UPDATED	EXPIRY
1	[redacted]	[redacted]	29 Jun 2001	15 May 2019	29 Jun 2023
2			30 Apr 2012	1 May 2017	30 Apr 2022
3			30 Apr 2012	30 Apr 2017	29 Apr 2022
4			31 Jan 2002	17 Jan 2017	31 Jan 2019
5			27 Jun 2007	13 Jun 2017	27 Jun 2019
6			13 Jun 2014	13 Jun 2014	13 Jun 2019
7			29 Jun 2001	15 Jun 2017	29 Jun 2019
8			26 Jun 2007	12 Jun 2016	26 Jun 2018
9			12 Jun 2014	12 Jun 2014	12 Jun 2019
10			12 Jun 2014	12 Jun 2014	12 Jun 2019
11			31 Jan 2002	17 Jan 2017	31 Jan 2019
12			12 Jun 2014	12 Jun 2014	12 Jun 2019

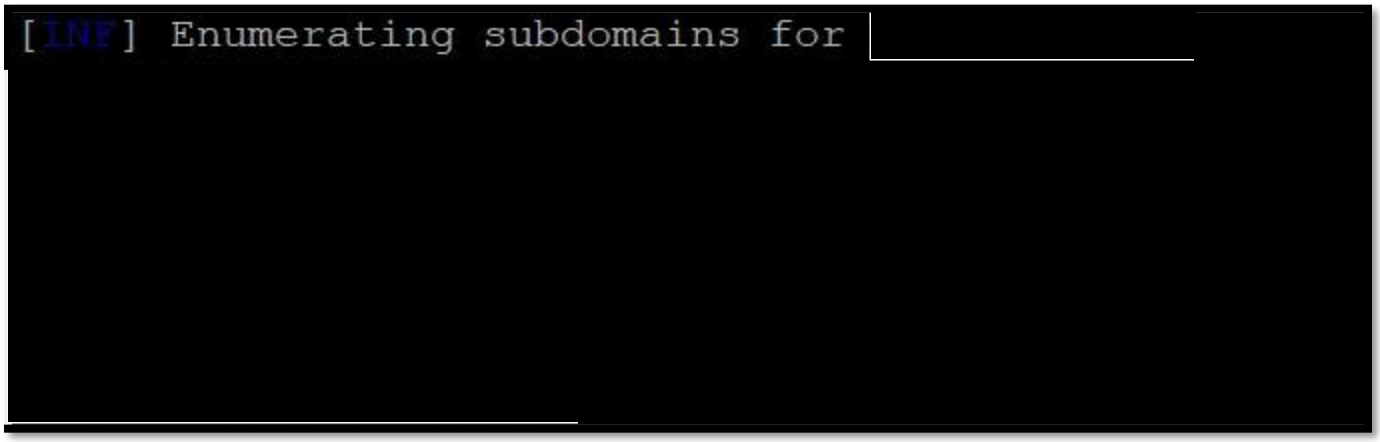
WHOXY – identified additional domains registered to the company (2 of 2)

Subdomain enumeration was performed using techniques such as wordlist-based DNS resolution, reverse IP address lookups, MX and SOA [redacted] inspection, Autonomous System (AS) number lookups, and certificate transparency log review. This helped provide a baseline of IP addresses and subdomains associated with <>, including server infrastructure and external web applications. These techniques allowed Abacus to establish an understanding of the full attack surface of the organization. This information was then corroborated by leveraging powerful open-source intelligence (OSINT) tools such as OWASP Amass.

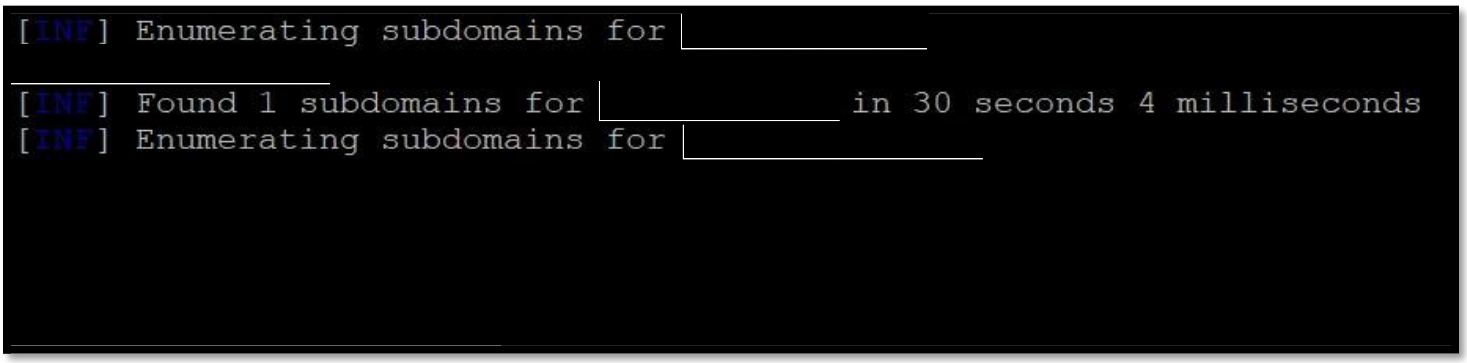
```
administrator@ubuntu-2404:~/2026Q1-
 03-31 17:08 > amass enum -passive -df whoxy-domains
rtml.com
```

OWASP Amass – passive subdomain enumeration was performed on the identified domains

OWASP Amass – passive subdomain enumeration identified ASN and IP information for the domains



subfinder – identified additional subdomains for each domain (1 of 2)



subfinder – identified additional subdomains for each domain (2 of 2)

DNS Zone Transfer (AXFR) requests were sent to the name servers for the domains. Name servers should not permit zone transfers towards any IP address from the internet. Since zone files contain complete information about domain names, subdomains, and IP addresses configured on the target name server, finding this information is useful for the reconnaissance of external and internal company information systems. However, no relevant DNS entries were found to be vulnerable to DNS Zone Transfer attempts.

```
04-09 13:17 > dig @ns47.domaincontrol.com
;; communications error to                end of file
;; communications error to                end of file
;; communications error to                end of file
;; Connection to 2603:5:2172::18#                    for            failed: network unreachable.
;; no servers could be reached
```

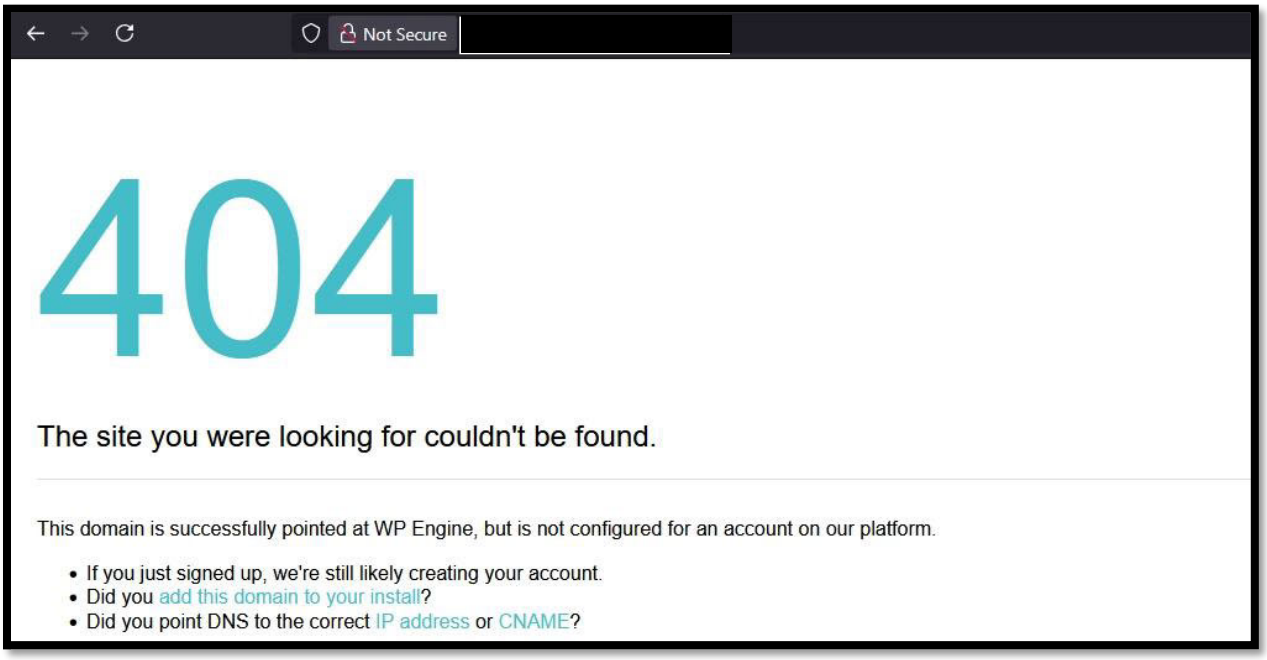
```
04-09 13:18 > dig @ns76.domaincontrol.com            AXFR
;; communications error to                end of file
;; communications error to                end of file
;; communications error to                end of file
;; Connection to 2603:5:22b4::30#                    for recordfg.com failed: network unreachable.
;; no servers could be reached
```

dig – no AXFR requests were successful

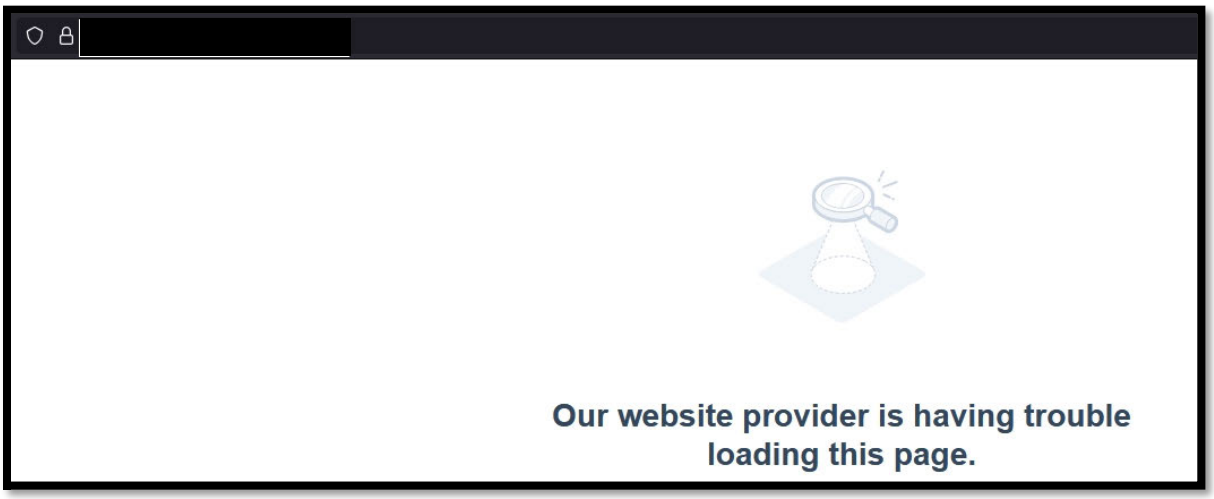
Scanning for subdomain takeover vulnerabilities was also performed on the identified domains. Subdomain takeover is a type of vulnerability that appears when an organization has configured a DNS CNAME entry for one of its subdomains pointing to an external service (e.g. Heroku, GitHub, Bitbucket, Desk, Squarespace, Shopify, etc.) but the organization no longer utilizes the service. An attacker could register to the external service and claim the affected subdomain. As a result, the attacker could host malicious code (e.g. for stealing HTTP cookies) on the organization's subdomain and use it to attack legitimate users. Three domains were identified that were possibly vulnerable to subdomain takeover utilizing HubSpot, WPE Proxy, and Freshservice services due to dangling DNS [redacted]

```
[INF] Current dnsx version 1.2.3 (latest)
www.              [CNAME] [              ]
www.                                [CNAME] [                              .co.uk]
www.              .co.uk [CNAME] [              .co.uk]
www.           uk [CNAME] [           .uk]
www.              .uk [CNAME] [              .uk]
www.              .com [CNAME] [              .com]
www.                           com [CNAME] [                              .com]
www.                           .co.uk [CNAME] [                              .co.uk]
www.              [CNAME] [           .com]
www.          uk [CNAME] [           .uk]
www.          mobi [CNAME] [           .mobi]
www.          com [CNAME] [           .wpeproxy.com]
www.                           .uk [CNAME] [                              .uk]
www.          [CNAME] [      .com]
www.          co.uk [CNAME] [           .co.uk]
insights.          com [CNAME] [7324295.group45.sites.hubspot.net]
www.              [CNAME] [           .com]
helpdesk.          com [CNAME] [fseuc-1b3-d49.freshservice.com]
www.                           com [CNAME] [                              .com]
www.              [CNAME] [           .biz]
```

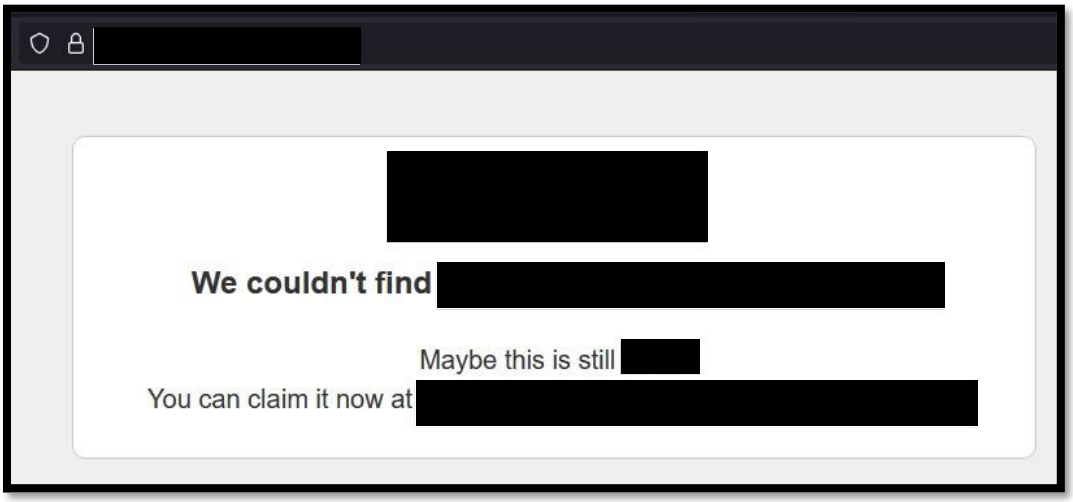
dnsx – identified dangling DNS [redacted] potentially vulnerable to subdomain takeover



Browser – identified a dangling WP Engine page that was not active

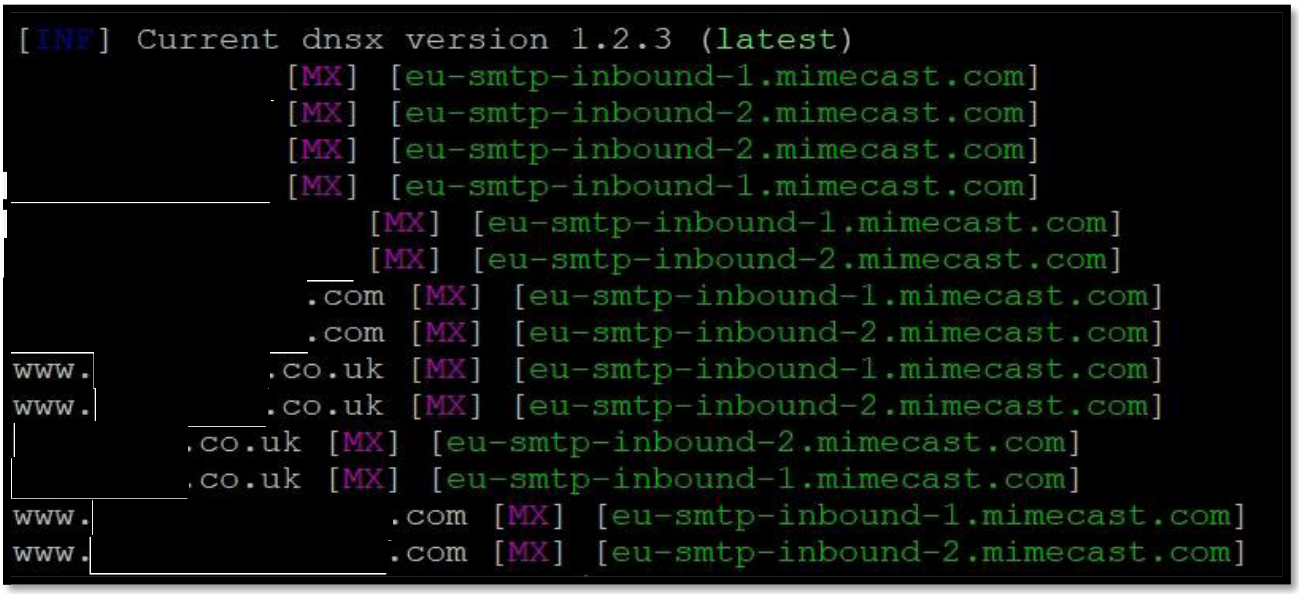


Browser – identified a dangling HubSpot page that was not active



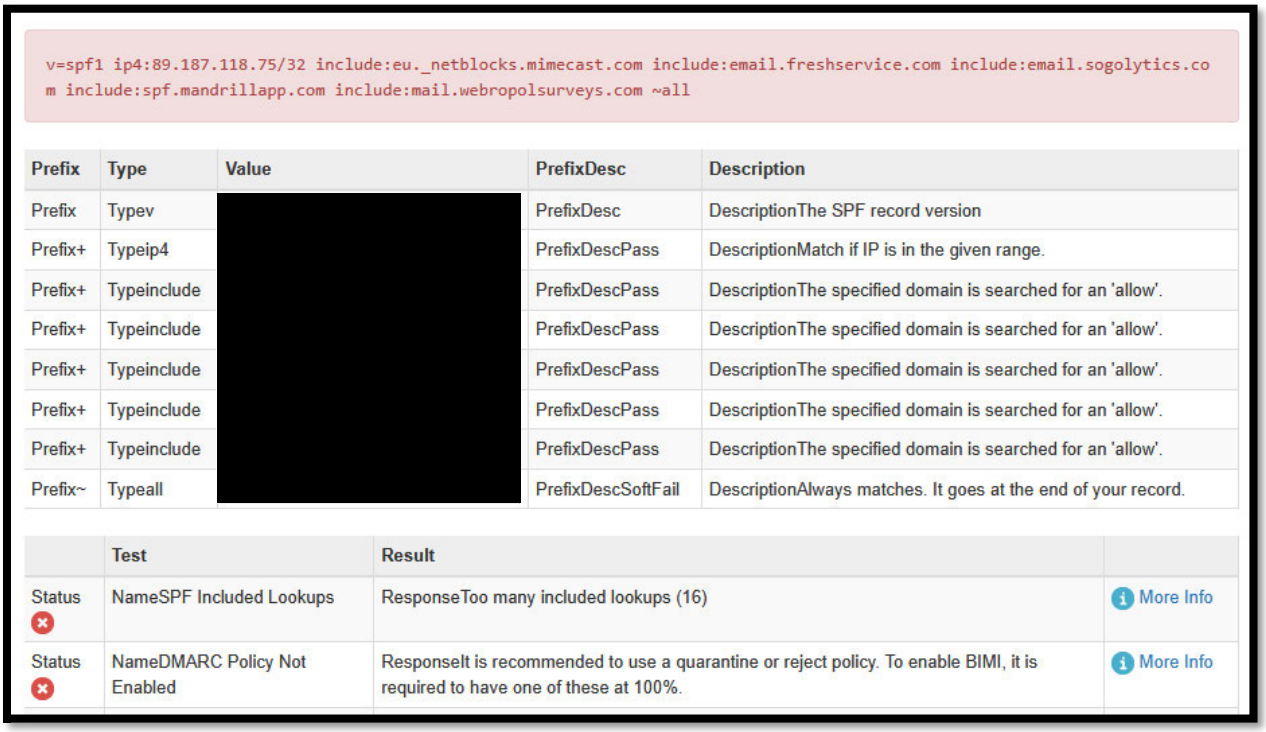
Browser – identified a dangling Freshservice page that was not active

Mail [redacted] (MX) and TXT [redacted] were analyzed for misconfigurations with Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). SPF works by ensuring that only approved mail servers can send emails on behalf of the organization. DKIM uses digital signatures to verify that email messages have not been tampered with or modified in transit. DMARC expands on these protections by enforcing a policy for unverifiable emails, which include actions like rejection or quarantine. Utilized together, these controls help mitigate email spoofing and help protect against phishing attacks.



dnsx – MX [redacted] identified Mimecast email services

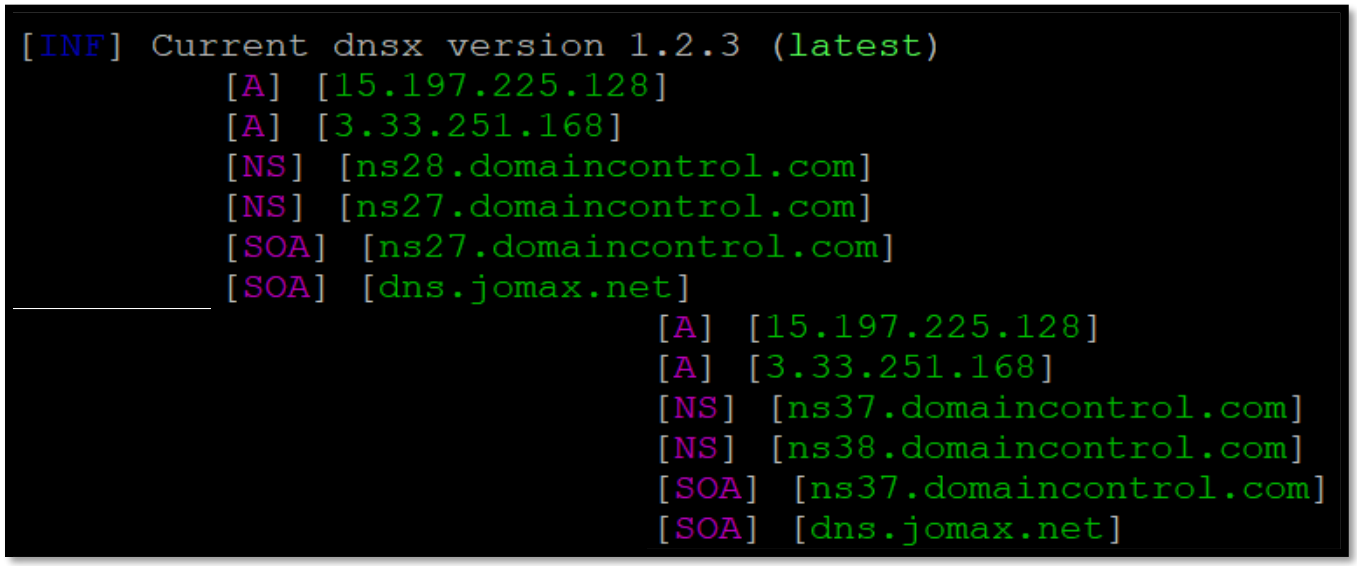
Abacus identified that the main "[redacted]com" domain implemented a misconfigured SPF [redacted] that resulted in more than 10 DNS lookups by the receiving server. Since this is a violation of RFC 7208, this could result in email delivery issues for receiving email servers. Additionally, Abacus identified that the DMARC policy was set to 'none' which does not provide a policy for receiving email servers for what to do with spoofed email.



MxToolbox – identified a misconfigured SPF and DMARC policy

dig – DMARC policy was set to 'none' rather than 'reject' or 'quarantine'

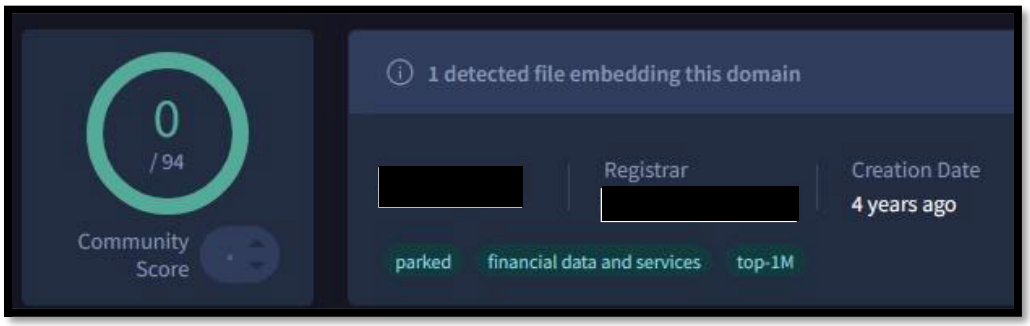
Abacus additionally noted that the parked domains redirected to the main "[redacted]com" domain, but did not include SPF and DMARC [redacted] to mitigate email spoofing. Non-sending domains that are not authorized to send email should be configured with SPF hard fail and DMARC 'reject' policies to mitigate email spoofing from owned but parked domains.



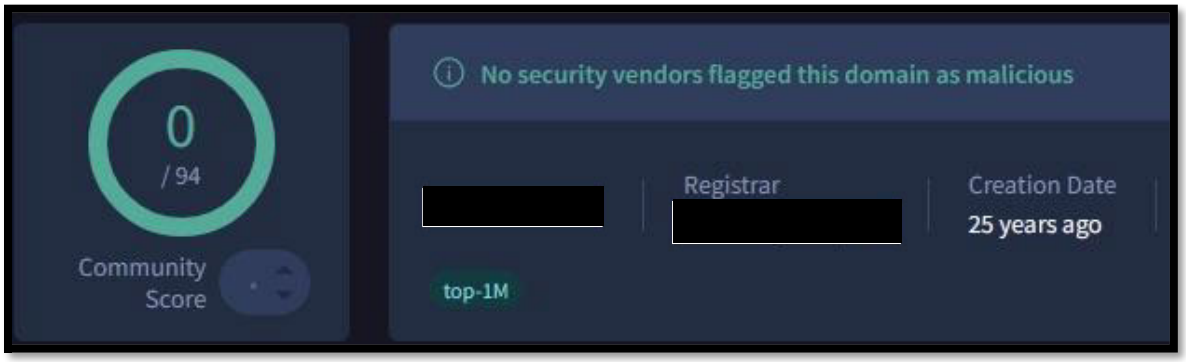
dnsx – parked domains did not include SPF [redacted] with hard fail on all authorized senders

dig – no DMARC policies were identified on parked domains with rejection policies

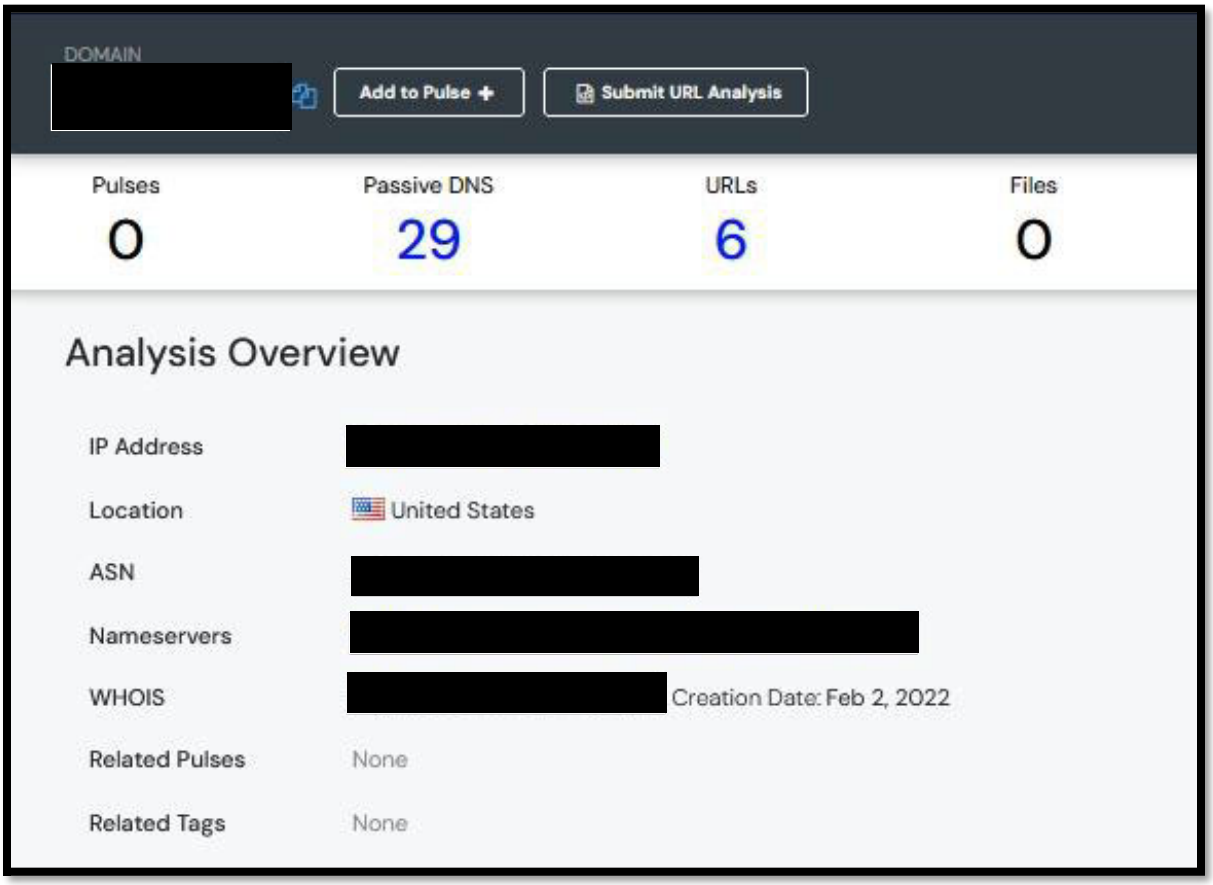
To further supplement passive analysis and OSINT data collection, Abacus utilized online threat intelligence platforms to collect information about any potential indicators of compromise (IoCs) and other relevant OSINT data potentially affecting [redacted] information systems. Google Dorking was also performed to search for exposed log files, company documents, login pages, databases, or paste dump sites that could appear online within search indexes. No indicators of compromise were identified, and no sensitive indexed files were found.



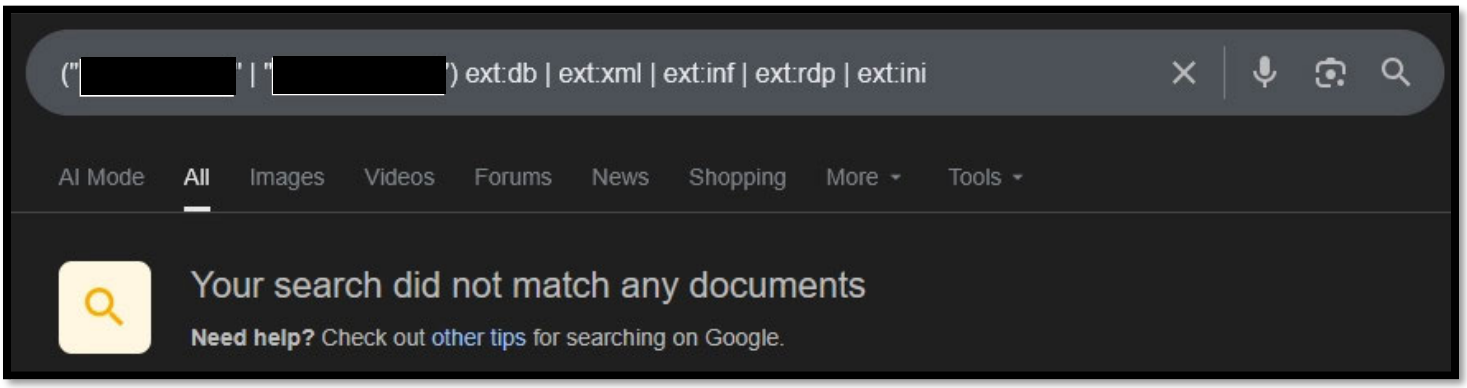
VirusTotal – no community flags for malicious activity were identified (1 of 2)



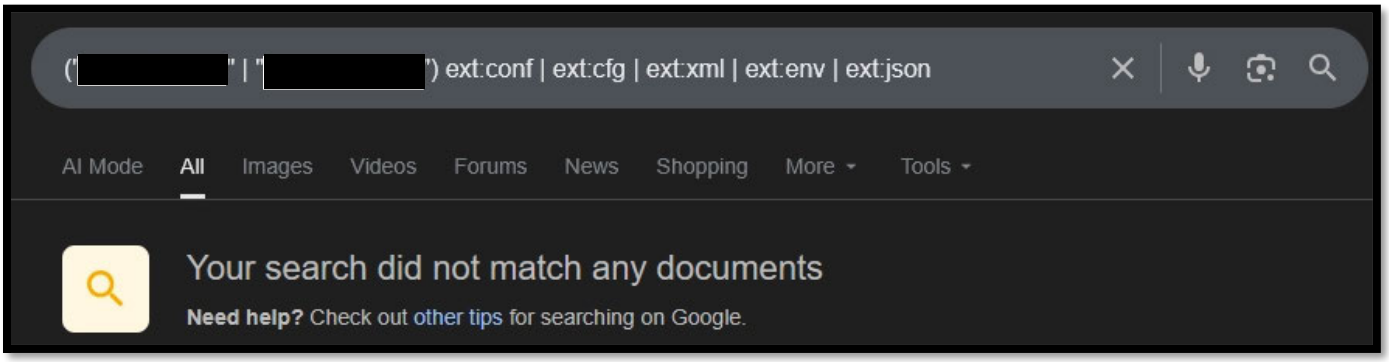
VirusTotal – no community flags for malicious activity were identified (2 of 2)



AlienVault OTX – no pulse alerts were identified for the domain



Google – no sensitive files were identified (1 of 2)

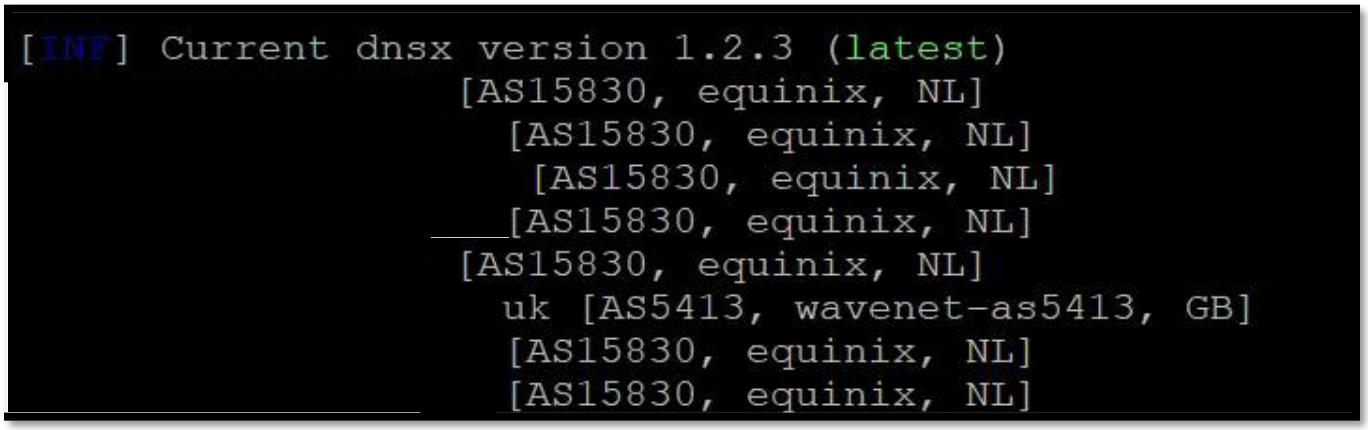


Google – no sensitive files were identified (2 of 2)

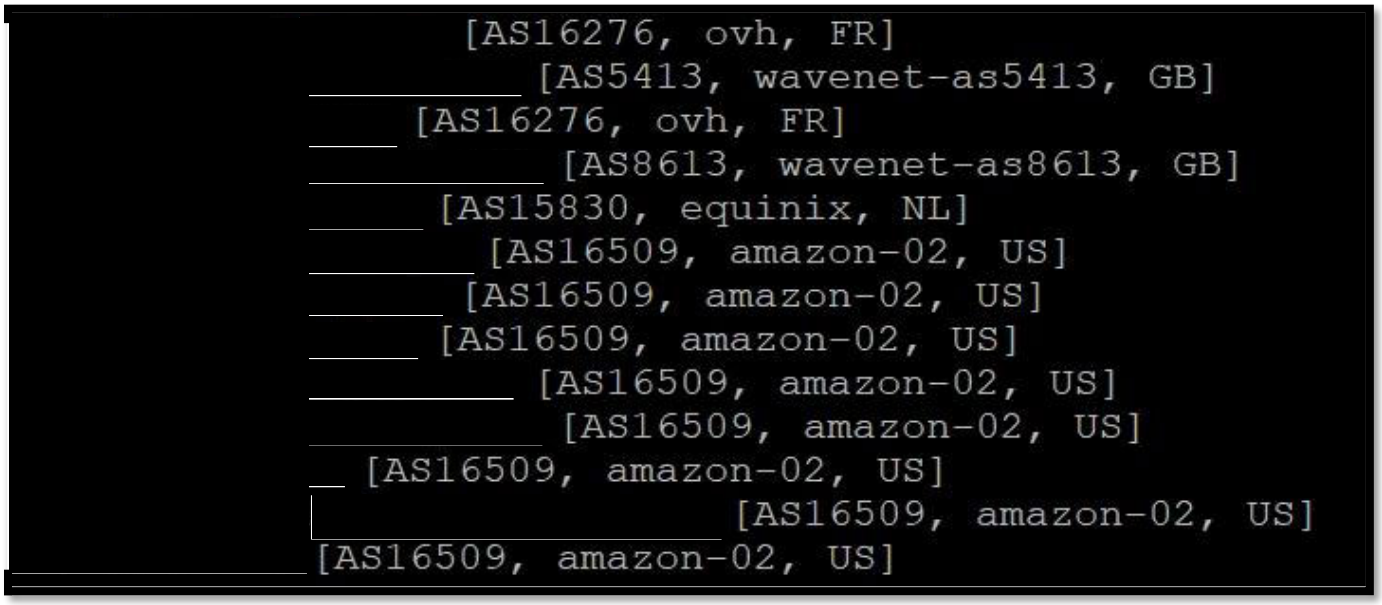
Abacus attempted to identify any previously breached credentials through large aggregated, publicly accessible databases. Threat actors target previously breached credentials because they're easy to obtain and often still valid due to password reuse. When users recycle passwords across accounts, attackers can leverage old breaches to gain initial access through credential stuffing or brute-force attempts. This makes reused credentials a persistent and dangerous entry point. Fortunately, Abacus did not identify any previously breached credentials with the [redacted] domains. That said, it is very possible that [redacted] personnel are using personal credentials for work-related purposes. [redacted] should be reminded that this is equally dangerous and that threat actors may also target individuals based on personal accounts and usernames.

ProxyNova – no breached password results were returned

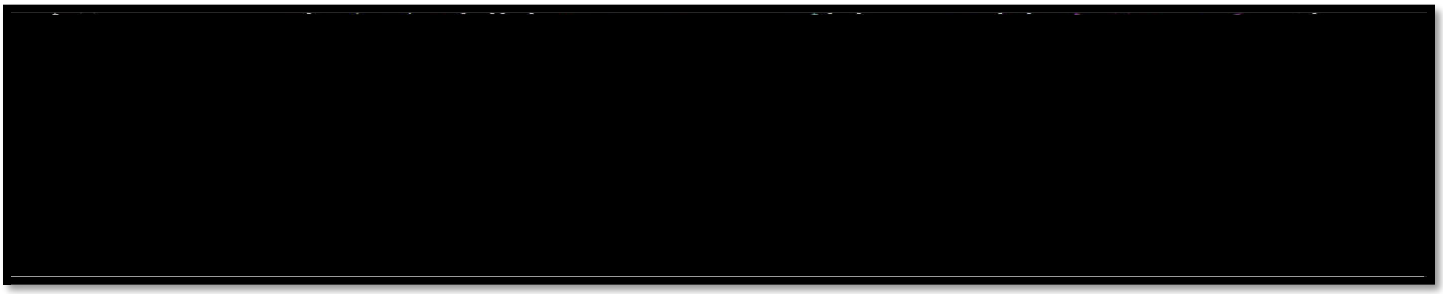
With a comprehensive list of domains, Abacus performed HTTP probing to identify the domains that responded to HTTP and HTTPS requests for valid web servers. Abacus additionally identified and reviewed content delivery networks (CDNs) and hosting infrastructure to obtain a more complete understanding of the web application attack surface.



dnsx – identified ASN, CDN, and location information for the domains (1 of 2)

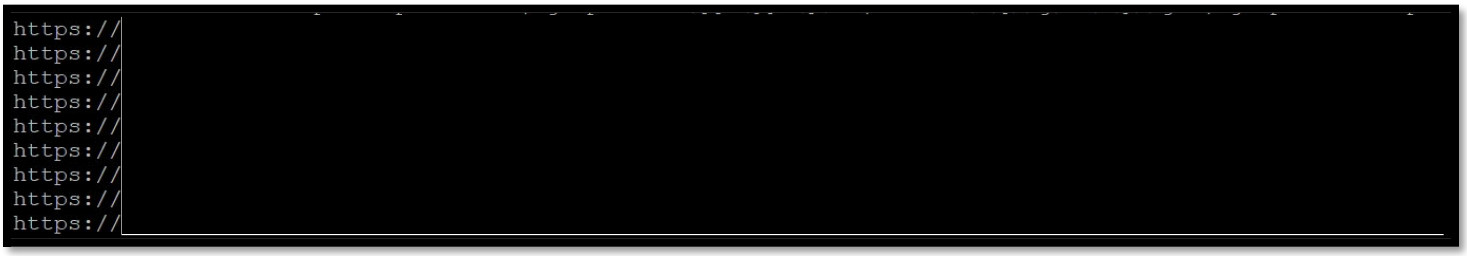


dnsx – identified ASN, CDN, and location information for the domains (2 of 2)



httpx – identified responding web servers on common ports and identified underlying web technologies and CDNs (1 of 2)

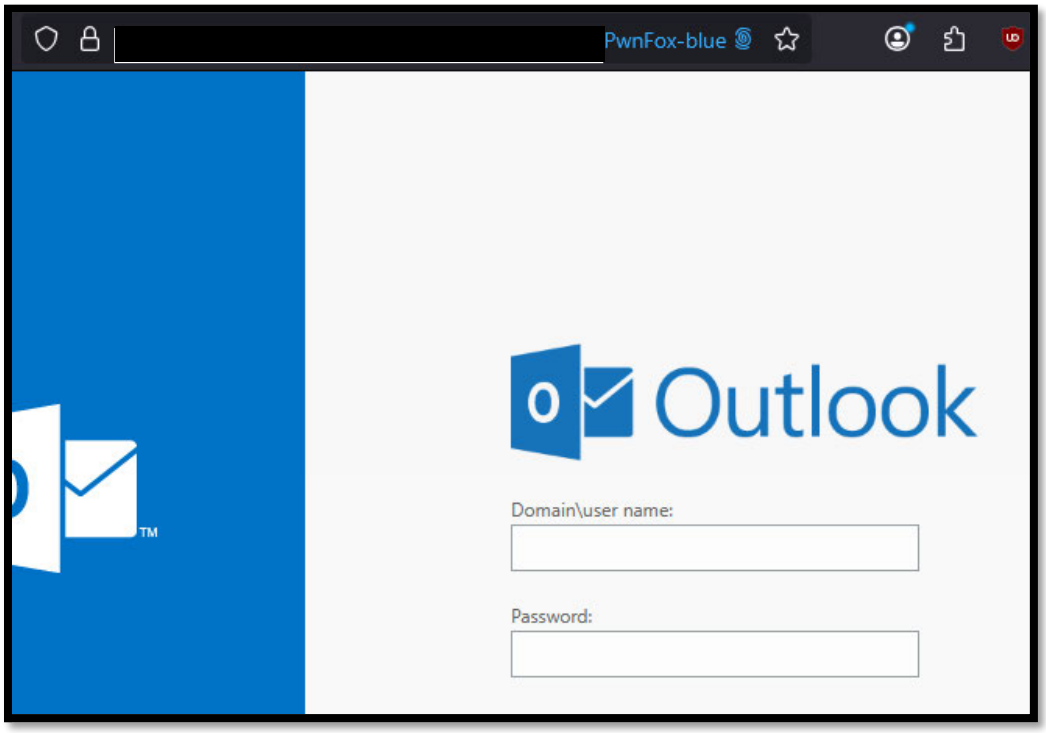
httpx – identified responding web servers on common ports and identified underlying web technologies and CDNs (2 of 2)



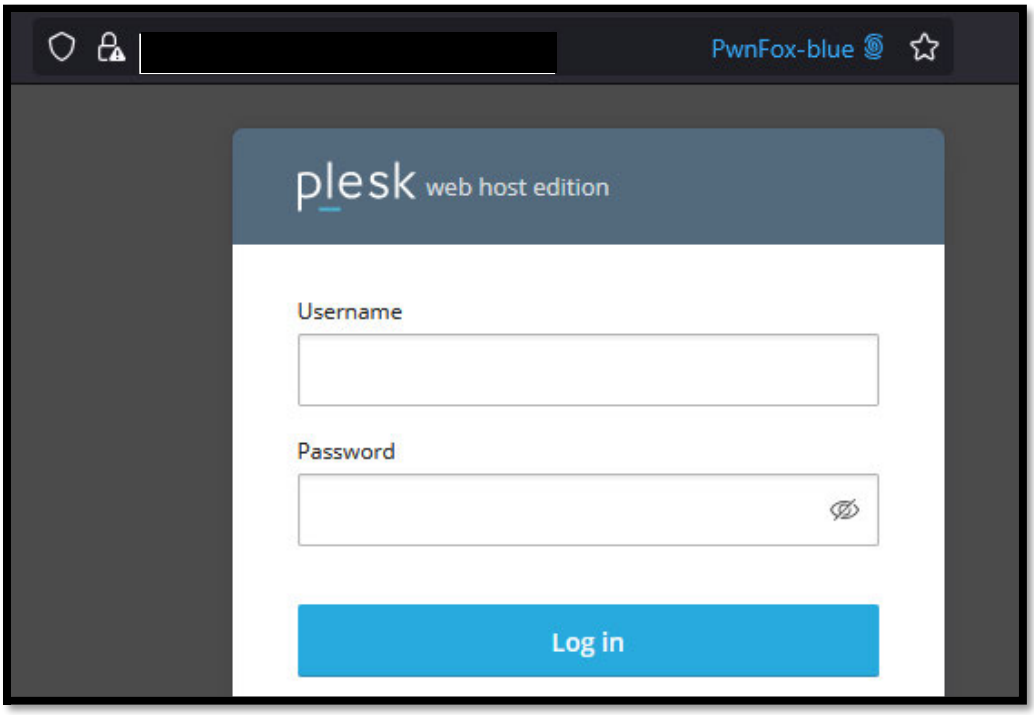
httpx – identified eight unique and alive web servers

Analysis was performed on the enumerated web applications to identify insecure TLS/SSL implementations, misconfigured HTTP headers, information disclosures, exposed credentials, vulnerable web technologies, and other web application misconfigurations that could enable initial access beyond the external perimeter.

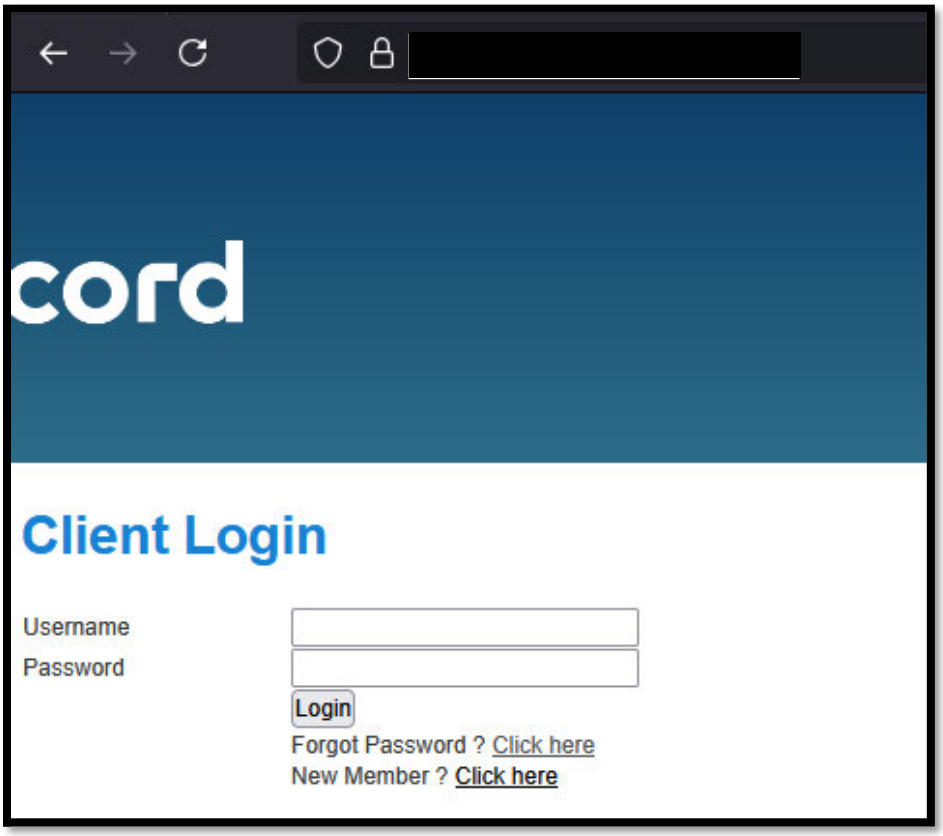
Abacus identified several login pages that may be targeted by a malicious actor to gain unauthorized access to relevant systems. Although multiple login portals were identified, Abacus did not attempt credential stuffing, password spraying, or other brute-force attacks to gain unauthorized access to these systems. It was also noted that some of the web applications redirected to a Microsoft login page for authentication.



Browser – identified an exposed Outlook web login page

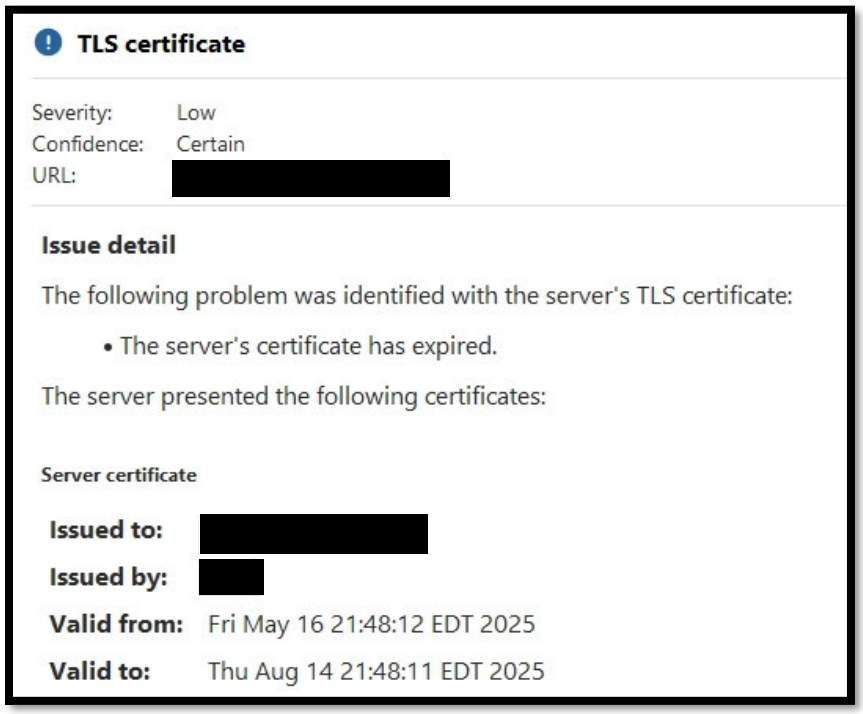


Browser – identified an exposed Plesk management login portal

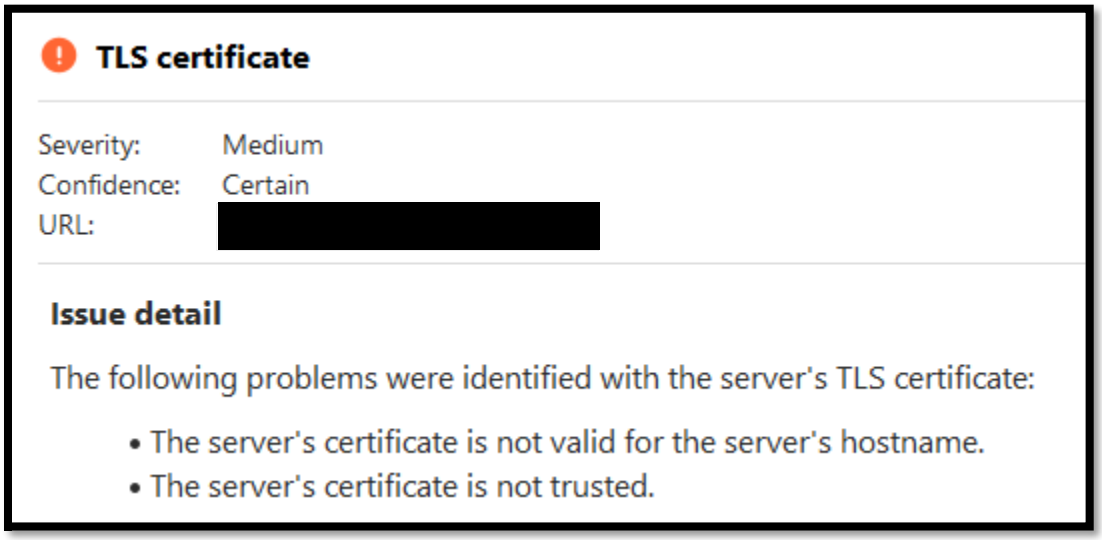


Browser – identified a client login portal

The in-scope web applications were checked for issues with TLS/SSL ciphers and certificates, which identified both expired and self-signed certificates in use. Expired and self-signed certificates result in browser security warnings for users and can be abused by a malicious actor using social engineering and adversary-in-the-middle attacks. Analysis of the TLS/SSL cipher suites in use also identified insecure cipher suites being negotiated, which could also allow a malicious actor to decrypt session traffic to the web applications.



Burp Suite – an alert was generated for an expired certificate



Burp Suite – an alert was generated for an untrusted and self-signed certificate

```
TLS 1.2 Cipher Suites:
  Attempted to connect using 156 cipher suites.

  The server accepted the following 10 cipher suites:
     TLS_RSA_WITH_AES_256_GCM_SHA384                  256
     TLS_RSA_WITH_AES_256_CBC_SHA256                  256
     TLS_RSA_WITH_AES_128_GCM_SHA256                  128
     TLS_RSA_WITH_AES_128_CBC_SHA256                  128
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            128       ECDH: prime256v1 (256 bits)
     TLS_DHE_RSA_WITH_AES_256_GCM_SHA384              256       DH (2048 bits)
     TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256       DH (2048 bits)
     TLS_DHE_RSA_WITH_AES_128_GCM_SHA256              128       DH (2048 bits)
     TLS_DHE_RSA_WITH_AES_128_CBC_SHA                 128       DH (2048 bits)
```

sslyze – identified insecure CBC cipher suites and cipher suites without ECDH on the "clients" subdomain

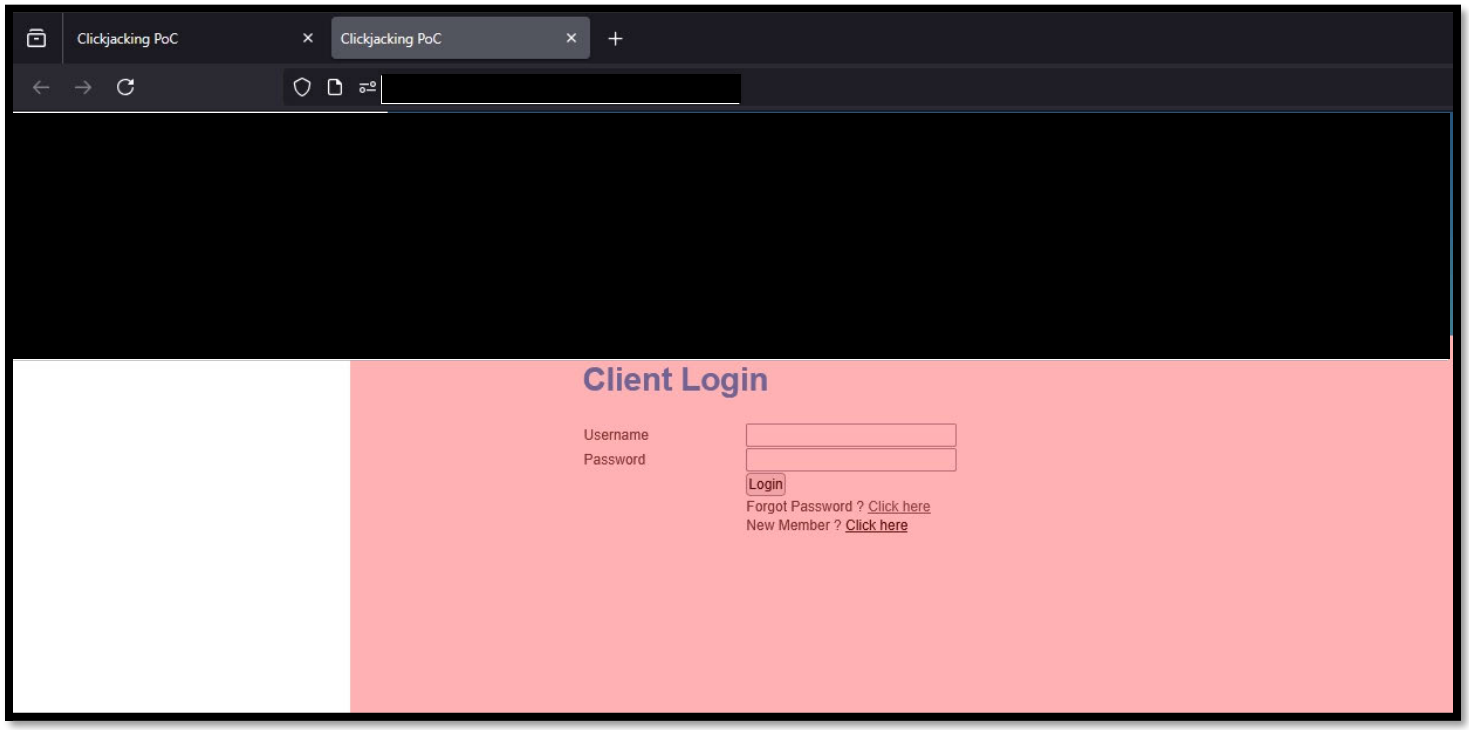
```
TLS 1.2 Cipher Suites:
  Attempted to connect using 156 cipher suites.

  The server accepted the following 12 cipher suites:
     TLS_RSA_WITH_AES_256_GCM_SHA384                  256
     TLS_RSA_WITH_AES_256_CBC_SHA256                  256
     TLS_RSA_WITH_AES_128_GCM_SHA256                  128
     TLS_RSA_WITH_AES_128_CBC_SHA256                  128
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384          256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384          256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256          128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256          128       ECDH: prime256v1 (256 bits)
```

sslyze – identified insecure CBC cipher suites and cipher suites without ECDH on the "helpdesk" subdomain

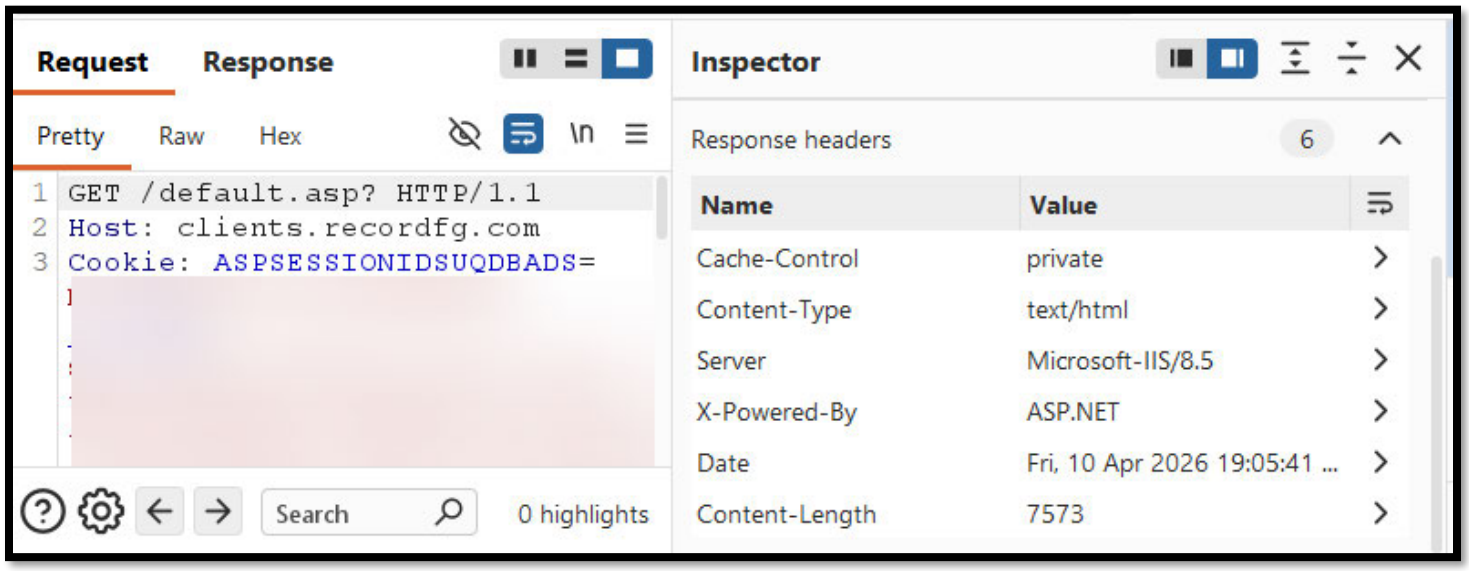
Abacus reviewed the security headers set by the web applications to determine if there were misconfigurations with HTTP "Stric-Transport-Security" (HSTS) or "Content-Security-Policy" (CSP) headers. The HSTS header specifies a period of time that the user agent, such as a web browser, should access the server only in a secure fashion over HTTPS. The CSP header provides an explicit policy specifying acceptable origins from which various site components can be loaded from and helps to mitigate attacks such as cross-site scripting (XSS) and clickjacking. Abacus found that some of the domains did not implement the HSTS header, which could allow a malicious actor to force unsecure connections to the web applications. Additionally, the CSP header was missing on some of the domains, which also allowed Abacus to demonstrate a double clickjacking proof-of-concept against the client login page. A malicious actor could exploit either of these issues to steal user credentials by utilizing social engineering attacks, which were out of scope for this engagement.

Burp Suite – alerts were generated for missing HSTS policies

Browser – the main domain was embedded within an invisible frame (iframe) with a clickjacking overlay (1 of 2)

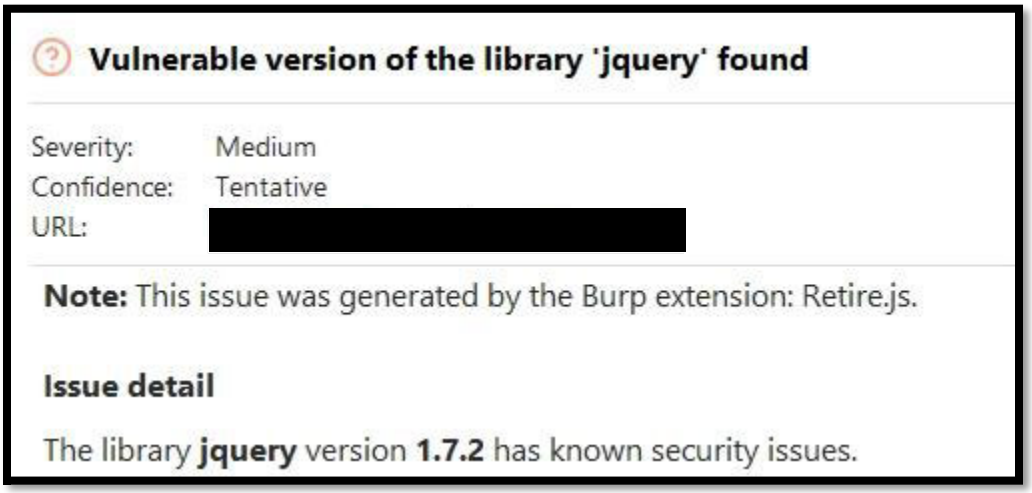


Browser – the overlay opened a new tab while embedding the client login page within an invisible frame (iframe) with another clickjacking overlay (2 of 2)



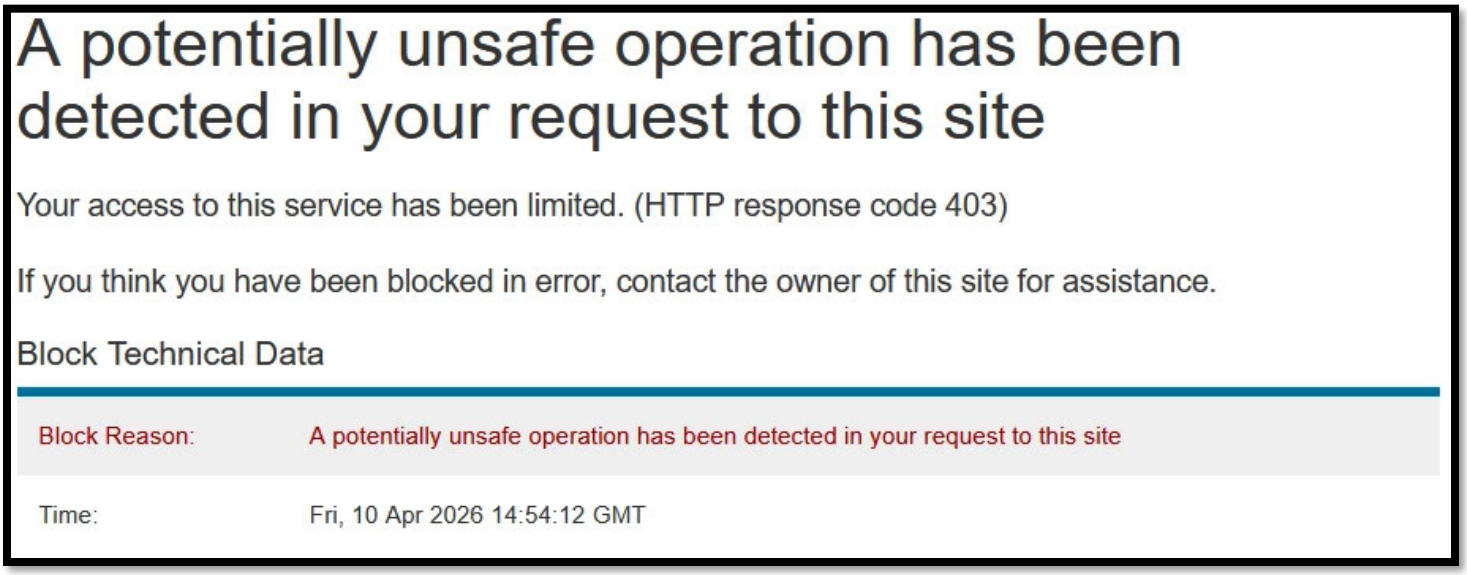
Burp Suite – server response headers did not include a CSP or HSTS policy

Vulnerable and outdated web technologies can allow exploits to grant unauthorized access to the application or underlying hosting infrastructure, such as authentication bypass or remote code execution. Abacus utilized browser-based extensions and Burp Suite scanners to review source files and responses for technology versions in use. An outdated and reportedly vulnerable version of jQuery was found in use by two applications; however no initial access or exploitation was achieved. Additionally, WordPress was also identified and utilized reportedly vulnerable plugins that were not likely to be exploited. Utilizing outdated and vulnerable technologies increases the attack surface of the web applications.



Burp Suite – an alert was generated for an outdated and vulnerable version of jQuery

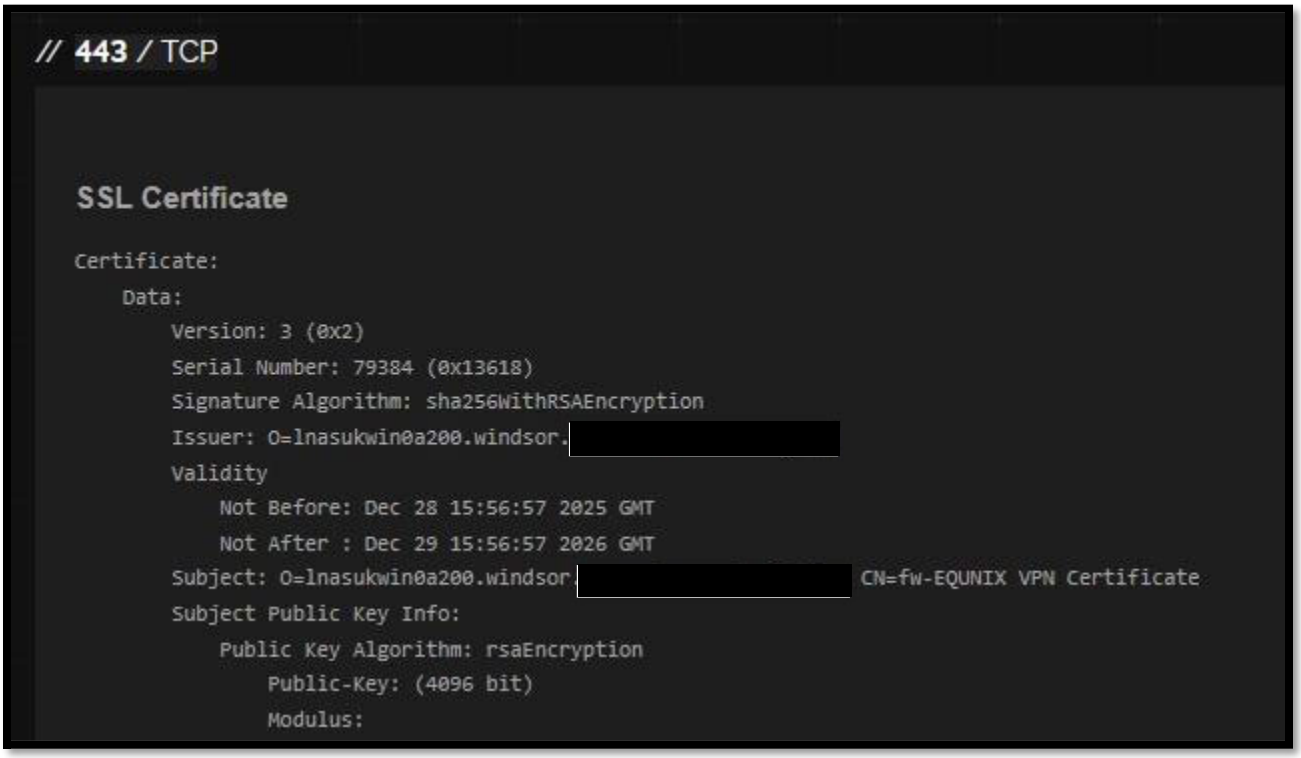
Burp Suite (WPScan) – identified plugin versions reportedly vulnerable to issues that were not exploitable



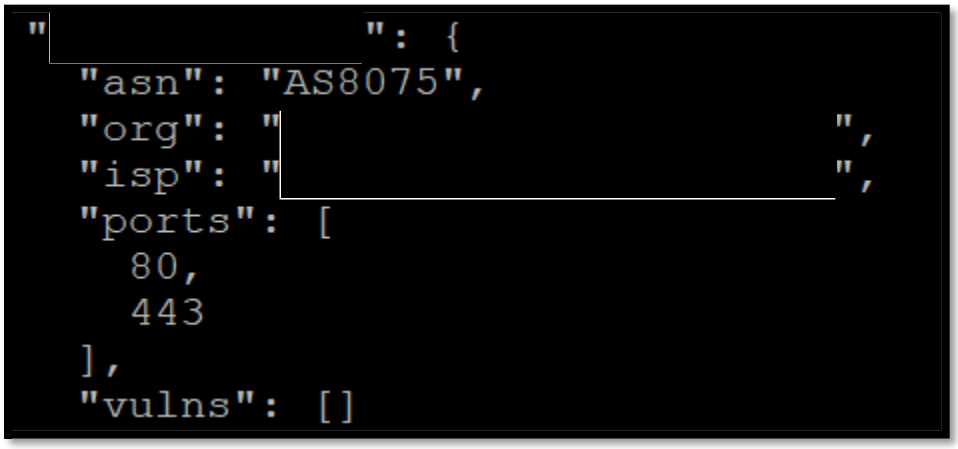
Browser – the Wordfence plugin successfully blocked an attempted XSS

Abacus then analyzed the in-scope IP addresses, network blocks, and other infrastructure for vulnerabilities and entry points into [redacted] network. Utilizing the list of enumerated subdomains and IP addresses, Abacus used a custom script to retrieve open-source data from Shodan. Shodan is a specialized search engine designed to discover, index, and provide detailed information about internet-connected devices and systems. This information was used to identify and validate the in-scope networks for scanning exposed ports, services, and potential vulnerabilities. These Shodan scans identified the use of a Checkpoint firewall and Global Protect VPN. Additionally, other infrastructure was identified utilizing Simple Network Management Protocol (SNMP) on internet-exposed devices. However, SNMP was configured to use version 3 and was not found to be insecure.

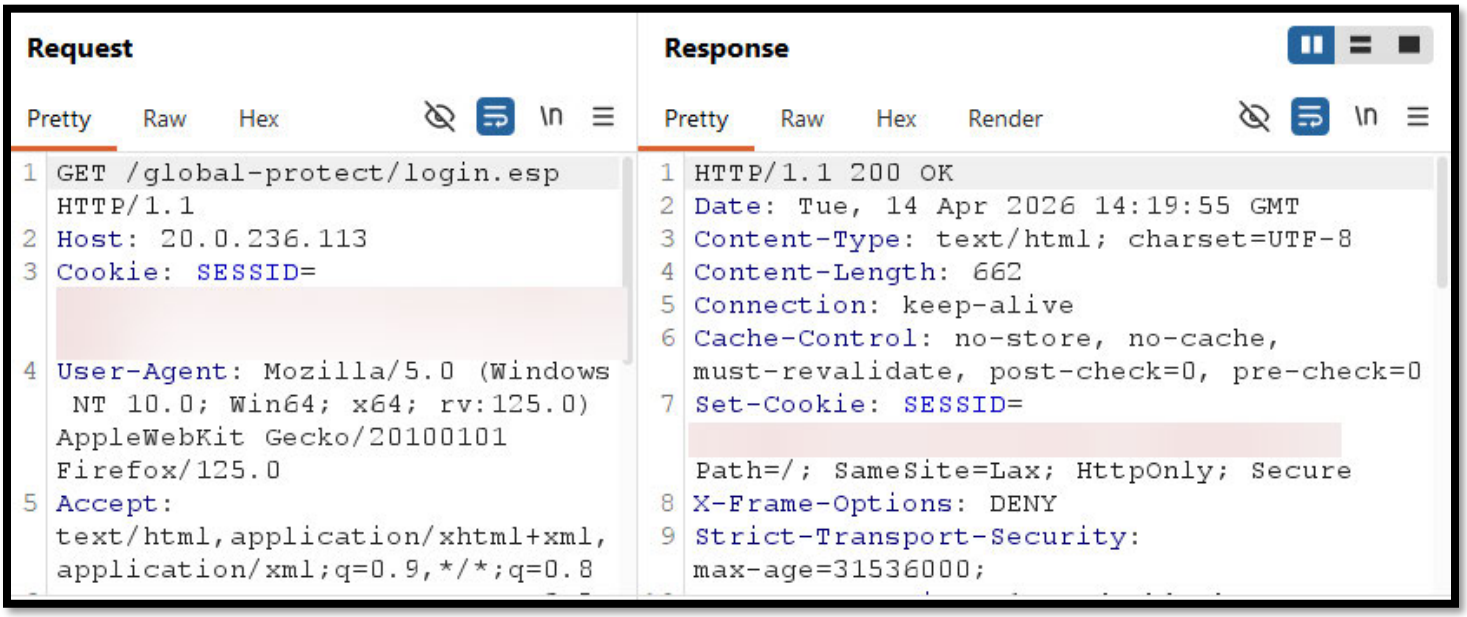
Shodan – identified a Checkpoint firewall host (1 of 2)



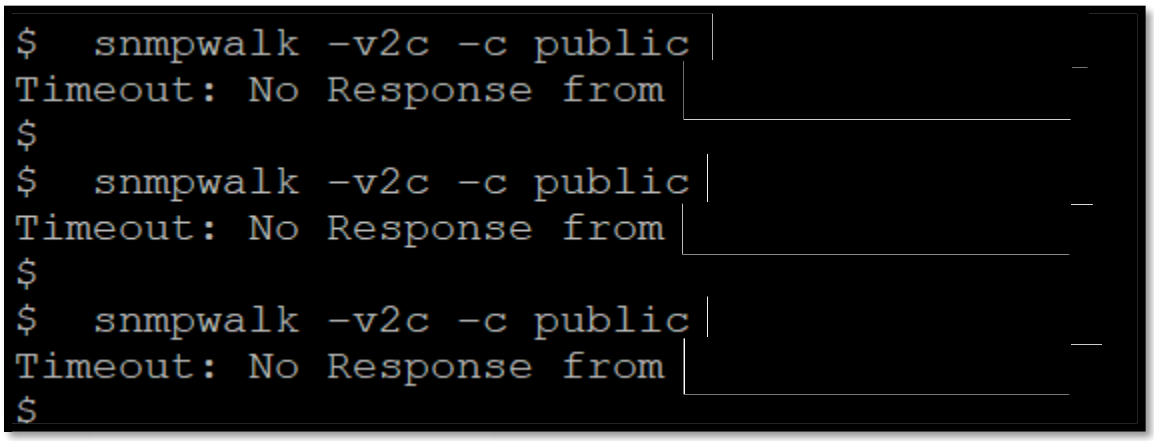
Shodan – identified a Checkpoint firewall host (2 of 2)



Shodan – identified a Global Protect VPN



Burp Suite – identified a Global Protect VPN endpoint that redirected to Microsoft login

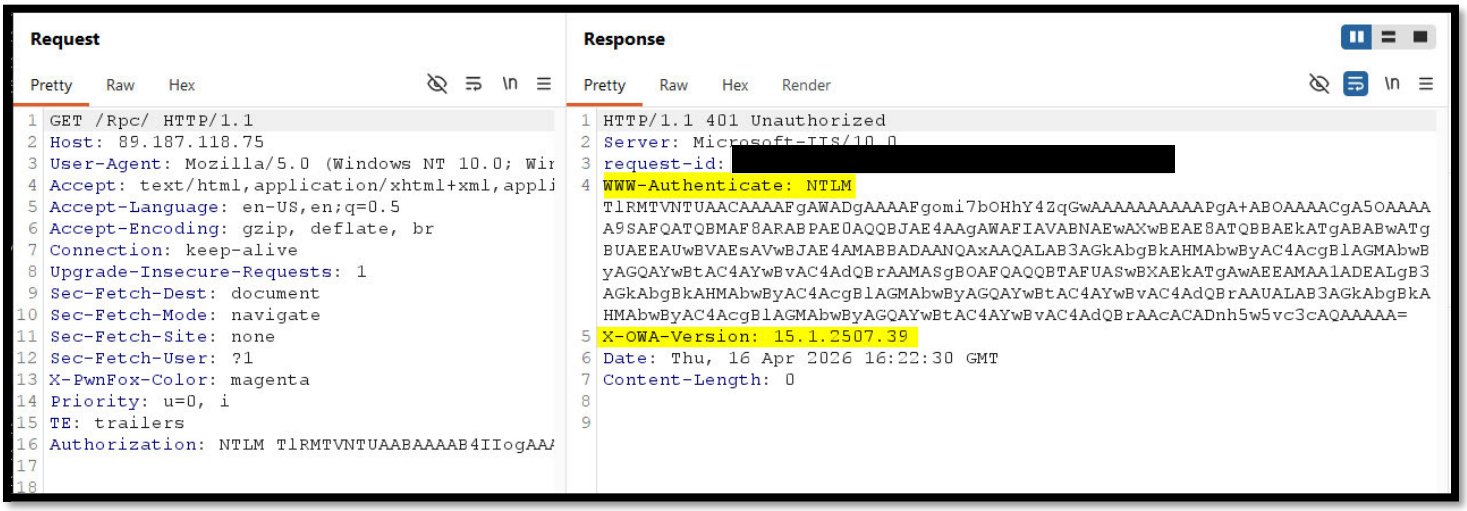


Shodan – SNMP version 2 was not configured for the Cisco devices

```
$  snmpwalk -v3 -n -u testinguser -l noAuthNoPriv 57.133.137.162
snmpwalk: Unknown host (testinguser) (Resource temporarily unavailable)
$
$  snmpwalk -v3 -u admin -A admin 57.133.137.163
Error: passphrase chosen is below the length requirements of the USM (min=8).
snmpwalk:  (The supplied password length is too short.)
Error generating a key (Ku) from the supplied authentication pass phrase.
$
$  snmpwalk -v3 -u administrator -A administrator 57.133.137.163
snmpwalk: Unknown user name
$
```

snmpwalk – no misconfigurations or weak credentials provided access to the device information

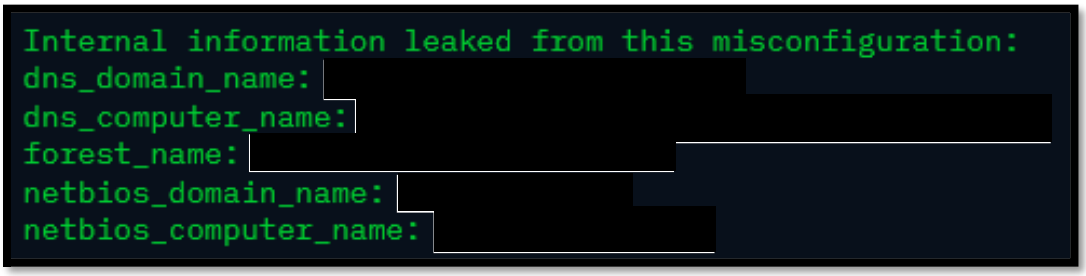
The Microsoft Exchange server identified previously was found to utilize a version that is end of support and potentially vulnerable to CVE-2025-64666 and CVE-2025-64667, which are privilege escalation and email spoofing vulnerabilities respectively. Abacus was unable to exploit either vulnerability to gain unauthorized access to the Exchange server. Additionally, the server exposed NTLM authentication to the internet which can be used to bypass multi-factor authentication (MFA) during brute-force login attempts and also reveal internal domain and computer names.



Burp Suite – identified NTLM authentication enabled and an end of support OWA version in use

```
[INF] Current httpx version v1.8.1 (outdated)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
https://[redacted]/Autodiscover/Autodiscover.xml [401]
https://[redacted]/Autodiscover/AutodiscoverService.svc/root [401]
https://[redacted]/Autodiscover [401]
https://[redacted]/EWS/ [401]
https://[redacted]/OAB/ [401]
https://[redacted]/PowerShell/ [401]
https://[redacted]/[redacted]/ [401]
$
```

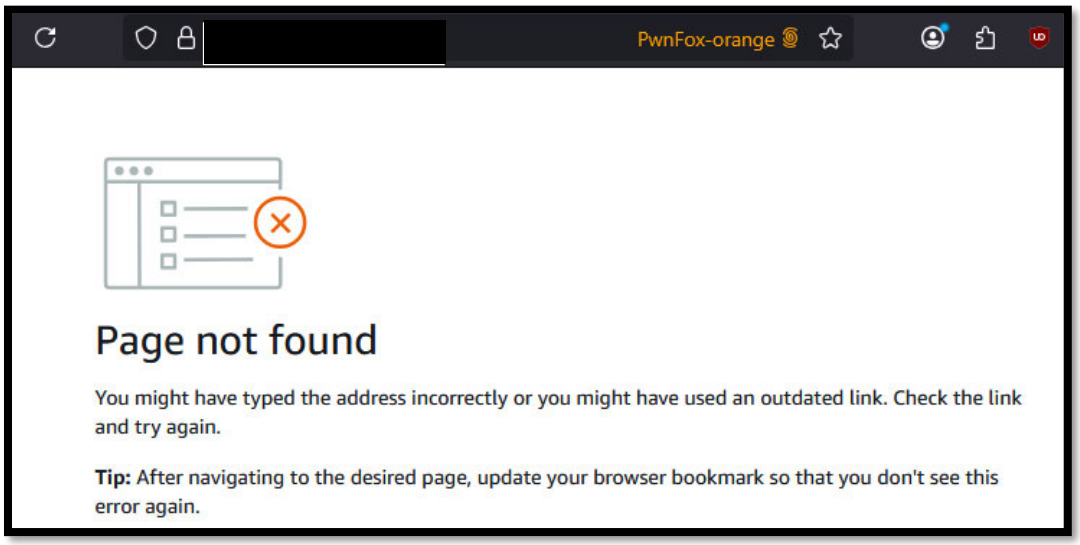
ntlmrecon & httpx – identified endpoints that accepted NTLM authentication on the host



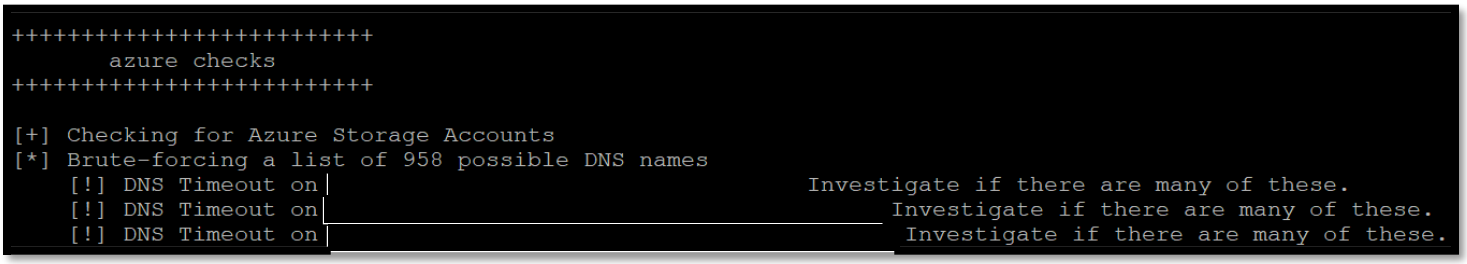
NodeZero – identified internal DNS information due to NTLM authentication

Abacus leveraged public search engines, and custom OSINT tooling to determine if [redacted] had any unintentionally exposed cloud resources. This process involved systematically enumerating common Azure Website DNS, storage accounts such as Amazon S3 buckets and Azure Blobs, databases, virtual machines, and more using keywords and common wordlists. No sensitive cloud assets were discovered or accessible while unauthenticated.

cloud_enum – identified an AWS application that was not accessible (1 of 2)



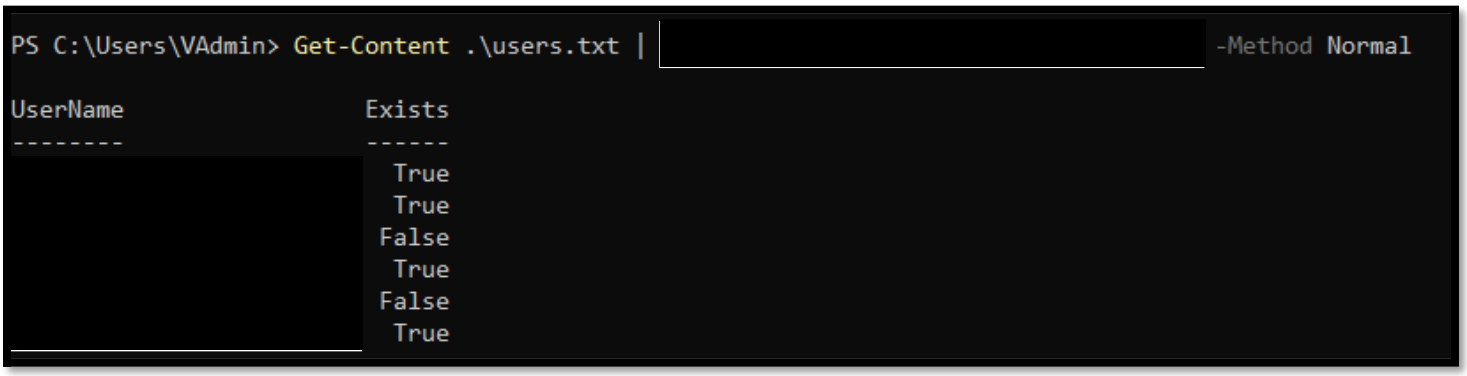
Browser – identified an AWS application that was not accessible (2 of 2)



cloud_enum – no Azure resources were identified or accessible

Having confirmed the domain being utilized, Abacus leveraged an open-source tool called AADInternals to enumerate details related to the Azure tenant, including associated domains, tenant id and region, and the use of DesktopSSO. DesktopSSO, also called Seamless SSO enables users to be automatically signed into the corporate network when using their corporate devices. While neither Abacus nor Microsoft considers this to be a vulnerability, it may allow a malicious actor to enumerate valid user email accounts to target for social engineering, brute-force, credential stuffing, or password spraying attacks.

AADInternals – identified the tenant ID and DesktopSSO



AADInternals – user enumeration was possible due to DesktopSSO enabled

Having exhausted all viable in-scope attack vectors, Abacus completed the external network penetration testing activities. Four moderate-risks, four low-risks, and one information severity risk findings were identified. No access was achieved beyond the external perimeter using purely technical means.

Internal Network Penetration Testing Narrative

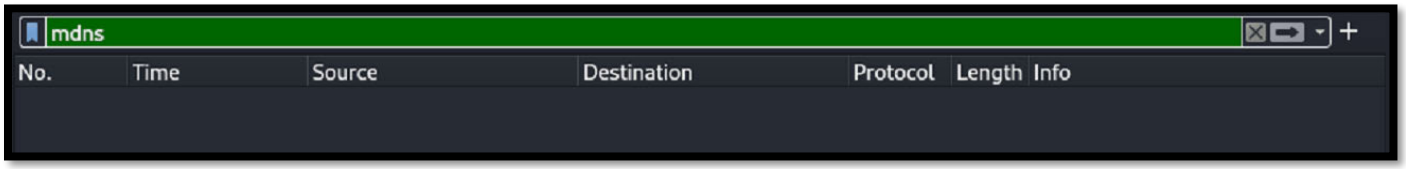
Abacus's role was to replicate the vantage point of a malicious actor who had breached [redacted] 's external perimeter and gained access to their internal network. To achieve this, a physical penetration testing device was remotely deployed on the standard user workstation virtual local area network (VLAN) within [redacted] 's office. This device Kali Linux device [redacted] allowed Abacus engineers to replicate the scenario that a malicious actor had compromised a standard user workstation. [redacted] provided the following scope and context prior to the engagement.

Initial reconnaissance was performed to determine network settings and route details on the internal network penetration testing appliance.

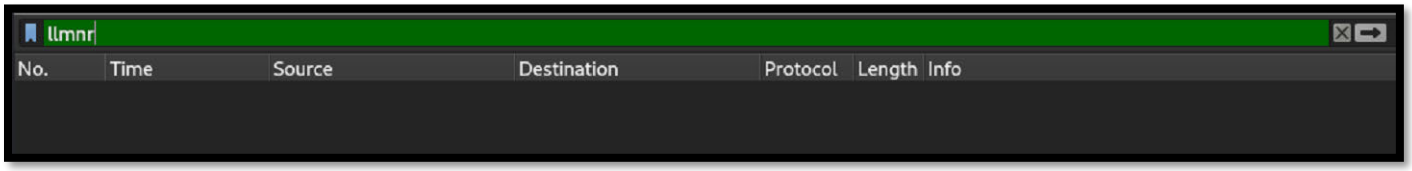
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::df39:b649:6e5:4e11  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:af:5a:65  txqueuelen 1000  (Ethernet)
        RX packets 182783944  bytes 14490588598 (13.4 GiB)
        RX errors 0  dropped 9297  overruns 0  frame 0
        TX packets 7262709  bytes 4289700286 (3.9 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Confirming the IP address of a Kali Linux virtual machine also used for penetration testing

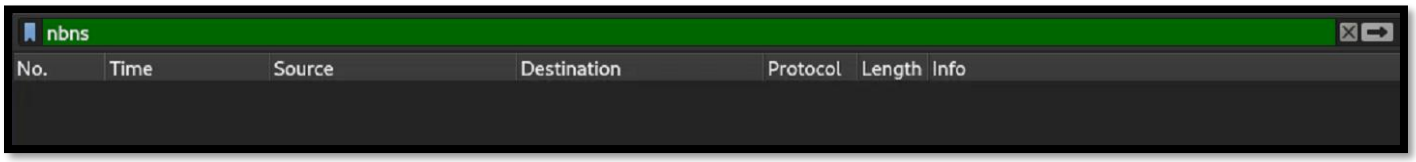
Passive reconnaissance was initiated by analyzing network traffic using tools such as Wireshark and Responder to understand the environment better. Captured traffic was filtered for services that could provide additional insight into the environment, such as CDP (Cisco Discovery Protocol), LLDP (Link-Layer Discovery Protocol), NBNS (NetBIOS), LLMNR (Link-Local Multicast Name Resolution), as well as assessing if the environment is dual-stack with the presence of IPv6 traffic.



Passive network analysis via Wireshark, identifying a lack of mDNS traffic



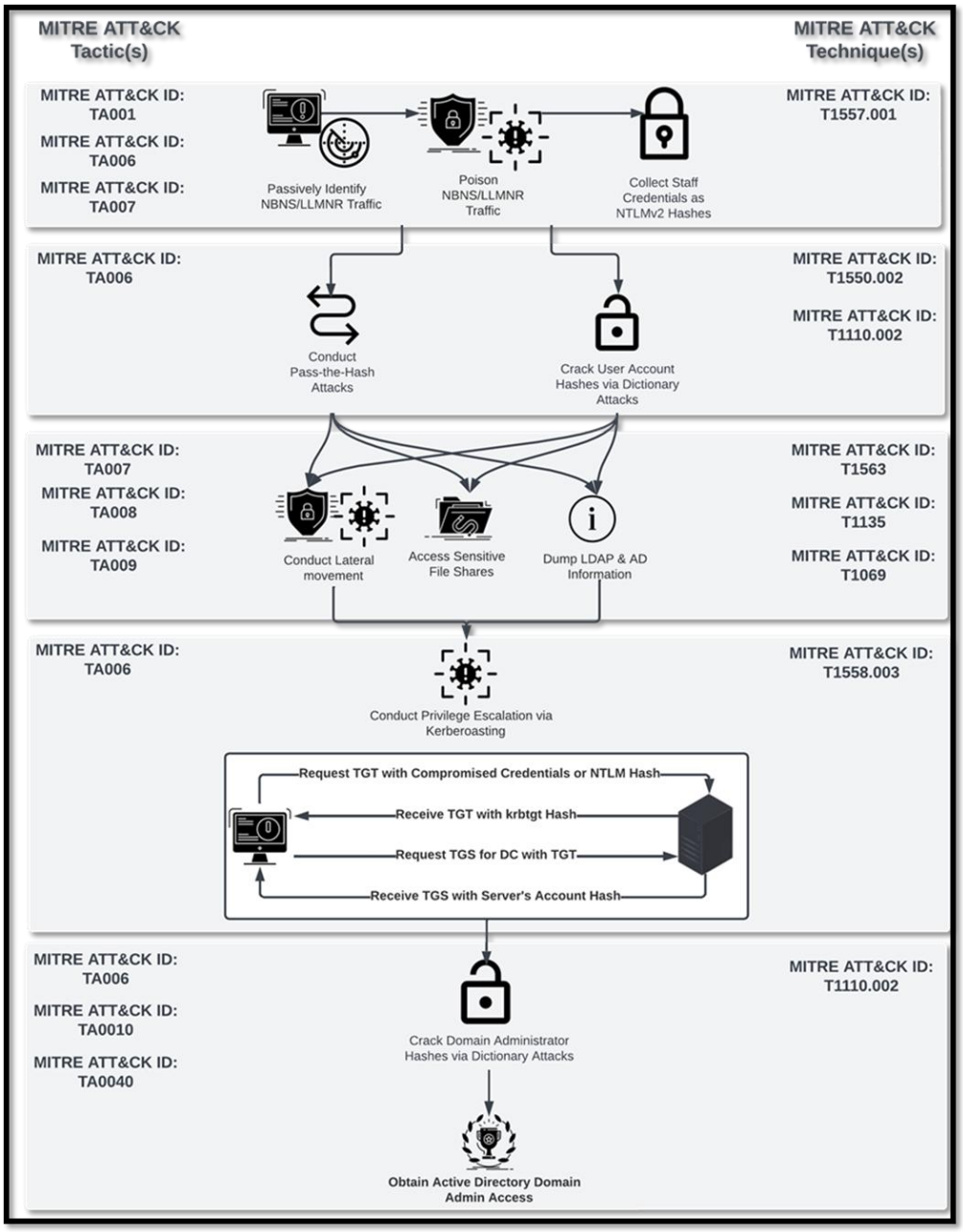
Passive network analysis via Wireshark, identifying a lack of LLMNR traffic



Passive network analysis via Wireshark, identifying a lack of NBNS traffic

In response to discovering either NBNS or LLMNR traffic, a malicious actor would often utilize a tool such as Responder to perform NetBIOS/LLMNR poisoning. First, Responder would listen to multicast NetBIOS/LLMNR queries, spoof a response under the right conditions, and direct the victim to the machine that Responder is running on. Should the victim machine then attempt to connect to the attacking machine, Responder exploits the connection and would steal NTLM hashes, which could then be cracked using other tools. This attack vector generally provides two potential paths for further system compromise. First, malicious actors can attempt to crack the captured hashes using large-scale dictionary attacks offline. Alternatively, malicious actors can choose to conduct a pass-the-hash attack, enabling the possibility of authentication on behalf of the victim without cracking the hashed password.

A malicious actor would utilize these aforementioned user credentials to conduct lateral movement to additional systems, enumerate additional information, explore network-attached file shares, and ultimately attempt to escalate privileges. One of the most common and reliable methods of active directory exploitation is known as Kerberoasting. During this type of attack, a compromised active directory account is used to query the domain controller to enumerate service principal names (SPNs), then use a valid Kerberos ticket-granting-ticket (TGT) to obtain a ticket-granting-service (TGS) associated with those SPNs. These recovered hashes would then be targeted in a dictionary-based attack or brute-forced to reveal the plain-text passwords and ultimately compromise the domain administrator, resulting in complete network compromise.



Demonstrating the potential attack vector leveraging NBNS/LLMNR poisoning

In order to validate if this would be possible within [redacted] environment, Abacus assessed if server message block (SMB) signing was being enforced across the environment. SMB signing is a protocol in which all SMB messages contain a signature generated by the advanced encryption standard (AES) algorithm, effectively defeating pass-the-hash attempts. This identified forty-seven endpoints with SMB signing enabled but not required; suggesting a high probability that the previously illustrated kill-chain could be realized within [redacted] environment given enough time.

```
Nmap scan report for [redacted]
Host is up (0.00051s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:50:56:AF:32:63 (VMware)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Identifying SMB signing enabled but not required on

Address resolution protocol (ARP) traffic was also analyzed to determine the potential viability of VLAN hopping to bypass any identified network segmentation controls.

arp

No.	Time	Source	Destination	Protocol	Length	Info
7	0.081391540	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
12	0.105397075	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
201	0.957269587	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
235	1.174020390	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
310	1.959308239	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
325	2.175212528	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
383	3.177430315	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell
439	4.180989105	CheckPointSo_82:0f:…	Broadcast	ARP	60	Who has [redacted] Tell

Analyzing ARP traffic via Wireshark

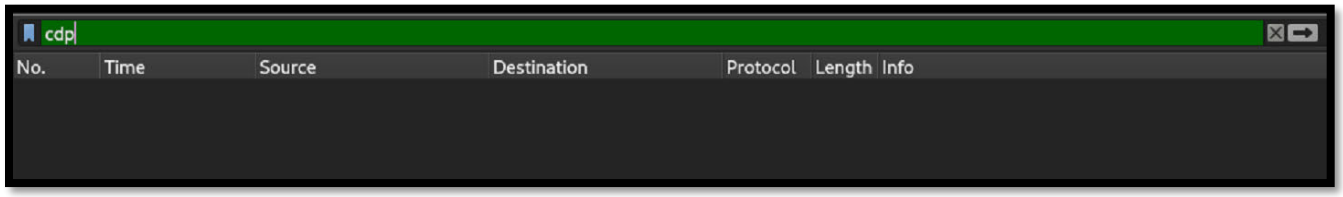
IPv6 traffic with a lack of first-hop security is a problematic networking vulnerability, as it introduces relatively easy attack vectors for malicious actors, such as leveraging IPv6 DNS takeover. However, assessing the presence of first-hop security controls would require access to network infrastructure, which Abacus did not obtain during this assessment. It would be prudent for the security team to assess, from a white-box perspective, the configuration of such implemented security controls to ensure protection from common IPv6-based attacks.

ipv6

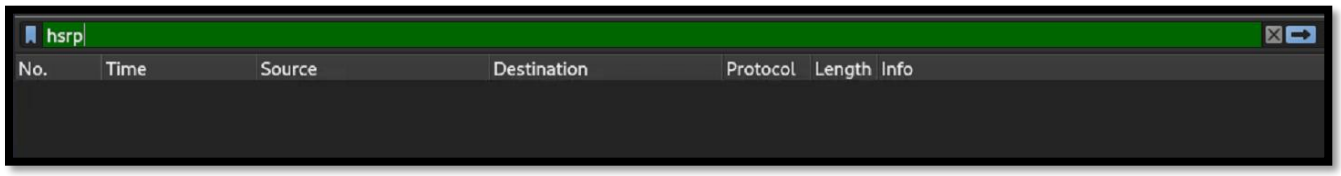
No.	Time	Source	Destination	Protocol	Length	Info

Analysis of IPv6 traffic via Wireshark indicated no traffic was found

Passive network analysis via Wireshark did not identify Cisco Discovery Protocol (CDP) nor Cisco Hot Standby Router Protocol (HSRPv2). The presence of these protocols is not indicative of a network vulnerability; however, it provided Abacus with the context that Cisco devices were not used within [redacted] network.

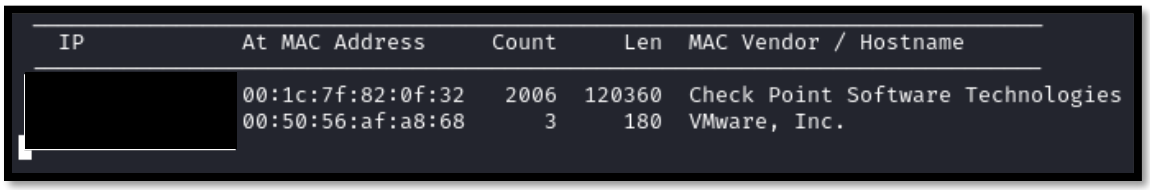


Passive network analysis via Wireshark identified CDP traffic



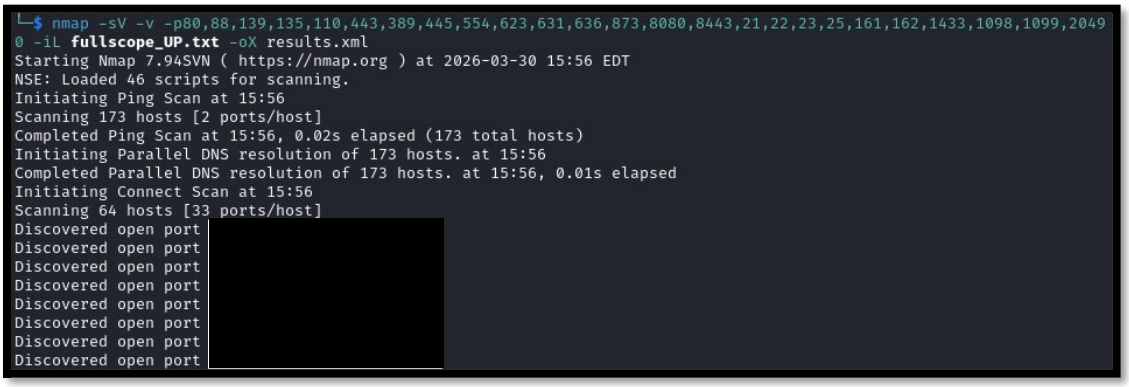
Passive network analysis via Wireshark identified HSRPv2 traffic

Next, Abacus systematically leveraged passive and active measures to map the internal attack surface. This reconnaissance began with a passive ARP scan of the local subnet to identify hosts for further analysis.

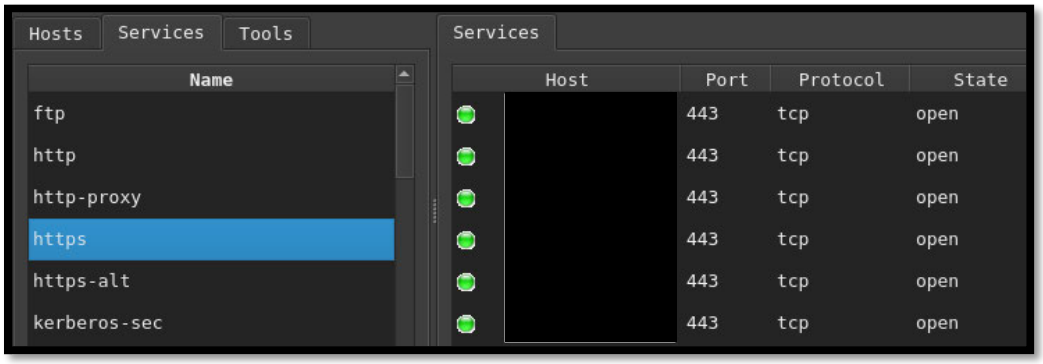


Passive ARP scanning via Netdiscover

Once an initial understanding of the local VLAN was obtained, Abacus leveraged a highly obfuscated Nmap scan to gather information across the scope of systems on open ports and services, operating systems, and version information. This scan provided Abacus engineers with a high-level view of the attack surface and allowed for the identification of systems and subnets to prioritize deeper analysis using tools such as Legion, Nikto, Metasploit auxiliary modules, OpenVAS, and more. Once combined with these additional tools, a comprehensive attack surface mapping was established.

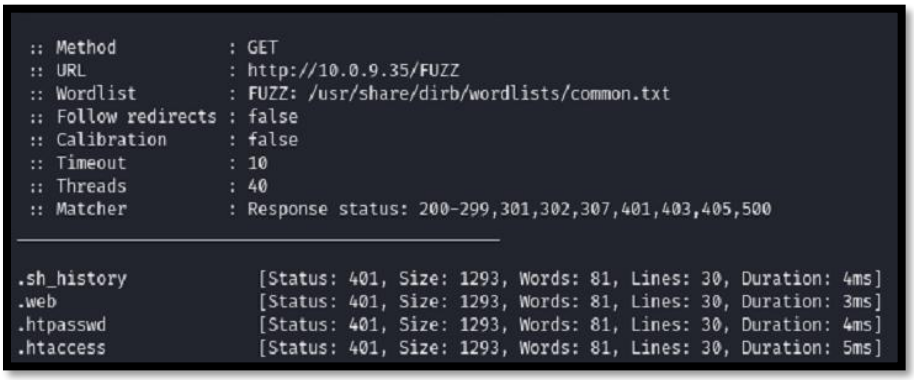


Target Attack surface enumeration of ports and services via Nmap

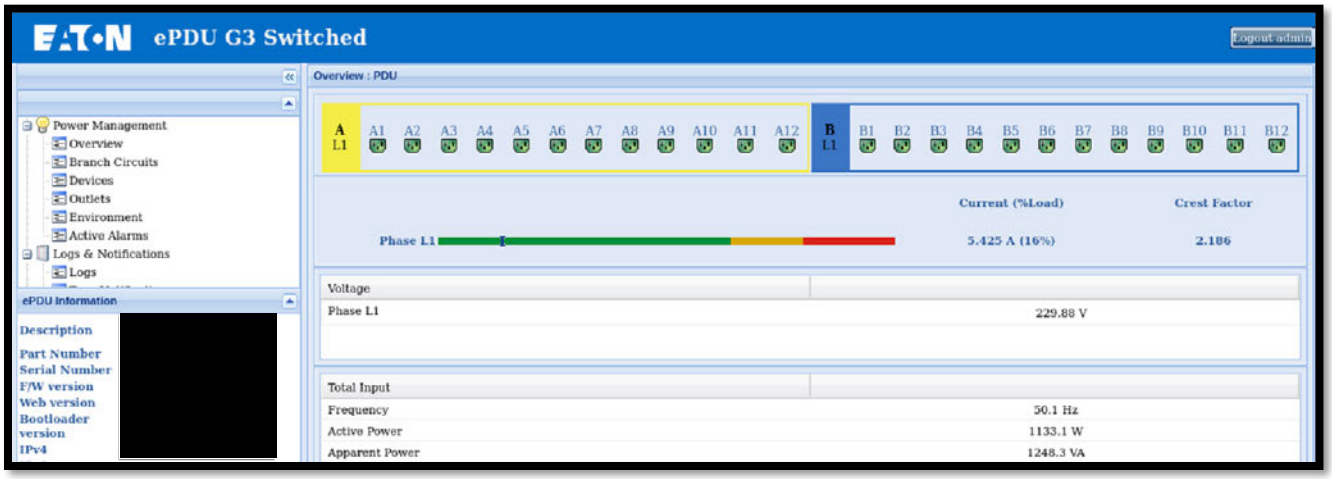


Attack surface analysis via Legion, an open-source and highly configurable pentesting framework developed by Abacus

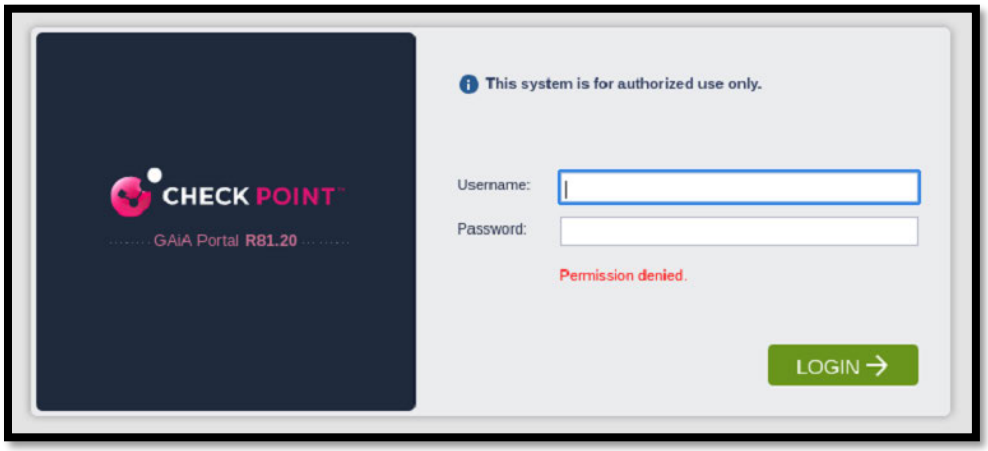
Abacus' ongoing penetration testing focused on protocols often vulnerable to exploitation, including directory busting, vendor default credentials on devices, and popular protocols such as Telnet, VNC, FTP, MSSQL, MYSQL, NFS, SNMP, and SSH. Following the enumeration of these services, an Eaton ePDU device was found to be utilizing vendor default credentials. Abacus was able to leverage the default admin account to access Eaton ePDU, which allows for exploitation of Denial-of-Service (DoS) attacks to critical network infrastructure.



Demonstrating failed directory busting using FFUF on 10.0.9.35

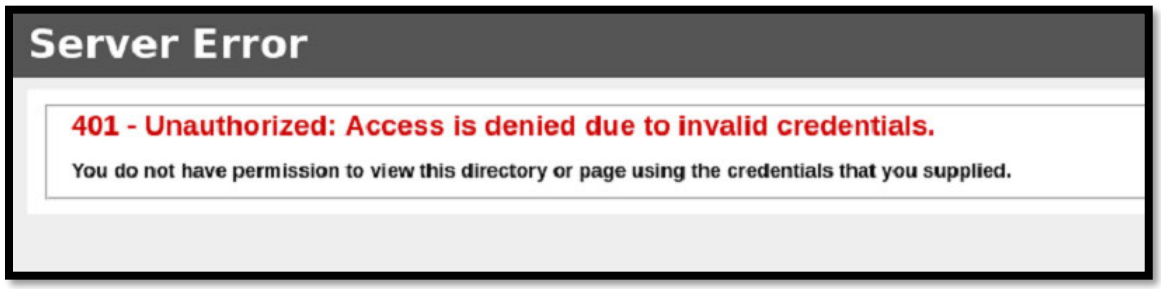


Demonstrating a successful login using default vendor credentials to an Eaton ePDU on host [redacted]
(Username: admin, Password: admin)

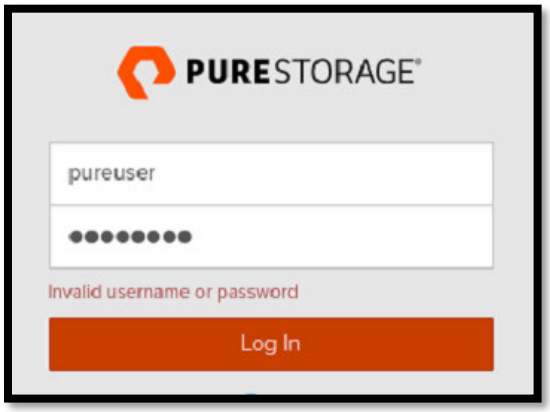


Demonstrating an unsuccessful login attempt to a Checkpoint firewall on [redacted]

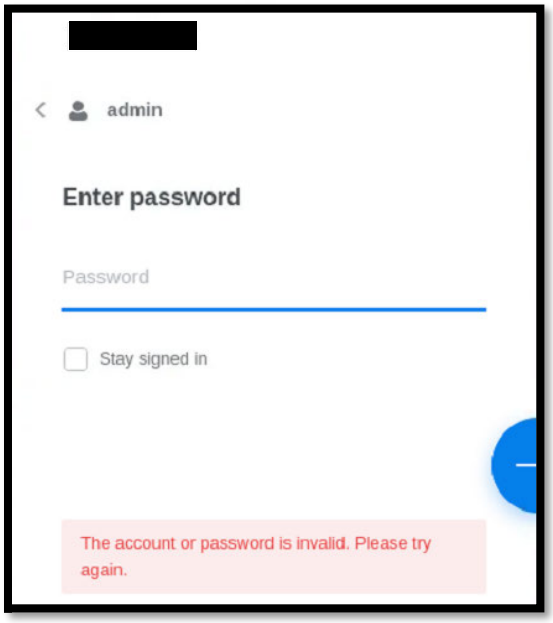
[redacted]



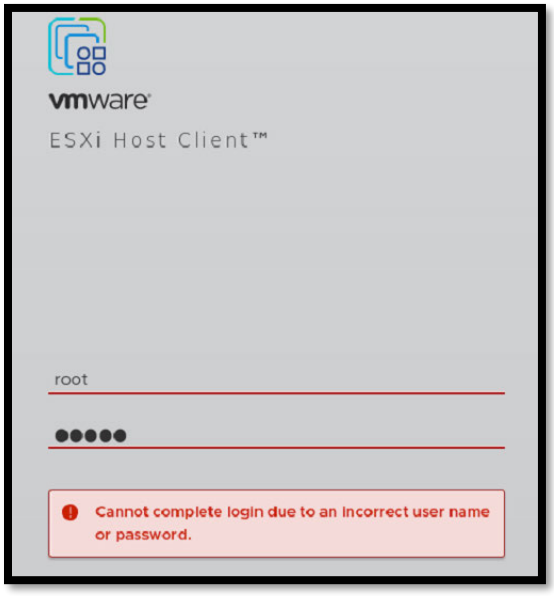
[redacted] *unsuccessful login attempt to an IoT device on* [redacted]



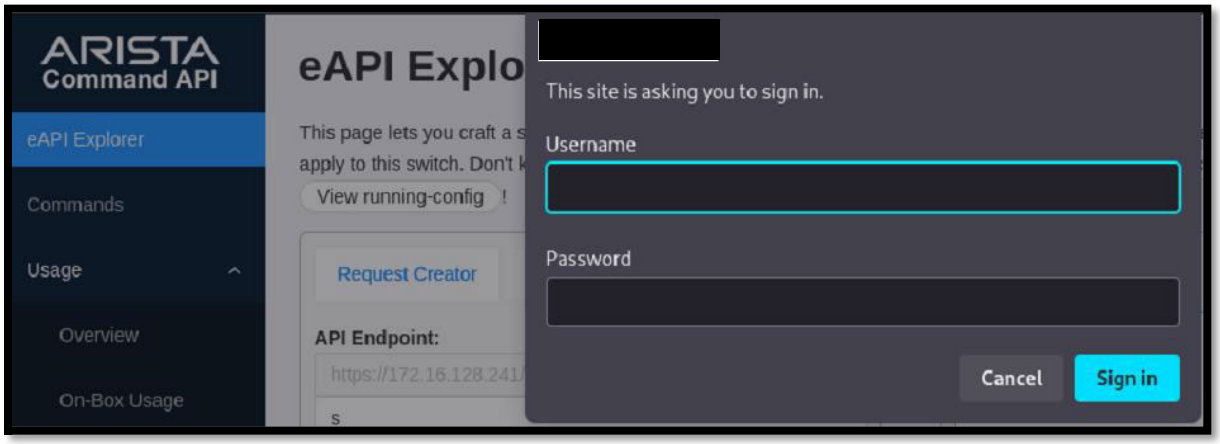
Demonstrating an unsuccessful login attempt to Pure Storage on [redacted]



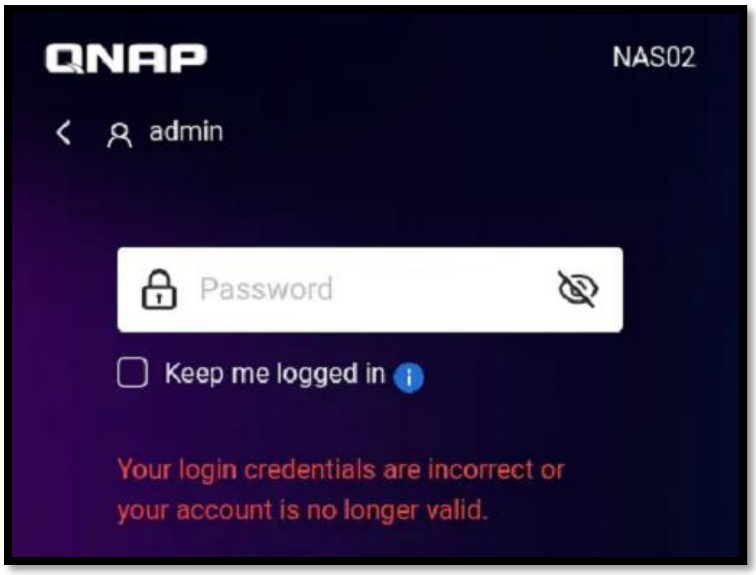
[redacted]



[redacted] *unsuccessful login attempt to VMware ESXi on* [redacted]

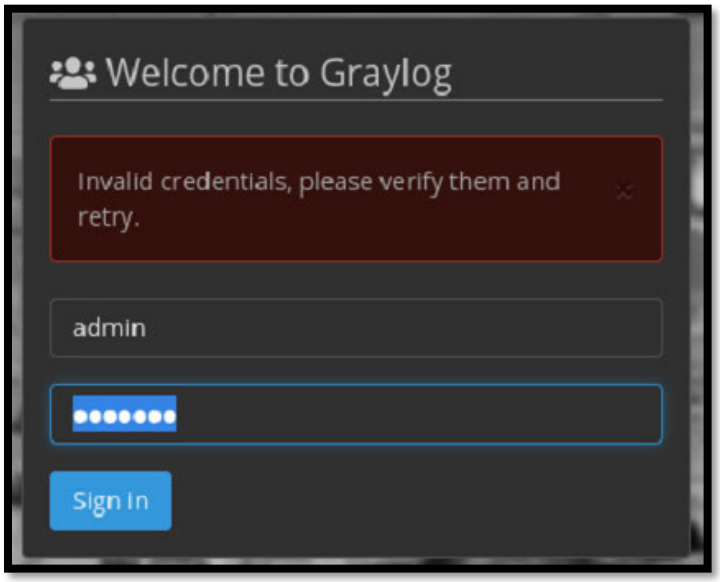


Demonstrating an unsuccessful login attempt to an Arista switch eAPI on [redacted]



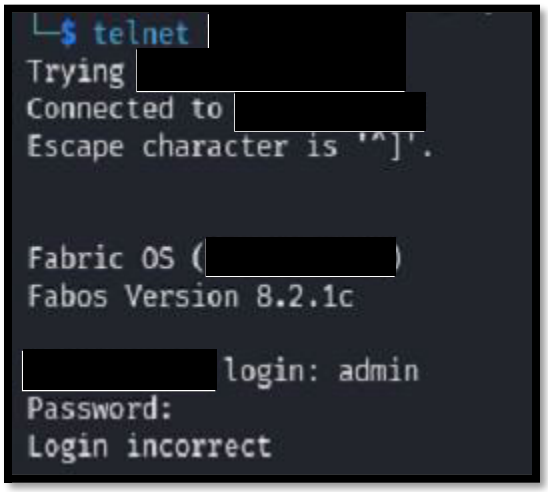
Demonstrating an unsuccessful login attempt to QNAP on [redacted]

[redacted] *unsuccessful login attempt to Calypso on* [redacted]

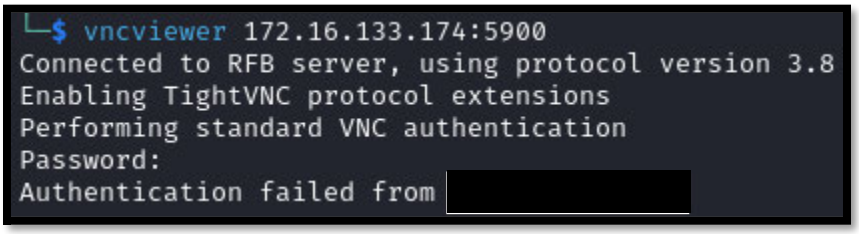


Demonstrating an unsuccessful login attempt to Graylog on [redacted]

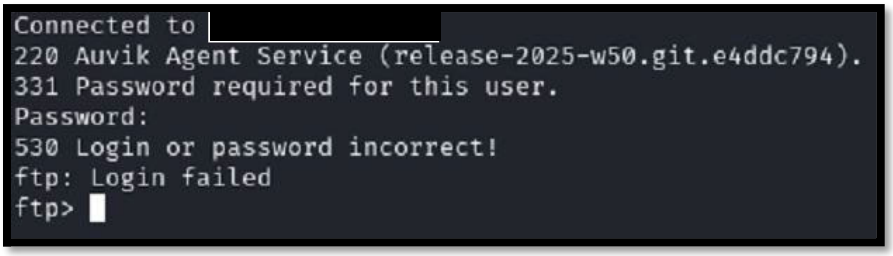
Demonstrating an unsuccessful login attempt to Horizon Omnissa on [redacted]



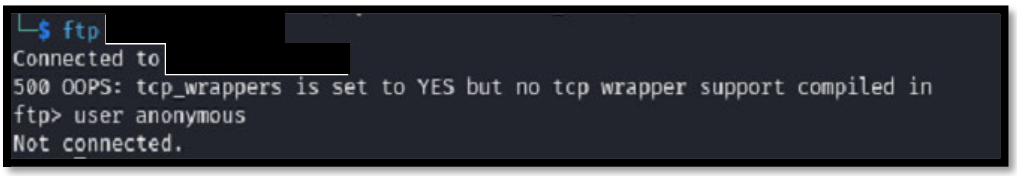
[redacted] *unsuccessful login attempt to Telnet on* [redacted]



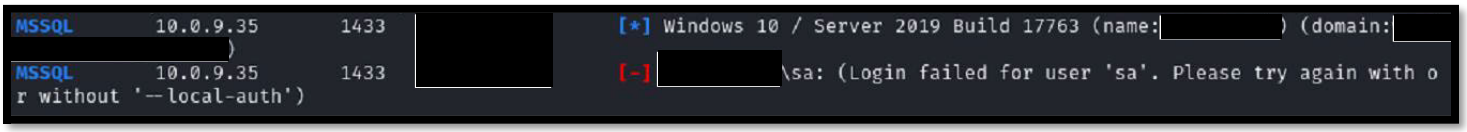
Demonstrating an unsuccessful login attempt using VNC on [redacted]



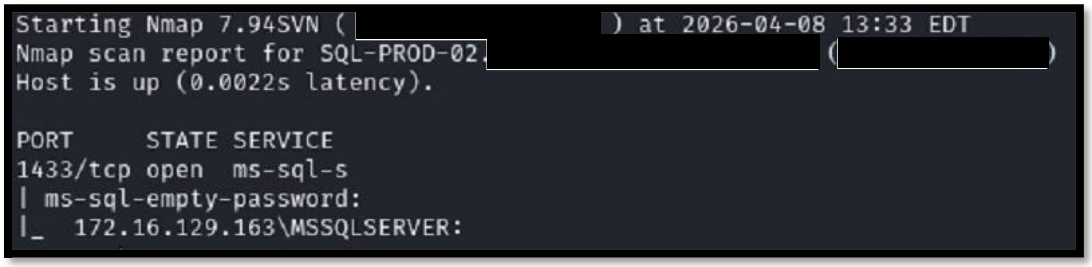
Demonstrating an unsuccessful login attempt using FTP on [redacted]



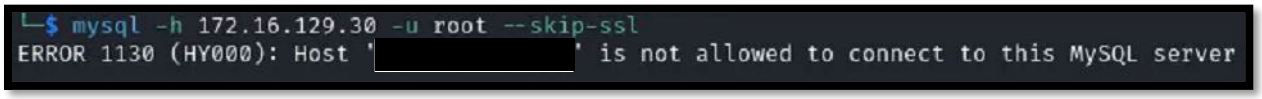
Demonstrating an unsuccessful anonymous login attempt using FTP on [redacted]



Demonstrating an unsuccessful login attempt using account "SA" via MSSQL on [redacted]



Demonstrating a lack of empty password via MSSQL on [redacted]



Demonstrating an unsuccessful login attempt using MySQL on [redacted]

Demonstrating enumeration of NFS mounts on [redacted]

```
└─$ sudo mount -t nfs -o vers=3 [redacted]
mount.nfs: access denied by server while mounting [redacted]/esx_nfs
```

Demonstrating unsuccessful NFS mount of shares on [redacted]

```
Starting Nmap 7.94SVN ( [redacted] ) at 2026-04-08 13:49 EDT
Nmap scan report for [redacted] ([redacted])
Host is up (0.0043s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|_  Couldn't find any accounts
```

Demonstrating unsuccessful enumeration of SMTP user accounts on [redacted]

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-08 15:15 EDT
Nmap scan report for [redacted] ([redacted])
Host is up (0.0031s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: SMTP RSET: failed to receive data: connection closed

Nmap done: 1 IP address (1 host up) scanned in 75.35 seconds
```

Demonstrating unsuccessful exploitation of SMTP open relay on [redacted]

```
└─$ snmpwalk -v 2c -c public 10.0.9.103
Timeout: No Response from 10.0.9.103
```

Demonstrating failed SNMPv2 Walk on [redacted]

Additionally, further enumeration of the SSH protocol led to the discovery of hosts susceptible to RegreSSHion (CVE-2024-6387), and numerous hosts running out of date SSH versions. Lastly, Abacus discovered the [redacted] internal portal, from which enumeration of documents lead to discovery of email addresses, names, and phone numbers of [redacted] staff. The various names, phone numbers, and email addresses could be used with social engineering to coerce [redacted] employees into divulging sensitive information and/or establish a permanent foothold in the environment.

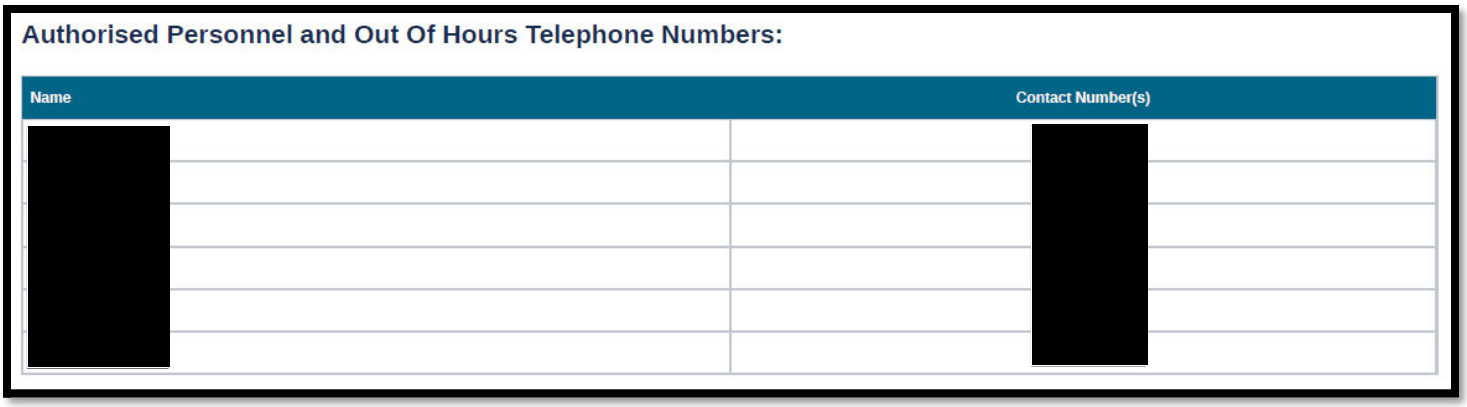
```
🚨 Servers likely vulnerable: 5
   [+] Server at 10.0.9.61 (running SSH-2.0-OpenSSH_8.9p1)
   [+] Server at 10.0.9.63 (running SSH-2.0-OpenSSH_8.9p1)
   [+] Server at 10.0.9.60 (running SSH-2.0-OpenSSH_8.9p1)
   [+] Server at 172.16.129.111 (running SSH-2.0-OpenSSH_8.7)
   [+] Server at 172.16.129.27 (running SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.14)
```

Demonstrating OpenSSH versions susceptible to RegreSSHion (CVE-2024-6387) on various hosts

```
Servers not vulnerable: 32
  [+] Server at 192.168.23.1 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.129.40 (running SSH-2.0-OpenSSH_7.4)
  [+] Server at 10.0.9.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.129.60 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.129.28 (running SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5)
  [+] Server at 172.16.132.16 (running SSH-2.0-OpenSSH_8.0)
  [+] Server at 10.0.9.59 (running SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.12)
  [+] Server at 172.16.132.20 (running SSH-2.0-OpenSSH_8.0)
  [+] Server at 172.16.134.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.133.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.135.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.131.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 10.0.9.119 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.199.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.132.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.130.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.129.10 (running SSH-2.0-OpenSSH_7.8)
  [+] Server at 172.16.132.30 (running SSH-2.0-OpenSSH_9.9)
  [+] Server at 10.0.9.23 (running SSH-2.0-OpenSSH_9.9)
  [+] Server at 10.0.9.141 (running SSH-2.0-OpenSSH_9.9)
  [+] Server at 10.0.9.142 (running SSH-2.0-OpenSSH_9.9)
```

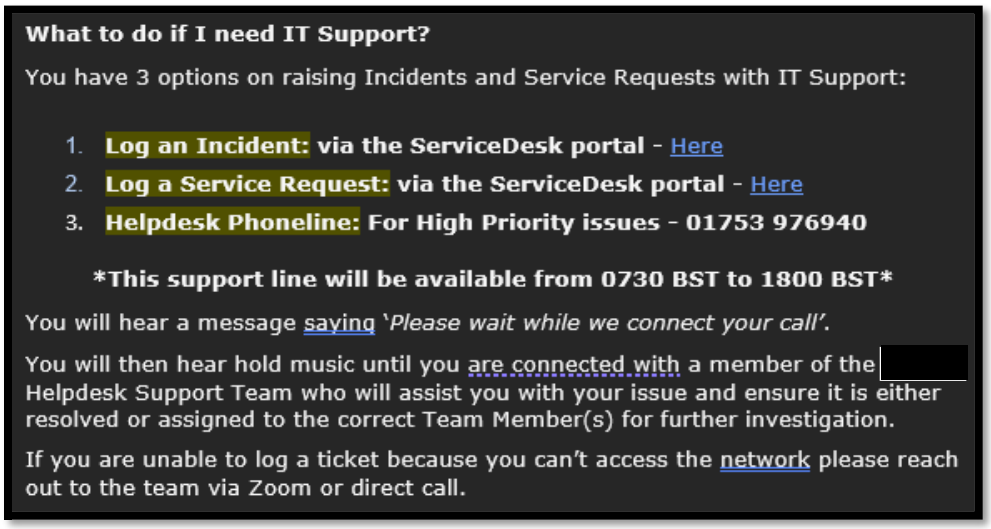
Demonstrating out of date OpenSSH versions running on various hosts

Demonstrating unauthenticated access to [redacted] *internal portal* [redacted]*co.uk* ([redacted] & [redacted])



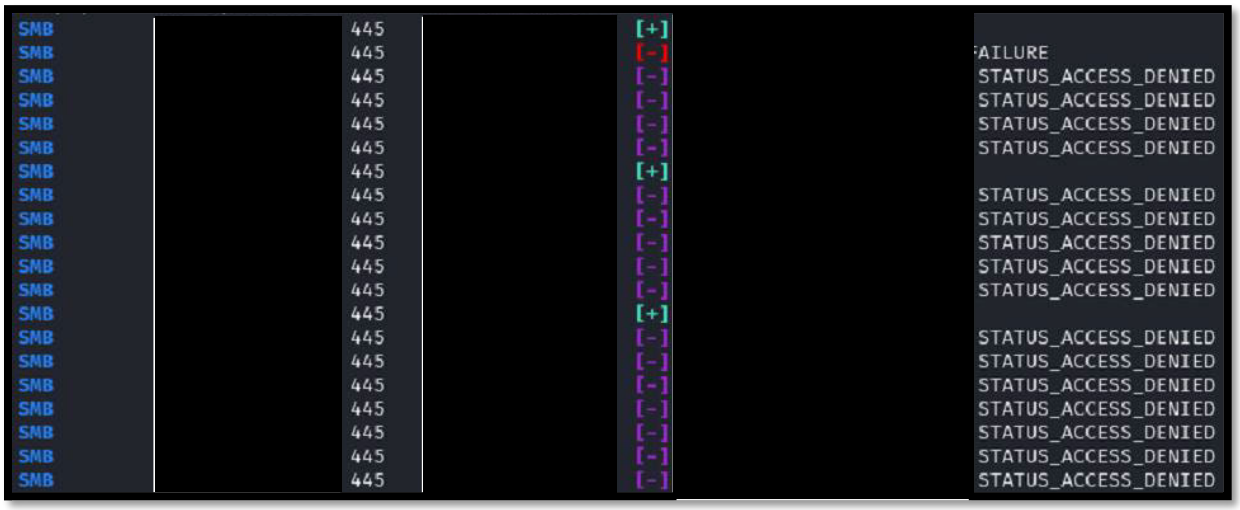
Demonstrating enumeration of staff information from [redacted] *internal portal via Business-Travel-Expenses-Policy.pptx (1 of 2)*

Demonstrating enumeration of an email address from [redacted] internal portal via Business-Travel-Expenses-Policy.pptx (2 of 2)



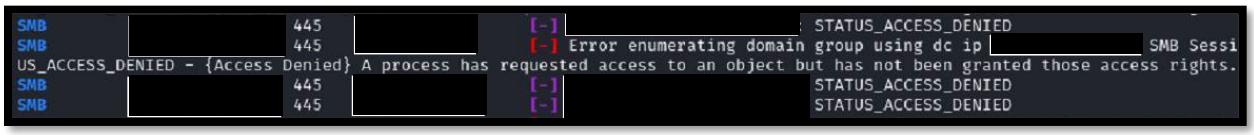
Demonstrating enumeration of IT Support number from [redacted] internal portal via How-to-get-in-touch-with-IT.docx

Abacus continued penetration testing by focusing on specific protocols that are often susceptible to manipulation, such as default credentials, Server Message Block (SMB), Microsoft Remote Procedure Call (MSRPC), Lightweight Directory Access Protocol (LDAP), and Kerberos. Abacus tested these protocols found numerous hosts with SMB Signing not enabled and was able to run a SMB Null Session on hosts but ultimately could not further the kill chain further due to compensating controls. Regarding LDAP, Abacus was able to channel-bind two vCenter servers, but no further exploitation could be carried out. On the other hand, Abacus was able to successfully AS-REP Roast the [redacted] domain controller and obtain a NTLM user hash for the local administrator account. The local administrator account could then be cracked offline and used to obtain access to the domain controller and the rest of the domain.



Demonstrating successful SMB Null Session enumeration on numerous hosts ([redacted] & [redacted]

Demonstrating the ability to enumerate SMB Users on device

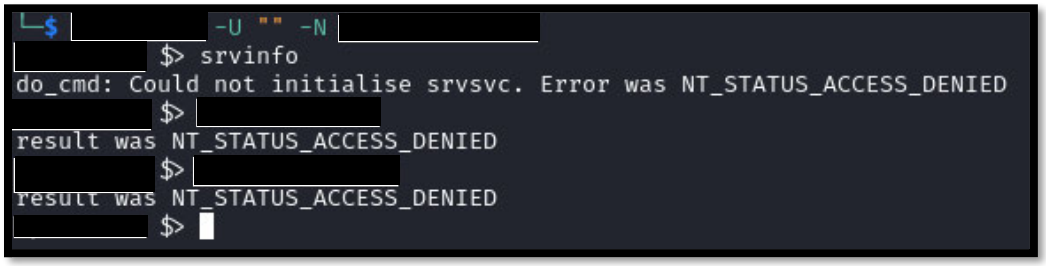


Demonstrating unsuccessful enumeration of SMB Groups on numerous devices

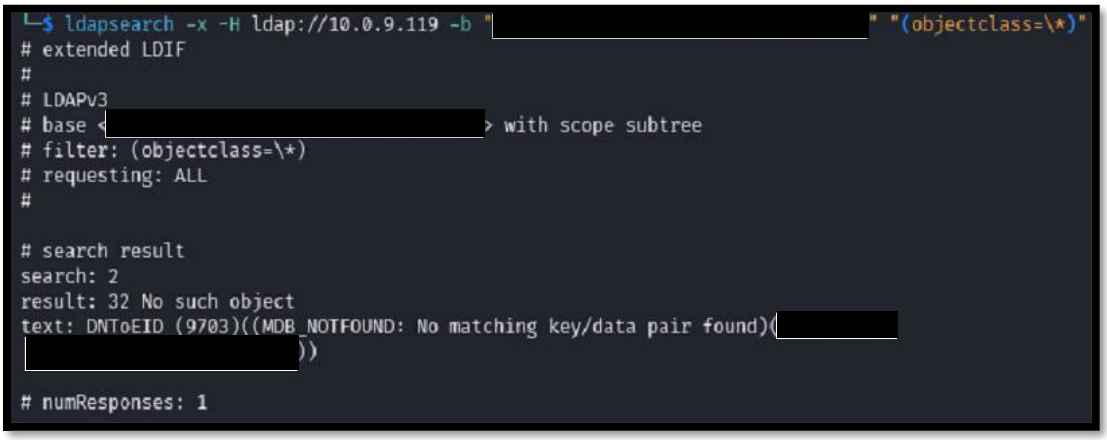
Demonstrating failed authentication utilizing SMB Guest account on numerous devices

Demonstrating the ability to enumerate SMB Password Policy on 10.0.9.145

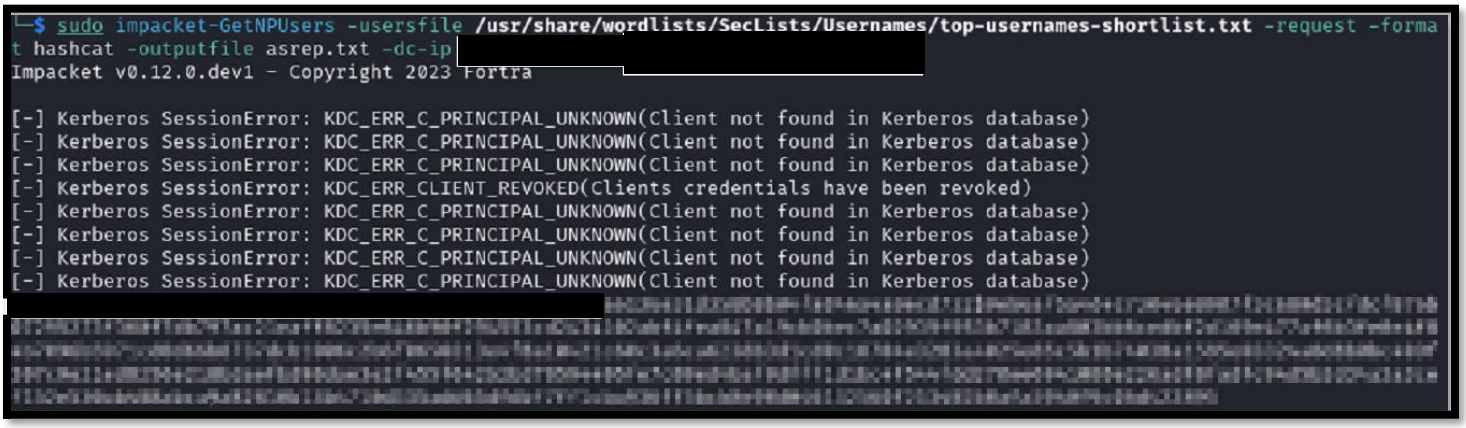
Demonstrating unsuccessful enumeration of SMB Shares on numerous devices on



Demonstrating failed user null session authentication over MSRPC via rpcclientt



Demonstrating unsuccessful LDAP Channel bind enumeration using Ldapsearch



Demonstrating successful Kerberoasting and subsequent captured NTLM user hash from host [redacted]

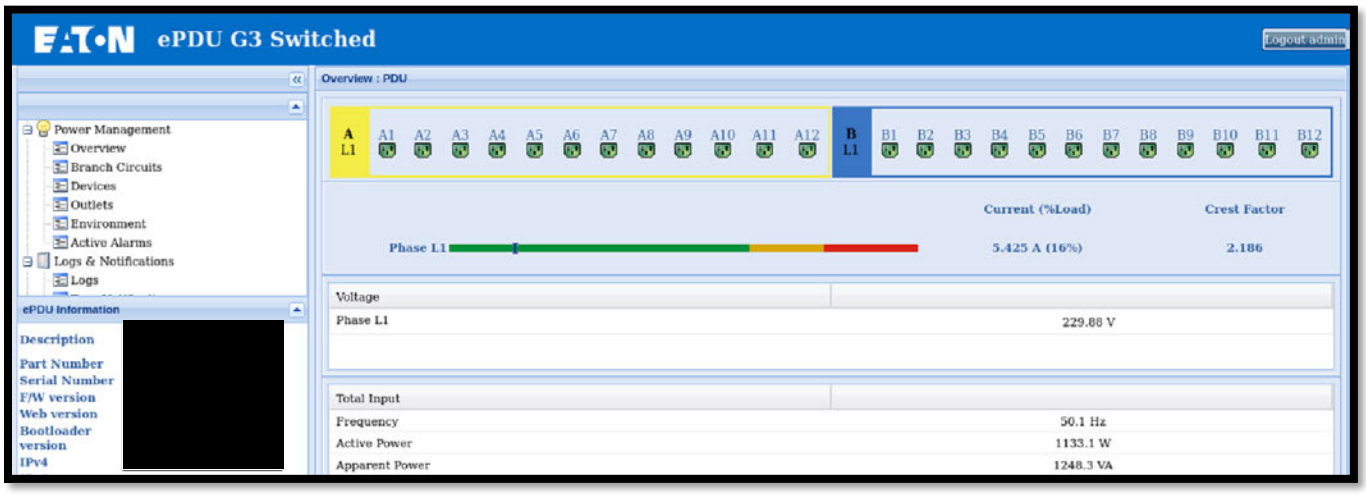
Throughout the comprehensive internal network penetration testing conducted by Abacus, numerous attack vectors were meticulously identified and rigorously tested. The testing activities were successfully concluded after exhausting all viable in-scope attack avenues. The assessment revealed two high-risk, three moderate-risk, one low-severity risk, and one informational-risk findings, each of which has been documented for further action.

Risk Details

PDU with Default Credentials [Internal]
MITRE ATT&CK Tactic: TA0006 – Credential Access
Exploited – Impact: High – **Ease:** High – **Risk:** High

Summary:
The affected endpoint utilized well-known vendor default credentials, which allowed Abacus Security engineers to login as an admin user using: Username: admin, Password: admin. While this access did not provide a pivot point into other devices, the ability to cause a Denial-of-Service (DoS) attack to downstream, connected devices, is possible. Through said DoS attack, could power off critical network infrastructure causing a severe infrastructure outage.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Change the default credentials to a unique password in accordance with internal password complexity requirements.

Reference(s):
https://attack.mitre.org/techniques/T1078/001/
https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/power-distribution-for-it-equipment/eaton-basic-rack-pdu/Eaton_ePDU_G3_Operations_Manual.133.pdf

Affected Endpoint(s):
[redacted]

ASREP Roasting – User Accounts With Kerberos Pre-Authentication Disabled [Internal]
MITRE ATT&CK Tactic: TA0006 – Credential Access
Exploited – Impact: High **– Ease:** High – **Risk:** High

Summary:
During the assessment, it was possible to enumerate and perform ASREP Roasting attacks against one user account that did not require Kerberos pre-authentication. Valid usernames were obtained via null session queries / Kerberos user enumeration. Offline cracking of the captured AS-REP would then allow threat actors credentialed authentication into the domain environment.

ASREP Roasting is a Kerberos abuse technique that targets Active Directory user accounts configured with "Do not require Kerberos preauthentication" (UF_DONT_REQUIRE_PREAUTH flag set, corresponding to the "Do not require Kerberos preauthentication" checkbox in the user account properties).

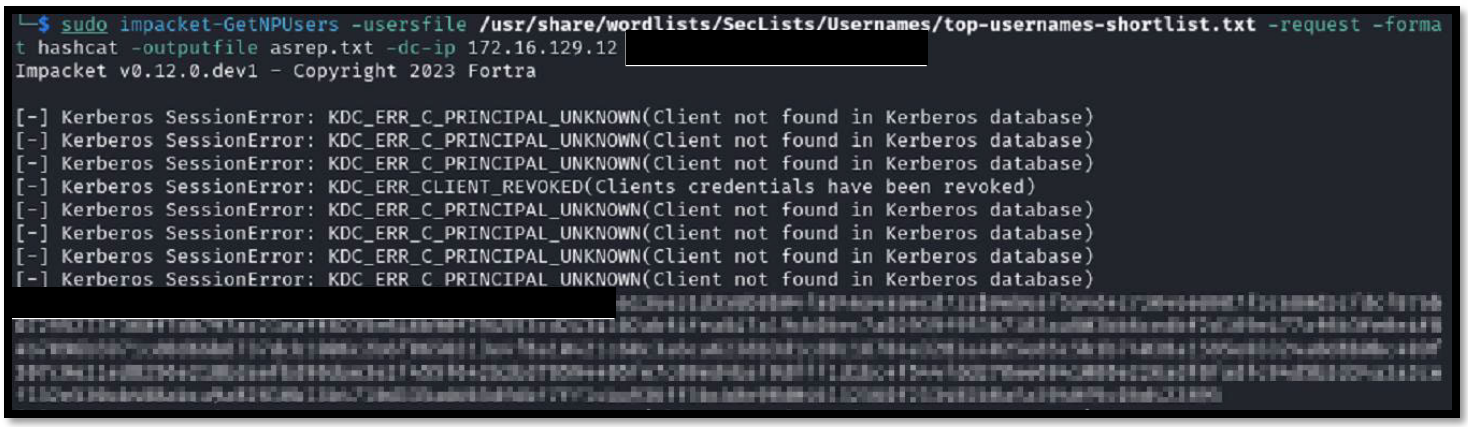
1. In a normal Kerberos authentication flow, when a user authenticates, the client first sends an AS-REQ without a timestamp encrypted with the user's long-term key. If pre-authentication is required (default and recommended setting), the KDC rejects this request and demands pre-authentication data (typically a timestamp encrypted with the user's hash).

2. When the account has pre-authentication disabled, the KDC trusts the initial AS-REQ and immediately responds with an AS-REP message that contains a TGT encrypted with the user's long-term key (NTLM hash or RC4/ARCFOUR in most environments).

3. An attacker who knows (or guesses) valid usernames can request an AS-REP for those accounts from anywhere on the network (no domain credentials required for the request itself).

4. The attacker receives the encrypted portion of the AS-REP, extracts the encrypted TGS (actually the encrypted TGT session key in this case), and then performs offline brute-force or dictionary attacks against it to recover the user's plaintext password (or NT hash).

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

Identify all accounts with the "Do not require Kerberos preauthentication" option enabled (UF_DONT_REQUIRE_PREAUTH flag) and disable it unless absolutely required by a legacy application.
Use Protected Users group or Authentication Policies/Silos where possible to further restrict vulnerable accounts.
Enforce strong, complex passwords (20+ characters) on any account that must retain this setting.
Monitor for Event ID 4768 with result code 0x19 (pre-auth not required) in large volumes, which indicates ASREP roast attempts.
Perform Account Audit
Get-ADUser -Filter * -Properties DoesNotRequirePreAuth | Where-Object {$_.DoesNotRequirePreAuth -eq $True -and $_.Enabled -eq $True} | Select-Object 'SamAccountName','DoesNotRequirePreAuth' | Sort-Object 'SamAccountName'

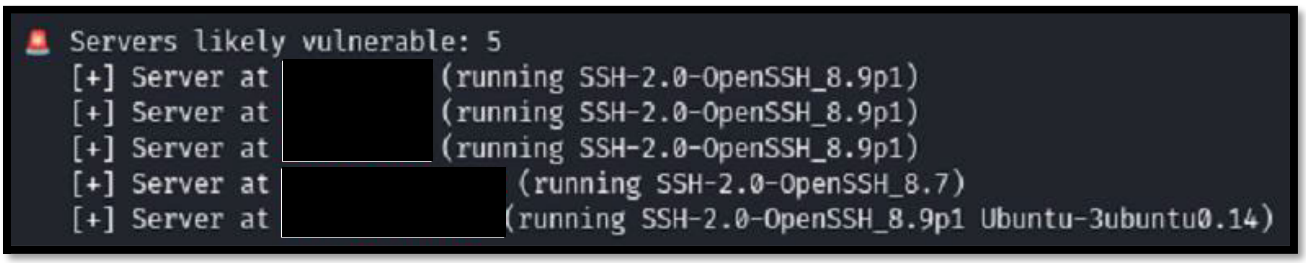
Reference(s):
https://attack.mitre.org/techniques/T1558/004
https://attack.mitre.org/detectionstrategies/DET0113
https://techcommunity.microsoft.com/blog/microsoft-security-blog/helping-protect-against-as-rep-roasting-withmicrosoft-defender-for-identity/2244089
https://learn.microsoft.com/en-us/defender-for-identity/security-posture-assessments/accounts

Affected Endpoint(s):
[redacted]

OpenSSH Susceptible to CVE-2024-6387 [Internal]
MITRE ATT&CK Tactic: TA0007 – Discovery
Detected: (QoD 85%) - **Impact:** Moderate – **Ease**: Moderate – **Risk**: Medium

Summary:
The affected endpoints were fingerprinted as utilizing OpenSSH with specific versions known to be susceptible to CVE-2024-6387 also known as regreSSHion. This vulnerability was publicly disclosed in July of 2024 and can be exploited by malicious actors to achieve unauthenticated remote code execution (RCE) as the root account.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Ensure all instances of OpenSSH are upgraded to the most recent version, which at the time of writing is version 10.3 released in April of 2026.

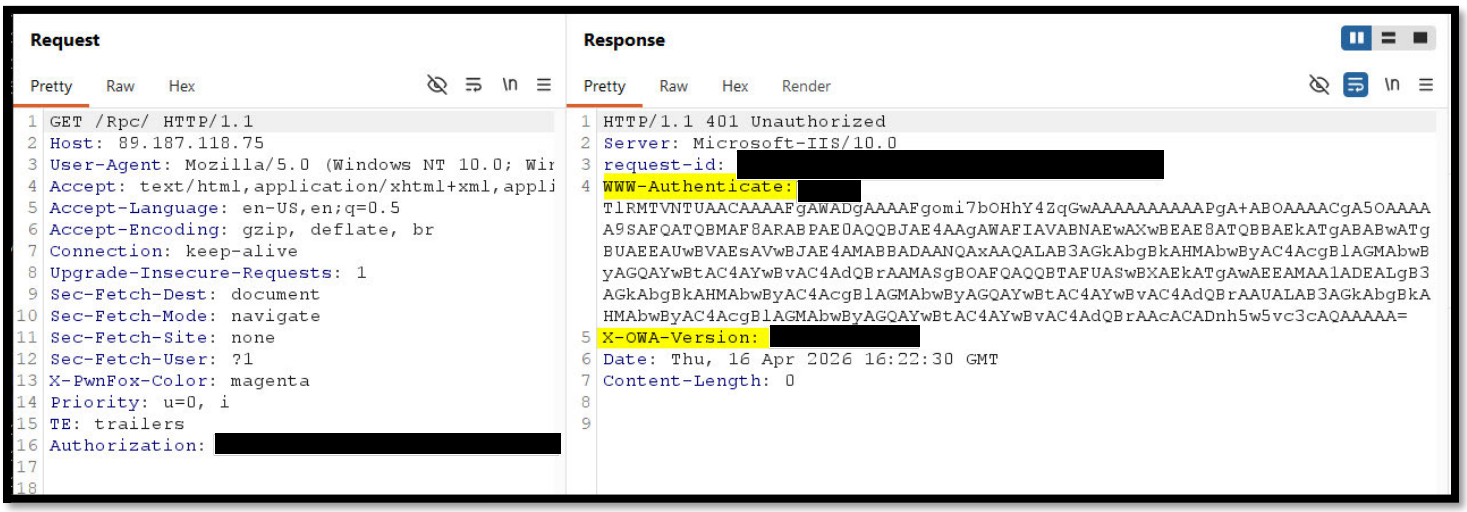
Reference(s):
https://nvd.nist.gov/vuln/detail/CVE-2016-1908
https://nvd.nist.gov/vuln/detail/CVE-2023-38408
https://www.openssh.com/releasenotes.html

Affected Endpoint(s):
[redacted], [redacted]

Externally Exposed NTLM Authentication [External]
MITRE ATT&CK Tactic: TA0001 – Initial Access
Detected: (QoD 95%) - **Impact:** High – **Ease**: Moderate – **Risk**: Medium

Summary:
NTLM authentication is exposed on the server's public endpoints. These endpoints are attractive to attackers because the NTLM protocol does not support multi-factor authentication (MFA). Attackers can freely conduct password spray and credential stuffing attacks against these endpoints, potentially leading to initial access and bypassing MFA. These endpoints also leak information such as internal company domain names and computer names.

Risk Detection Result(s):




```
[INF] Current httpx version v1.8.1 (outdated)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
https://89.187.118.75/Autodiscover/Autodiscover.xml [401]
https://89.187.118.75/Autodiscover/AutodiscoverService.svc/root [401]
https://89.187.118.75/Autodiscover [401]
https://89.187.118.75/EWS/ [401]
https://89.187.118.75/OAB/ [401]
https://89.187.118.75/PowerShell/ [401]
https://89.187.118.75/Rpc/ [401]
$
```

```
Internal information leaked from this misconfiguration:
dns_domain_name: [redacted]
dns_computer_name: [redacted]
forest_name: [redacted]
netbios_domain_name: [redacted]
netbios_computer_name: [redacted]
```

Risk Mitigation Recommendation(s):

- Block network access to the NTLM endpoint from the internet, or disable NTLM authentication entirely.
- Implement Extended Protection for Authentication utilizing Microsoft's PowerShell script for Exchange servers.
- Update the Exchange server to a supported version with up-to-date configuration options.

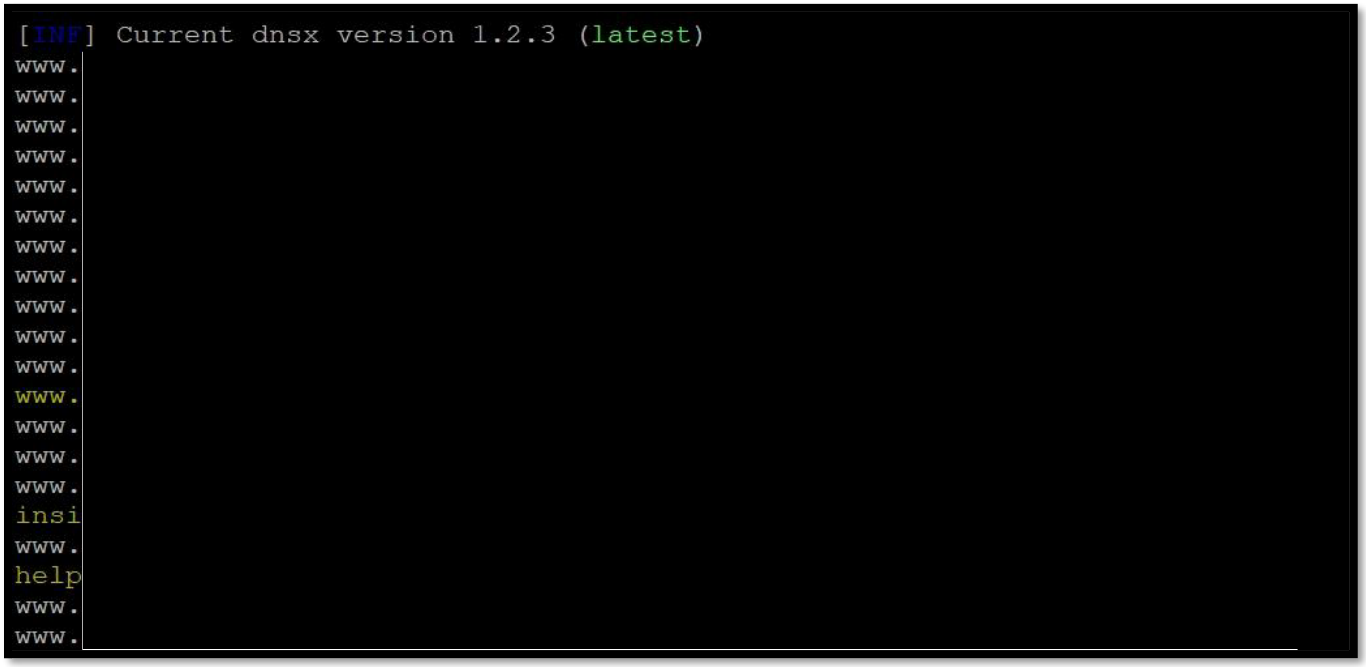
Reference(s):
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-ntlm-authentication-in-this-domain
https://www.microsoft.com/en-us/msrc/blog/2024/12/mitigating-ntlm-relay-attacks-by-default
https://microsoft.github.io/CSS-Exchange/Security/ExchangeExtendedProtectionManagement/
https://learn.microsoft.com/en-us/microsoft-365/enterprise/hybrid-modern-auth-overview?view=o365-worldwide
https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs#disable-ws-trust-windows-endpoints-on-the-proxy-from-extranet

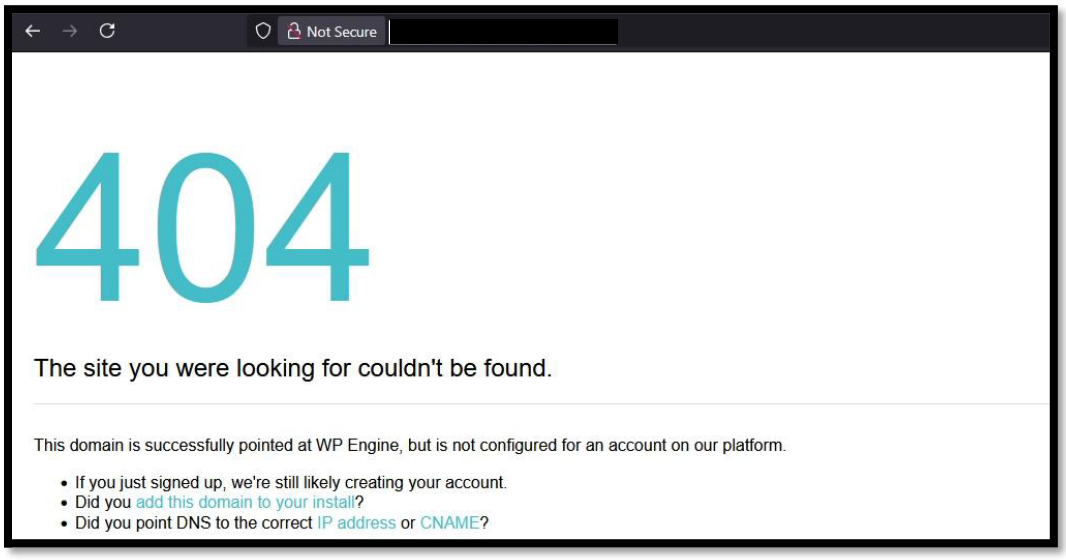
Affected Endpoint(s):
[redacted]

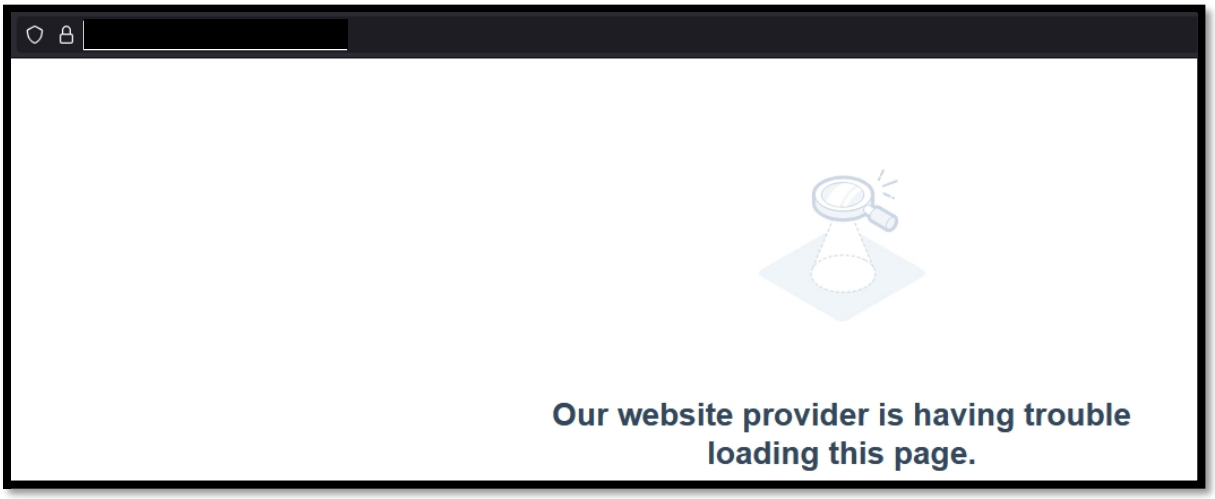
Subdomain Takeover via Dangling DNS [redacted] [External]
MITRE ATT&CK Tactic: TA0042 – Resource Development
Detected: (QoD 95%) - **Impact:** Moderate – **Ease**: Moderate – **Risk**: Medium

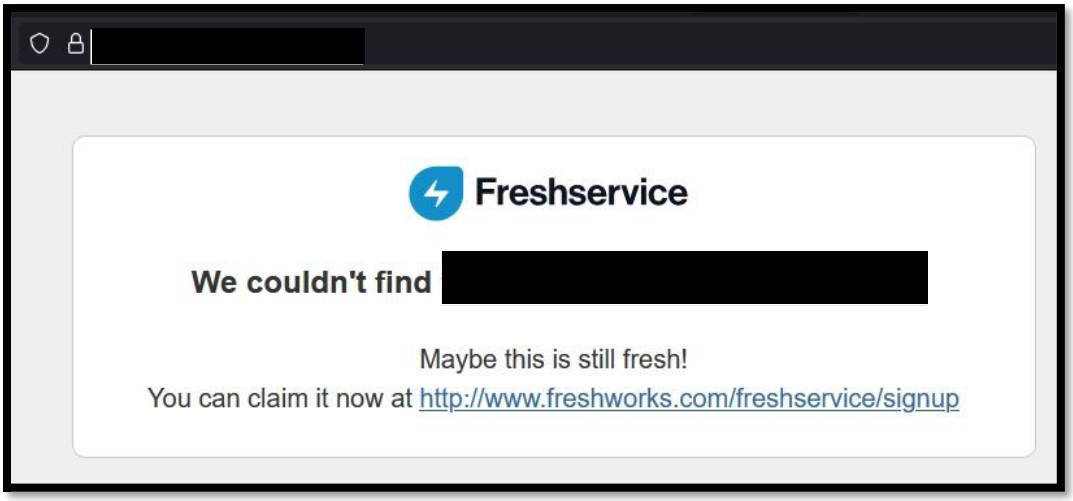
Summary:
Abacus identified subdomains with dangling CNAME records that were vulnerable to subdomain takeover. The DNS CNAME records for the affected domains point to parked or expired resources which could be claimed by a malicious actor. Subdomain takeover is a type of vulnerability that appears when an organization has configured a DNS CNAME entry for one of its subdomains pointing to an external service, but those services are no longer utilized. A malicious actor could register to the services and claim the subdomains in order to host malicious content or leverage the trusted domains for social engineering.

Risk Detection Result(s):









Risk Mitigation Recommendation(s):

- Remove CNAME entries from DNS records on the affected subdomains if the services are no longer needed, or point the CNAME record to a valid, provisioned resource.

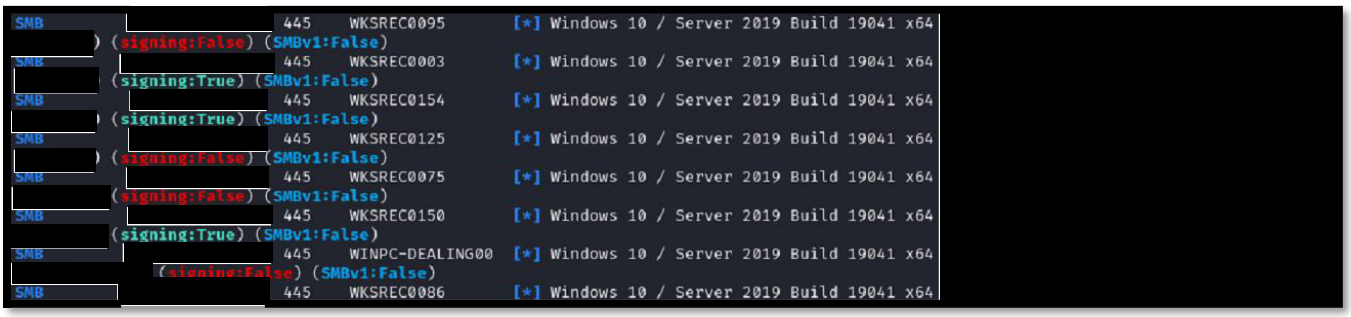
Reference(s):
https://www.paloaltonetworks.com/cyberpedia/what-is-a-dangling-dns
https://developer.mozilla.org/en-US/docs/Web/Security/Attacks/Subdomain_takeover
https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Affected Endpoint(s):

SMB Signing Not Required and Enforced [Internal]
MITRE ATT&CK Tactic: TA0040 – Impact
Detected: (QoD 85%) - **Impact:** High – **Ease**: High – **Risk**: Medium

Summary:
The affected endpoints do not have SMB signing enabled. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps to prevent NTLM pass-the-hash attacks. However, considerations should be made as to whether all of the devices need SMB and Windows filesharing enabled.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Enable SMB signing using registry edits or group policy. For group policy, set "Digitally Sign Communications -- Always"
- SMB signing can also be enabled using PowerShell with the following command:
  - Set-SmbServerConfiguration -RequireSecuritySignature $True -EnableSecuritySignature $True -EncryptData $True -Confirm:$false

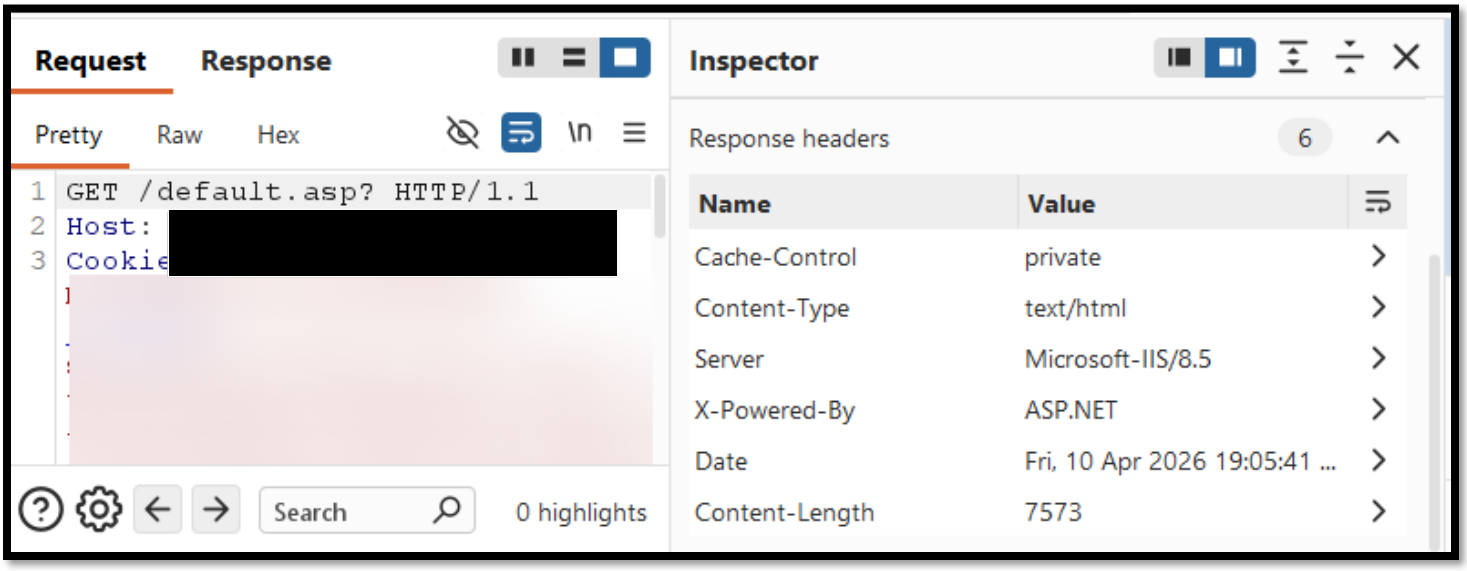
Reference(s):
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always

Affected Endpoint(s):

Missing HTTP Security Headers [External]
MITRE ATT&CK Tactic: TA0001 – Initial Access
Detected: (QoD 95%) - **Impact:** Moderate – **Ease**: Moderate – **Risk**: Medium

Summary:
The affected web applications did not implement a robust "Content-Security-Policy" (CSP) header or an HTTP "Strict-Transport-Security" (HSTS) policy. A strong CSP adds an additional layer of protection against client-side attacks such as Cross-Site Scripting (XSS), clickjacking, and form jacking. HSTS is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTP (HTTPS) connections. The server communicates the HSTS Policy to the user agent via an HTTP response header field named Strict-Transport-Security. HSTS Policy specifies a period of time during which the user agent shall access the server in only a secure fashion.

Risk Detection Result(s):



Strict transport security not enforced

Severity: Low
Confidence: Certain
URL: [redacted]

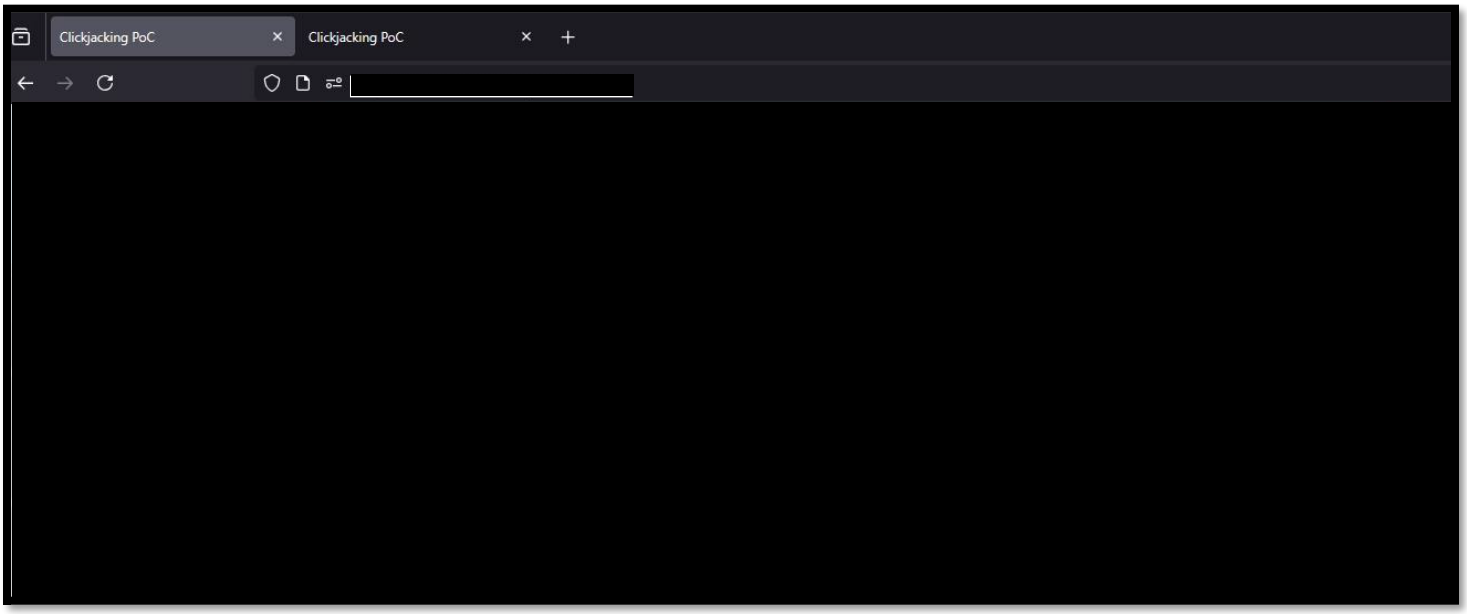
Issue detail

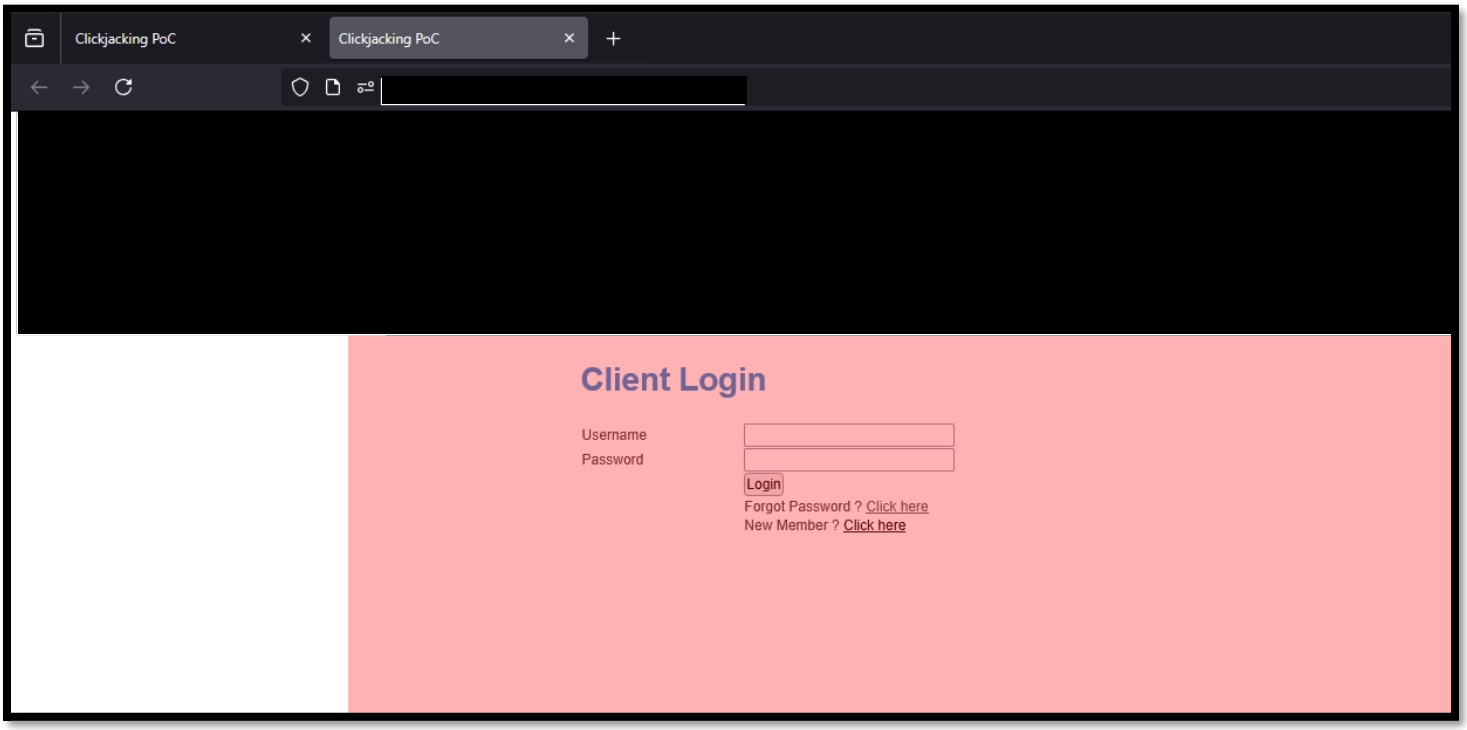
4 instances of this issue were identified, at the following locations:

- /
- /default.asp
- /index.asp
- /noflash.asp

Frameable response (potential Clickjacking)

Severity: Information
Confidence: Firm
URL: [redacted]





Risk Mitigation Recommendation(s):

- Implement a CSP with the 'default-src', 'base-uri', 'script-src', 'style-src', and 'object-src' directives for all websites
- Implement form jacking protection for all websites via the 'form-src' directive, which should be set to 'self' or 'none'.
- Implement the 'frame-ancestors' directive across all websites to protect against clickjacking.
- Consider implementing the 'upgrade-insecure-requests' directive to better protect against machine-in-the-middle attacks.
- Consider implementing the 'report-uri' directive for reporting CSP violations.
- Implement the Strict-Transport-Security HTTP header with an appropriate max-age setting, such as two years. For example:
    - Strict-Transport-Security: max-age=63072000; includeSubDomains always;

Reference(s):
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Content_Security_Policy_Cheat_Sheet.md
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

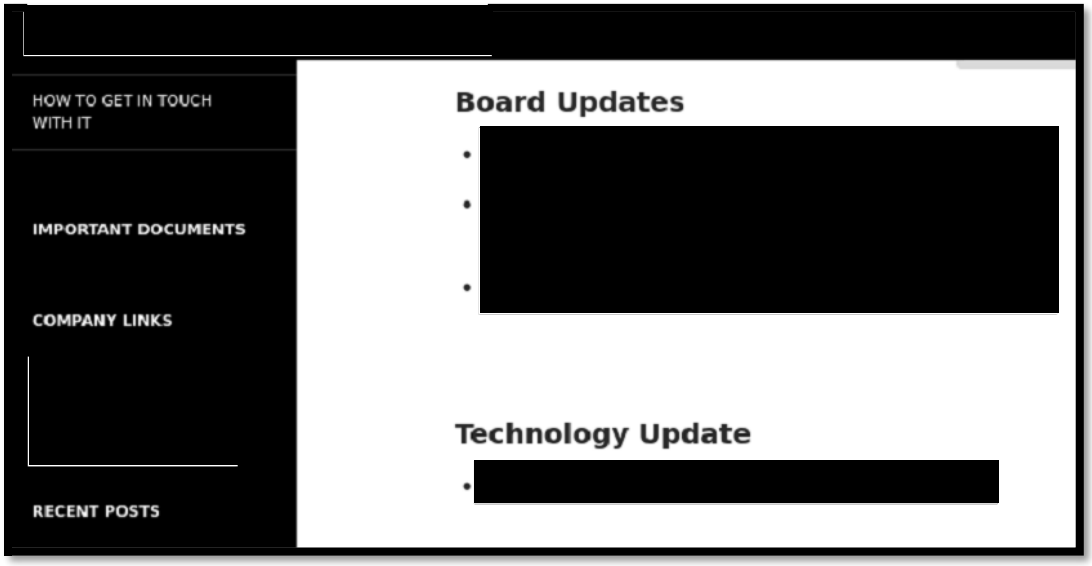
Affected Endpoint(s):

[redacted]

Unauthenticated Internal Web Portal [Internal]
MITRE ATT&CK Tactic: TA0042 – Resource Development
Exploited – Impact: Moderate – **Ease**: Moderate – **Risk**: Medium

Summary:
Abacus discovered that no authentication is required to access the internal '[redacted] portal. Any user on the internal network can access this internal portal without the need to provide credentials. As a result, sensitive data could be fully enumerated and exfiltrated. Examples of sensitive data are the presence of Board Updates, Technology Updates, access to company guidelines, policies, client information, and contact information. Discovery of these documents lead to uncovering a phone number for the help desk, which could be potentially used for social engineering.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Implement authenticated user access: username/password in conjunction with Multi-Factor Authentication (MFA)

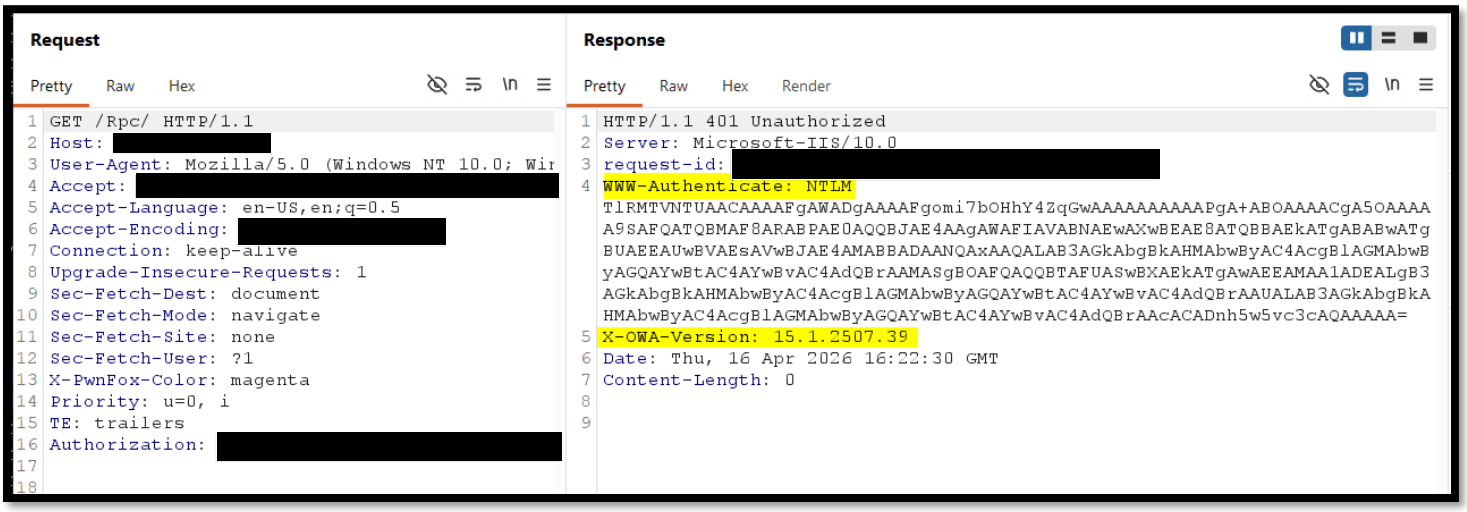
Reference(s):
https://attack.mitre.org/techniques/T1078/
https://learn.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/plan-user-authentication

Affected Endpoint(s):
[redacted]

End of Support Exchange Server [External]
MITRE ATT&CK Tactic: TA0001 – Initial Access
Detected: (QoD 100%) - **Impact:** Moderate – **Ease:** Moderate – **Risk:** Medium

Summary:
The identified Microsoft Exchange server was fingerprinted by HTTP response headers as version 15.1.2507.39, which was identified as Exchange Server 2026 CU 23 from April 2024. This version is no longer supported by Microsoft (end of support) and no longer receives security updates. Additionally, patches for CVE-2025-64666 and CVE-2025-64667 are not applied, which could result in privilege escalation or email spoofing.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Restrict access to the server behind a reverse proxy, VPN, or gateway to mitigate internet exposure.
- Update the Exchange server to a supported version with up-to-date configuration options.

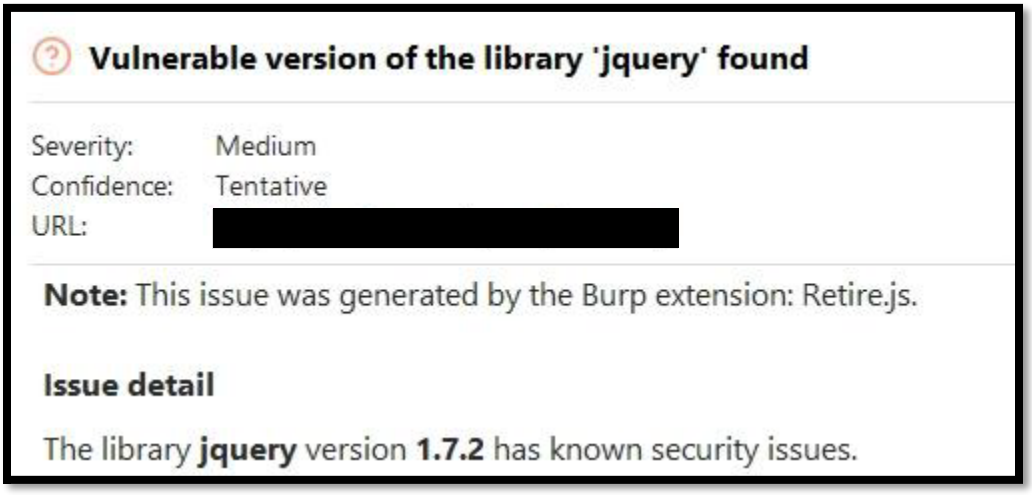
Reference(s):
https://www.messageware.com/microsoft-exchange-server-build-numbers-and-release-dates/
https://learn.microsoft.com/en-us/lifecycle/products/exchange-server-2016

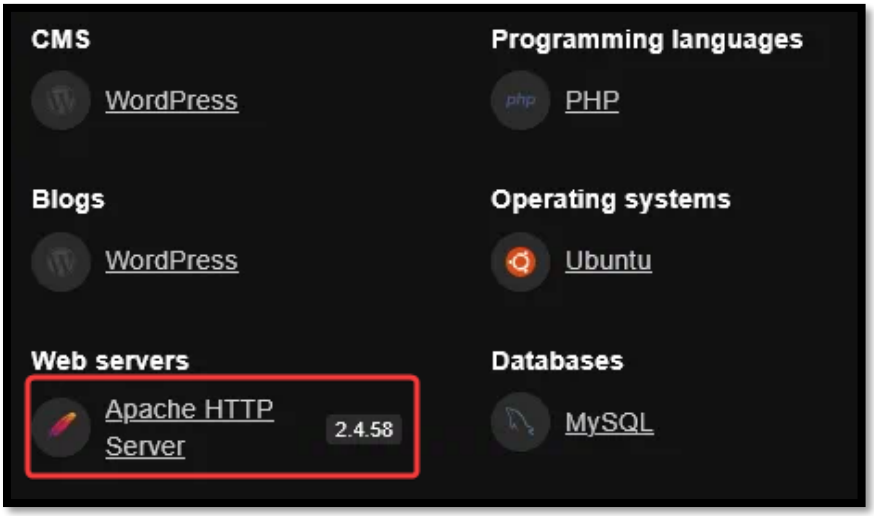
Affected Endpoint(s):
[redacted]

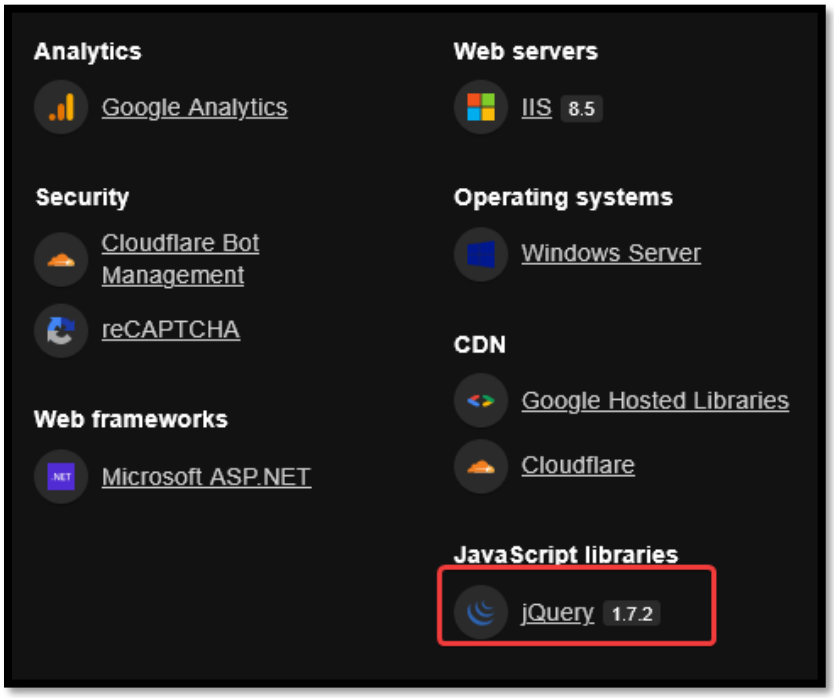
Vulnerable and Outdated Web Technologies [External]
MITRE ATT&CK Tactic: TA0042 – Resource Development
Detected: (QoD 70%) - **Impact:** Low – **Ease**: Low – **Risk**: Low

Summary:
The web applications were found to utilize outdated and reportedly vulnerable technologies. The "prod" subdomain was found to use an outdated version of Apache web server and WordPress plugins with reported vulnerabilities. The "clients" and "insights" subdomains also utilized a reportedly vulnerable version of jQuery which did not result in successful cross-site scripting. Utilizing outdated and vulnerable web technologies increases the attack surface of the web applications and can provide additional entry points for a malicious actor.

Risk Detection Result(s):







Risk Mitigation Recommendation(s):

- Update jQuery to the latest non-vulnerable version, which at the time of writing is 4.0.0.
- Update Apache to the latest non-vulnerable version, which at the time of writing is 2.4.66.
- Consider updating WordPress plugins to the latest versions.

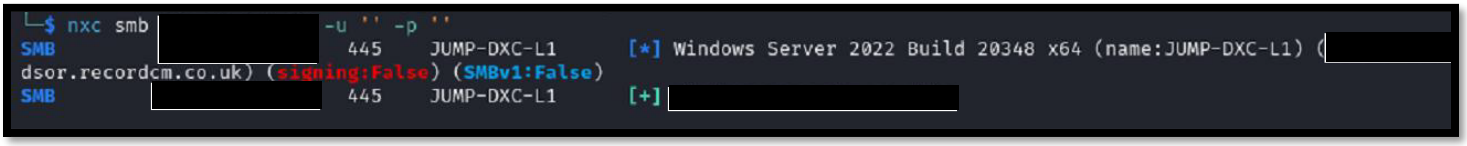
Reference(s):
https://security.snyk.io/package/npm/jquery/1.7.2
https://httpd.apache.org/security/vulnerabilities_24.html
https://wpscan.com/vulnerability/7dbafbe2-abbc-4191-a587-afa89c2f7421/
https://www.cvedetails.com/vulnerability-list/vendor_id-20123/product_id-57126/version_id-1840504/year-2025/Icegram-Email-Subscribers-Newsletters-5.7.29.html

Affected Endpoint(s):
[redacted]

SMB Null Session Allowed [Internal]
MITRE ATT&CK Tactic: TA0006 – Credential Access
Detected: (QoD 75%) - **Impact:** Low – **Ease**: Low – **Risk**: Low

Summary:
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. However, Abacus was not able to enumerate various SMB groups, shares, users, password-policy, etc. from various network hosts.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- 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.

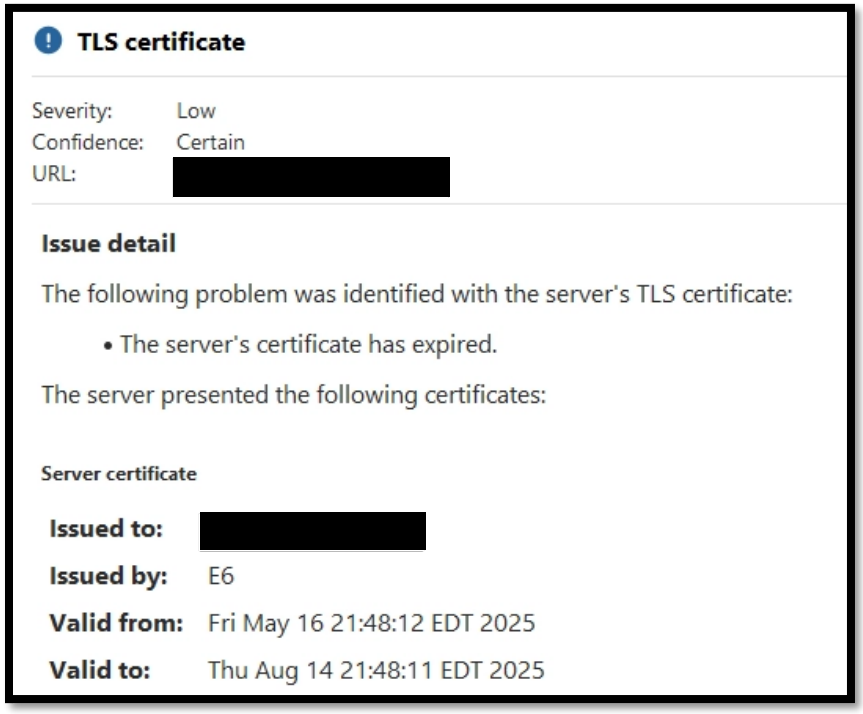
Reference(s):
https://cwe.mitre.org/data/definitions/284.html
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-prote...
https://seneej.wordpress.com/2015/07/29/how-to-disable-smbnetbios-null-session-on-domain-controller...
https://techcommunity.microsoft.com/blog/filecab/smb-and-null-sessions-why-your-pen-test-is-probabl...
https://techcommunity.microsoft.com/blog/filecab/smb-and-null-sessions-why-your-pen-test-is-probabl...
https://techgenix.com/share-permissions/
https://attack.mitre.org/techniques/T1135/

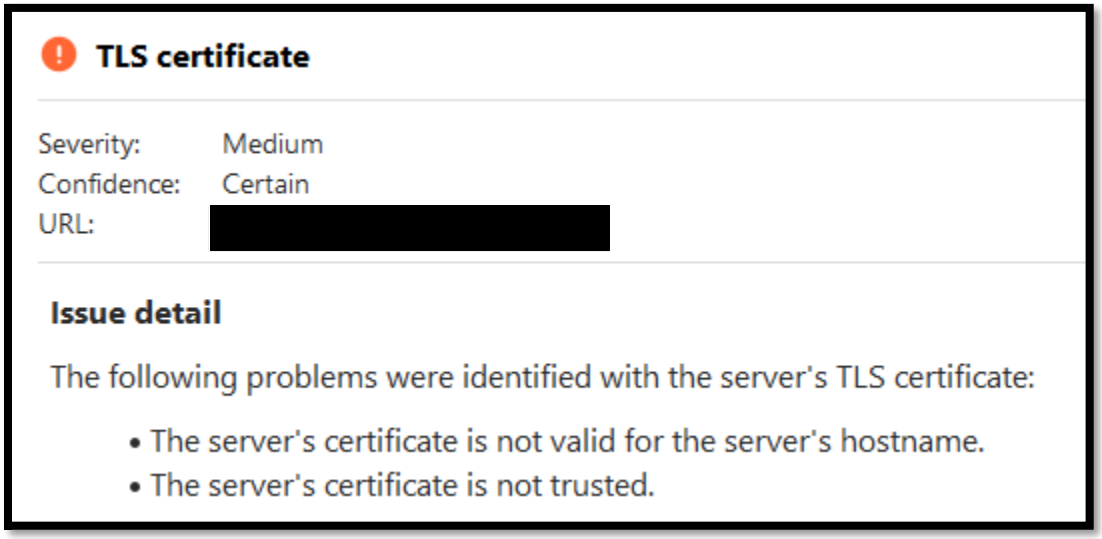
Affected Endpoint(s):
[redacted] 10.0.9.145

Expired and Untrusted TLS/SSL Certificates [External]
MITRE ATT&CK Tactic: TA0043 – Reconnaissance
Detected: (QoD 100%) - **Impact:** Low – **Ease**: Low – **Risk**: Low

Summary:
The SSL/TLS certificate has expired on the "prod" subdomain. The "ir" subdomain was identified as a Plesk Obsidian application and utilized a self-signed and untrusted certificate. Expired or self-signed certificates cause 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. A malicious actor can take advantage of this by launching adversary-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 or untrusted certificate, users won't be able to browse to it at all.

Risk Detection Result(s):





Risk Mitigation Recommendation(s):

- Renew the certificate
- If not in use, shut down the web site with the expired certificate
- Configure network access controls to prevent public access to the web site that is using the self-signed certificate

Reference(s):
https://letsencrypt.org/docs/
https://en.wikipedia.org/wiki/Public_key_certificate
https://https.cio.gov/hsts/

Affected Endpoint(s):
[redacted]

Missing or Misconfigured SPF and DMARC Records [External]
MITRE ATT&CK Tactic: TA0042 – Resource Development
Detected: (QoD 100%) - **Impact:** Low – **Ease:** Low – **Risk:** Low

Summary:
A DMARC record was identified for the domain; however, the domain did not implement a quarantine or rejection policy to mitigate phishing and email spoofing, which could enable social engineering attacks. Additionally, the SPF record for the domain included authorized senders that exceeded the 10 lookup limit defined in RFC 7208. When the SPF record is queried by receiving email servers, the record is parsed and reverse DNS lookups are performed on each included domain. Due to the recursive nature of the DNS lookups against the "freshservice.com" inclusion, the SPF record was not fully parsed by the receiving server, which could introduce email deliverability issues.

Risk Detection Result(s):

```
v=spf1 ip4:89.187.118.75/32 include:eu._netblocks.mimecast.com include:email.freshservice.com include:email.sogolytics.co
m include:spf.mandrillapp.com include:mail.webropolsurveys.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version
Prefix+	Typeip4	Value89.187.118.75/32	PrefixDescPass	DescriptionMatch if IP is in the given range.
Prefix+	Typeinclude	Valueeu._netblocks.mimecast.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typeinclude	Valueemail.freshservice.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typeinclude	Valueemail.sogolytics.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typeinclude	Valuespf.mandrillapp.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typeinclude	Valuemail.webropolsurveys.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix~	Typeall	Value	PrefixDescSoftFail	DescriptionAlways matches. It goes at the end of your record.

	Test	Result	
Status	NameSPF Included Lookups	ResponseToo many included lookups (16)	More Info
Status	NameDMARC Policy Not Enabled	ResponseIt is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%.	More Info

```
[                ] ["v=DMARC1; p=none; pct=100; fo=1; ri=3600;
=mailto:6f2964a2@inbox.          .com,mailto:49aea29ec59f759@
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	include	sendgrid.net	Pass	The specified domain is searched for an 'allow'.
+	include	emailus.freshservice.com	Pass	The specified domain is searched for an 'allow'.
+	include	emaileuc.freshservice.com	Pass	The specified domain is searched for an 'allow'.
+	include	emailmum.freshservice.com	Pass	The specified domain is searched for an 'allow'.
+	include	emailsyd.freshservice.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

Risk Mitigation Recommendation(s):

- Implement a quarantine or reject policy for DMARC, such as:
  - v=DMARC1; p=quarantine; pct=100; rua=mailto:postmaster@domainname.com; ruf=mailto:postmaster@domainname.com; fo=1

- Remove included domains from the SPF record to flatten and mitigate SPF recursive lookups
  - Consider implementing ip4 statements in lieu of include statements in the SPF record

Reference(s):
https://mxtoolbox.com/dmarc/dmarc-setup?lm=NAV-PD
https://mxtoolbox.com/dmarc/details/dmarc-tags/dmarc-policy-options
https://www.dmarcanalyzer.com/dmarc-deployment-workflow/
https://mxtoolbox.com/problem/spf/spf-included-lookups

Affected Endpoint(s):
[redacted]

Insecure TLS 1.2 Cipher Suites [External]
MITRE ATT&CK Tactic: TA0042 – Resource Development
Detected: (QoD 100%) - **Impact:** Low – **Ease**: Low – **Risk**: Low

Summary:
Abacus found that the web applications utilized deprecated AES-CBC cipher suites. Support is no longer recommended for ciphers that utilize Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode, as this configuration is inherently vulnerable to timing attacks, such as the Lucky Thirteen class of attacks. Additionally, cipher suites utilizing RSA without Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) are not recommended, as the RSA key exchange lacks Perfect Forward Secrecy (PFS). This means that, if an attacker were to compromise the RSA private key, all previously encrypted communications could be decrypted. It is instead recommended to consider utilizing TLS 1.3 or to utilize TLS 1.2 with AES in Galois/Counter Mode (GCM) with ECDHE RSA for key exchange.

Risk Detection Result(s):

```
TLS 1.2 Cipher Suites:
  Attempted to connect using 156 cipher suites.

  The server accepted the following 10 cipher suites:
     TLS_RSA_WITH_AES_256_GCM_SHA384                  256
     TLS_RSA_WITH_AES_256_CBC_SHA256                  256
     TLS_RSA_WITH_AES_128_GCM_SHA256                  128
     TLS_RSA_WITH_AES_128_CBC_SHA256                  128
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            128       ECDH: prime256v1 (256 bits)
     TLS_DHE_RSA_WITH_AES_256_GCM_SHA384              256       DH (2048 bits)
     TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256       DH (2048 bits)
     TLS_DHE_RSA_WITH_AES_128_GCM_SHA256              128       DH (2048 bits)
     TLS_DHE_RSA_WITH_AES_128_CBC_SHA                 128       DH (2048 bits)
```

```
TLS 1.2 Cipher Suites:
  Attempted to connect using 156 cipher suites.

  The server accepted the following 20 cipher suites:
     TLS_RSA_WITH_AES_256_GCM_SHA384                  256
     TLS_RSA_WITH_AES_256_CBC_SHA256                  256
     TLS_RSA_WITH_AES_256_CBC_SHA                     256
     TLS_RSA_WITH_AES_128_GCM_SHA256                  128
     TLS_RSA_WITH_AES_128_CBC_SHA256                  128
     TLS_RSA_WITH_AES_128_CBC_SHA                     128
     TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256      256       ECDH: X25519 (253 bits)
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256    256       ECDH: X25519 (253 bits)
     TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384          256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384          256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA             256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256          128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256          128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA             128       ECDH: prime256v1 (256 bits)
```

```
TLS 1.2 Cipher Suites:
  Attempted to connect using 156 cipher suites.

  The server accepted the following 12 cipher suites:
     TLS_RSA_WITH_AES_256_GCM_SHA384                256
     TLS_RSA_WITH_AES_256_CBC_SHA256                256
     TLS_RSA_WITH_AES_256_CBC_SHA                   256
     TLS_RSA_WITH_AES_128_GCM_SHA256                128
     TLS_RSA_WITH_AES_128_CBC_SHA256                128
     TLS_RSA_WITH_AES_128_CBC_SHA                   128
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384          256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384          256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA             256       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256          128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256          128       ECDH: prime256v1 (256 bits)
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA             128       ECDH: prime256v1 (256 bits)
```

Risk Mitigation Recommendation(s):

- Update TLS configurations for modern security and intermediate compatibility.
- Recommended Encryption Algorithms and Cipher Suites:
- Cipher suites (TLS 1.3):
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256

- Cipher suites (TLS 1.2):
    - ECDHE-ECDSA-AES128-GCM-SHA256
    - ECDHE-RSA-AES128-GCM-SHA256
    - ECDHE-ECDSA-AES256-GCM-SHA384
    - ECDHE-RSA-AES256-GCM-SHA384
    - ECDHE-ECDSA-CHACHA20-POLY1305
    - ECDHE-RSA-CHACHA20-POLY1305

Reference(s):
https://wiki.mozilla.org/Security/Server_Side_TLS
https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html
https://sweet32.info/
https://www.netsparker.com/blog/web-security/how-the-beast-attack-works/

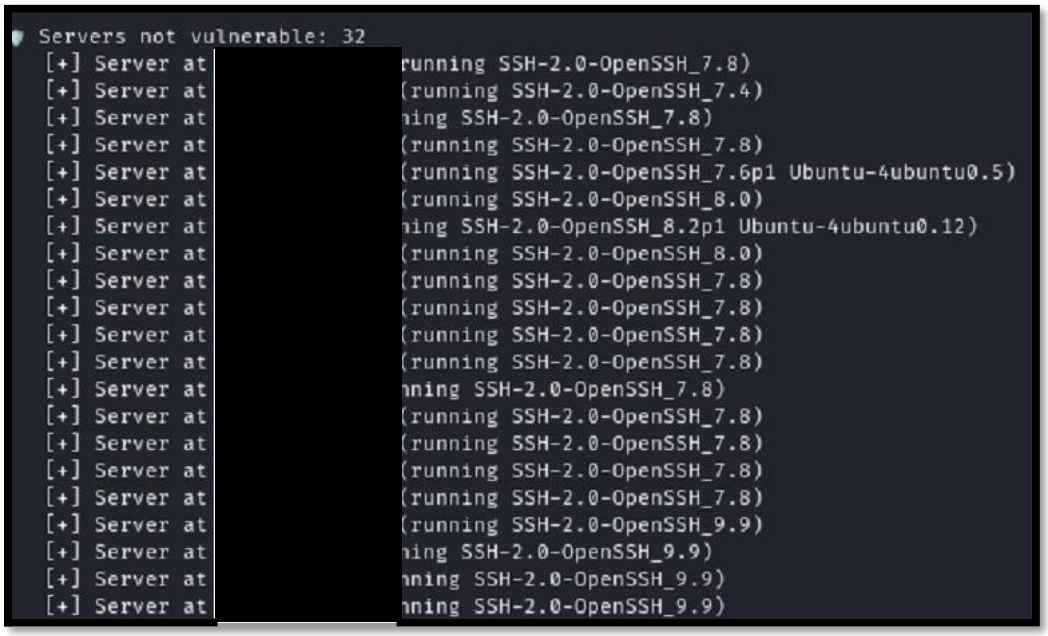
Affected Endpoint(s):

[redacted]

Outdated OpenSSH With Known Vulnerabilities [Internal]
MITRE ATT&CK Tactic: TA0043 – Reconnaissance
Informational

Summary:
Active analysis identified an OpenSSH service which was fingerprinted as version 6.6.1p1, which was originally released in 2012. This version has been associated with numerous vulnerabilities to include CVE 2023-38408 and CVE-2020-15778.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Ensure all instances of OpenSSH are upgraded to the most recent version, which at the time of writing is version 10.3.

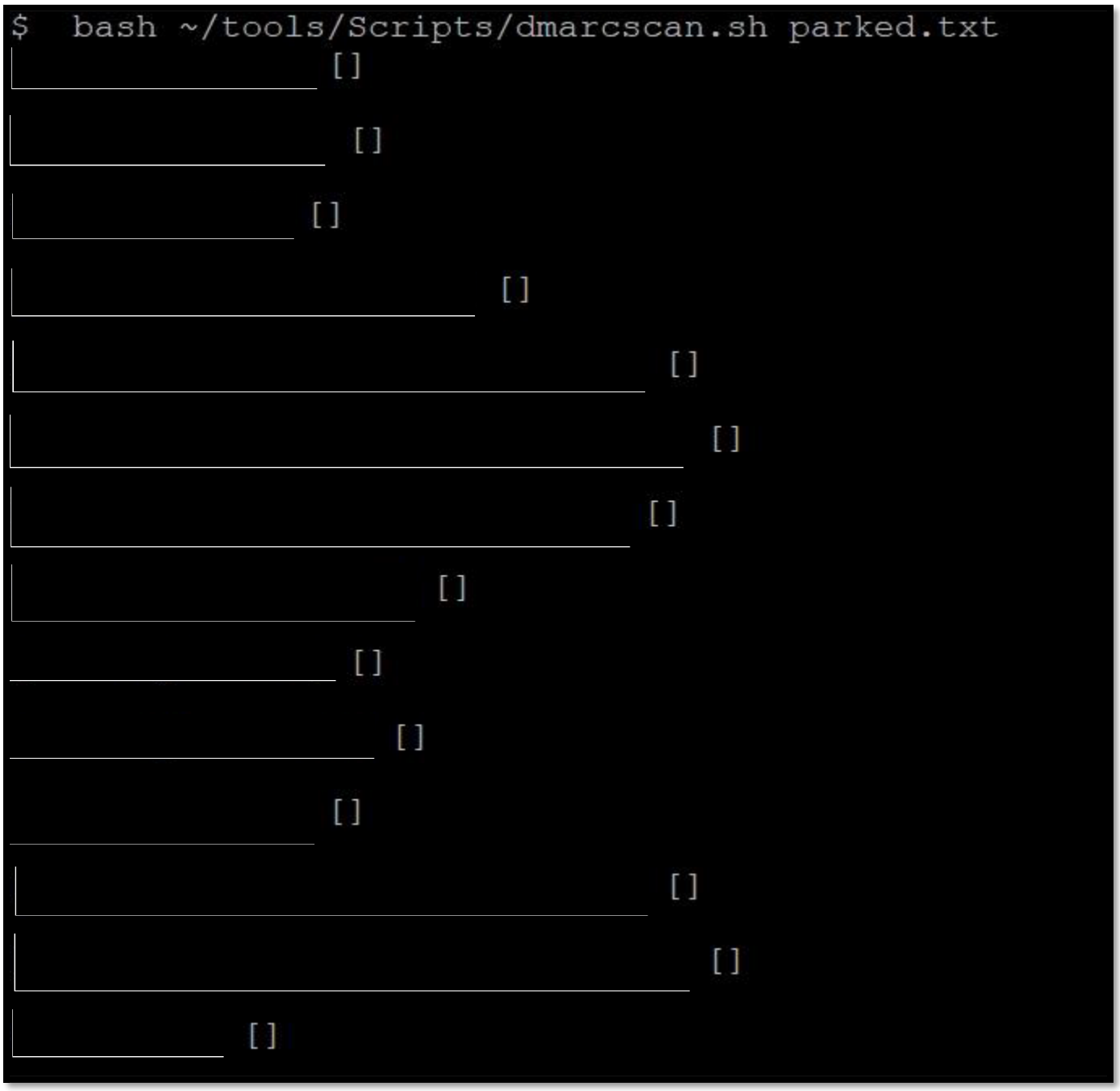
Reference(s):
https://nvd.nist.gov/vuln/detail/CVE-2016-1908
https://nvd.nist.gov/vuln/detail/CVE-2023-38408
https://www.openssh.com/releasenotes.html

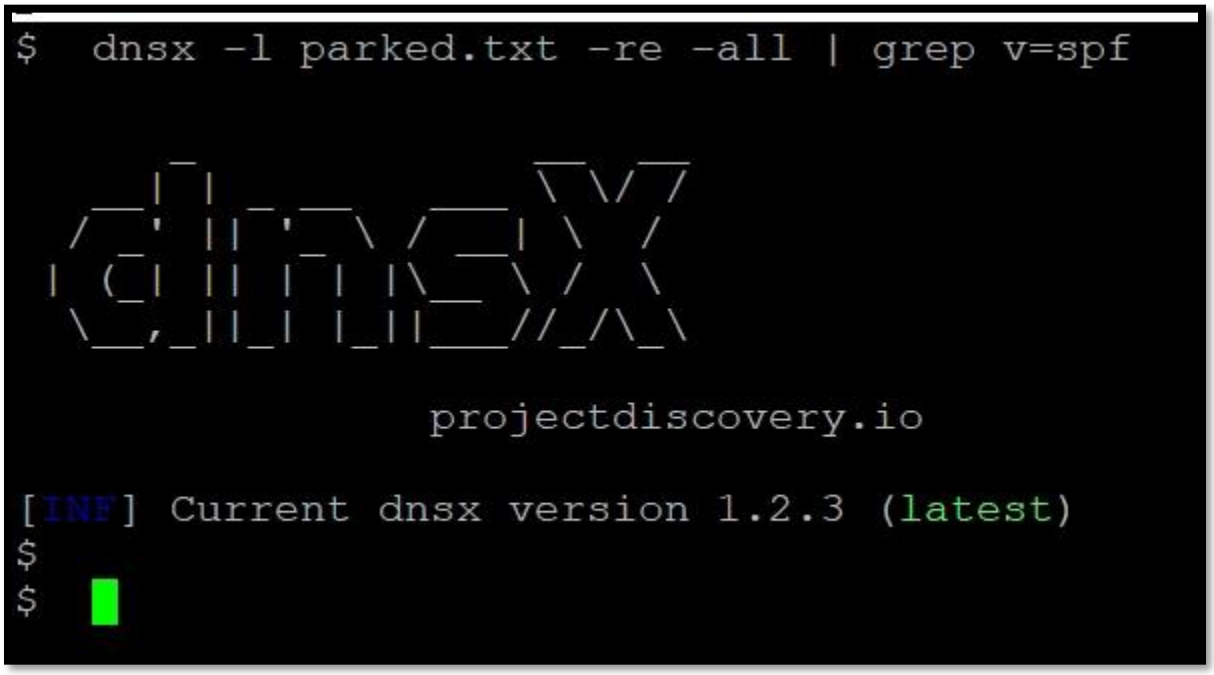
Affected Endpoint(s):
172.16.129.55, [redacted]

Missing SPF Hard Fail and DMARC Reject [External]
MITRE ATT&CK Tactic: TA0042 – Resource Development
Informational

Summary:
The affected domains did not implement an SPF policy with hard fail or a DMARC rejection policy. Parked domains that are not configured to send or receive email should implement SPF and DMARC hard failures to prevent email spoofing from malicious email servers. Without the SPF and DMARC controls, a malicious actor can spoof email from the parked domains and perform social engineering attacks against the organization or users coming from a trusted domain.

Risk Detection Result(s):





Risk Mitigation Recommendation(s):

- Consider implementing an SPF record with hard fail on parked domains:
  - v=spf1 -all

- Consider implementing a DMARC policy with reject on parked domains:
  - v=DMARC1; p=reject; rua=mailto:postmaster@domainname.com

Reference(s):
https://autospf.com/blog/using-spf-hardfail-for-non-email-sending-domains-a-guide/
https://powerdmarc.com/spf-softfail-vs-hardfail/
https://mxtoolbox.com/dmarc/details/dmarc-tags/dmarc-policy-options
https://www.dmarcanalyzer.com/dmarc-deployment-workflow/

Affected Endpoint(s):

[redacted]

Conclusion

While Abacus makes a best effort to rank the severity of vulnerabilities, it is not possible for any assessment to guarantee that low-risk issues cannot be chained together and significantly impact [redacted] systems. All risk ratings in this report are a combination of industry-standard ratings and considerations for unique business risk as identified by Abacus. Special consideration should also be given to the fact that multiple low-risk issues may compound into higher-risk threats.

Abacus completed the external network penetration testing, finding four moderate risks, four low risks, and one informational item. A Microsoft Exchange server was exposed to the internet that was identified as end of support and was no longer receiving security updates from Microsoft. In addition, the server was configured to accept NTLM authentication that could provide an entry point into [redacted] environment through relay attacks or brute-force. Three other domains were identified with dangling DNS records that could result in subdomain takeover using social engineering attacks in tandem with the identified misconfigured email security records. Most of the identified in-scope web applications were missing important security headers to mitigate adversary-in-the-middle, downgrade attacks, and clickjacking, which could result in credential compromise using social engineering. Other lower severity issues were identified for vulnerable and outdated web technologies and expired or untrusted TLS certificates that expand the overall external attack surface. However, no initial access was achieved beyond the external perimeter.

Abacus completed the internal network penetration testing activities, two high-risk, three moderate-risk, one low-severity risk, and one informational-risk findings. From an internal perspective, [redacted] attack surface presented minimal avenues for practical exploitation. However, with sufficient time, in conjunction with successful ASREP Roasting of a domain controller, a threat actor could utilize the captured local administrator NTLM hash. Through which, one could establish access and dump user hashes to conduct privilege escalation and persistence in [redacted] environment. Furthermore, a malicious actor could exploit vendor default credentials on the Eaton ePDU to carry out a Denial-of-Service (DoS) attack by shutting down key network infrastructure. Also to note, SMB Signing Enabled but Not Required was observed on many hosts, but the lack of mDNS, LLMNR, and NBNS traffic, in addition to compensating controls effectively stopped the SMB poising kill chain in its tracks. Lastly, the presence of hosts susceptible to RegreSSHion (CVE-2024-6387) was identified, along with numerous out-of-date OpenSSH versions running on various infrastructure in [redacted] diverse IT ecosystem.

It is important to note that the risk mitigation recommendations contained in this report reflect industry best practices and Abacus's limited knowledge of [redacted] Abacus does not warrant the compatibility or operational effectiveness of the risk mitigation recommendations provided in this report, as Abacus does not have any understanding of the nuances and caveats of [redacted] network environment. Abacus highly recommends that [redacted] technology department assesses the compatibility and operational effectiveness of the risk mitigation recommendations provided in this report and uses a change management process to validate, plan and implement remediation changes in a UAT environment first.

About the Security Testers:

Founded in 2008, Abacus is an innovative, award-winning IT and Cybersecurity managed service provider offering an enterprise integrated platform specifically designed for the unique needs of the financial services industry. Abacus's Red Team has deep industry expertise that provides high-quality security testing and continuous monitoring which is tailored to meet the unique needs of financial & healthcare services firms against evolving threats and compliance demands.

Appendix A - MITRE ATT&CK Tactic Definitions

TA0043 – Reconnaissance
Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

TA0042 – Resource Development
Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access or stealing code signing certificates to help with Defense Evasion.

TA0001 – Initial Access
Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

TA0002 – Execution
Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

TA0003 – Persistence
Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

TA0004 – Privilege Escalation
Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

TA0005 – Defense Evasion
Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross listed here when those techniques include the added benefit of subverting defenses.

TA0006 – Credential Access
Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

TA0007 – Discovery
Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

TA0008 – Lateral Movement
Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own

remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

TA0009 – Collection
Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

TA0011 – Command and Control
Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

TA0010 – Exfiltration
Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command-and-control channel or an alternate channel and may also include putting size limits on the transmission.

TA0040 – Impact
Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.