Comprehensive Vulnerability Assessment Report

Executive Summary

This report documents the findings of a vulnerability assessment conducted on a target network. The assessment includes a vulnerability scan using Nmap and an asset discovery scan. The results are summarized, and potential security implications are discussed. The project demonstrates vulnerability assessment capabilities by conducting and documenting results, including scan configuration, summary of findings, vulnerability classification, discovered systems and services, critical asset identification, and basic network mapping.

Methodology

Tools Used

- Nmap: Network scanning and vulnerability detection.
- Parrot OS: Operating system used for conducting the scans.

Scan Configuration

1. Vulnerability Scan using Nmap
    - Command: **sudo nmap -sV --script vuln 192.168.64.1**
    - Description: This scan identifies open ports, services running on those ports, and known vulnerabilities associated with those services.
2. Asset Discovery Scan
    - Command: **sudo nmap -sn 192.168.64.0/24**
    - Description: This scan identifies all active hosts within the specified subnet.

Findings

Vulnerability Scan Results

Scan Details

- Date: 2025-01-29
- Time: 17:45 UTC
- Target: 192.168.64.1

Summary of Findings

- Hosts Up: 1
- Open Ports:
    - 53/tcp: Domain (generic DNS response: NOTIMP)
    - 8080/tcp: HTTP-proxy
    - 9000/tcp: cslistener?
- Services:
    - Port 53: DNS Service
    - Port 8080: HTTP Proxy
    - Port 9000: Potentially a custom service (cslistener)

Vulnerability Classification

- DNS Service (Port 53):
    - Vulnerability: Potential for DNS spoofing and cache poisoning.
    - Severity: Medium

    - Recommendation: Ensure DNS server is configured securely and patched regularly.
- HTTP Proxy (Port 8080):
    - Vulnerability: Potential for unauthorized access and data leakage.
    - Severity: Medium
    - Recommendation: Restrict access to trusted IPs and ensure proper configuration.
- Unknown Service (Port 9000):
    - Vulnerability: Potential for unauthorized access and data leakage.
    - Severity: Medium
    - Recommendation: Identify the service and ensure proper configuration and access controls.

Asset Discovery Scan Results

Scan Details

- Date: 2025-01-27
- Time: 20:55 UTC
- Target: 192.168.64.0/24

Summary of Findings

- Hosts Up: 2
- MAC Addresses:
    - 72:AE:D5:E2:81:64 (Unknown)
    - 72:AE:D5:E2:81:65 (Unknown)

Critical Asset Identification

- 192.168.64.1: Likely a server hosting DNS service, HTTP Proxy, and an unknown service on port 9000.
- 192.168.64.2: Another active host, possibly a client or secondary server.

Basic Network Mapping

- Subnet: 192.168.64.0/24
- Active Hosts: 192.168.64.1, 192.168.64.2
- Services: DNS Service, HTTP Proxy, Unknown service on port 9000

Security Implications

Potential Risks

- DNS Spoofing: Unpatched vulnerabilities in the DNS service can lead to DNS spoofing and cache poisoning, allowing attackers to redirect traffic.
- Data Leakage: Misconfigured HTTP Proxy or unknown services on port 9000 can lead to unauthorized access and data leakage.
- Unauthorized Access: Open ports and services can be exploited by attackers to gain unauthorized access to the network.

Recommendations

- Patch Management: Ensure all software and services are up-to-date with the latest security patches.
- Access Control: Implement strict access controls to limit exposure of

critical services.

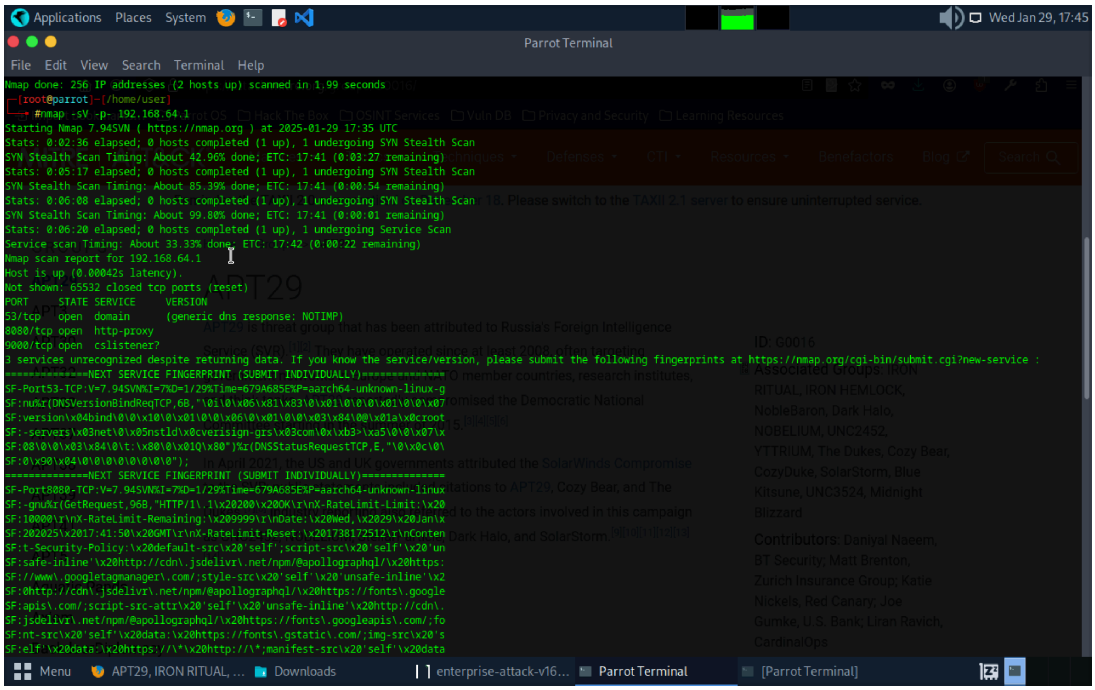
- Network Segmentation: Segment the network to isolate critical assets and reduce the attack surface.
- Regular Scans: Conduct regular vulnerability scans to identify and mitigate new vulnerabilities.
- Service Identification: Identify and document all running services to understand their purpose and security requirements.

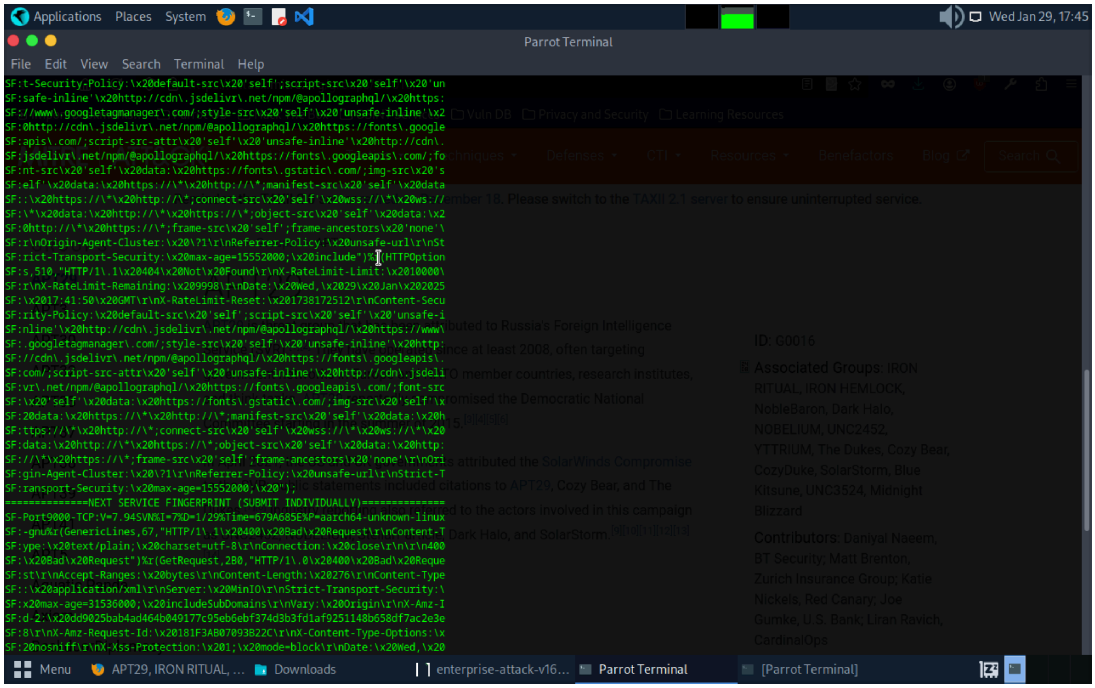
Conclusion

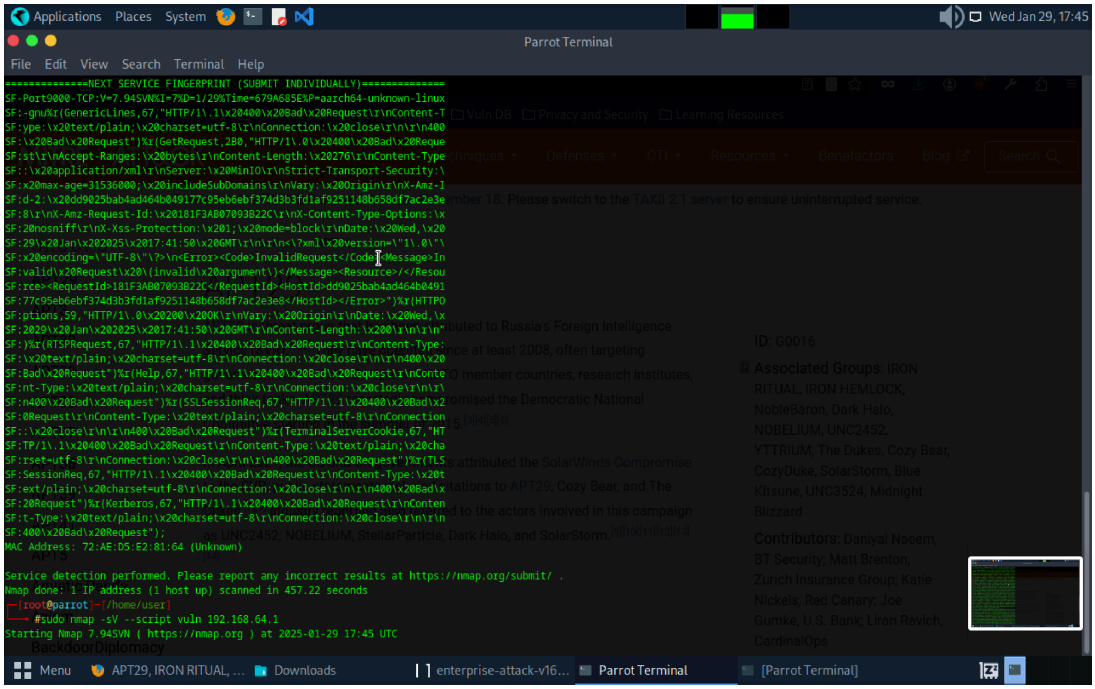
The vulnerability assessment identified several medium-severity vulnerabilities in the target network. Immediate action is recommended to patch vulnerabilities, implement access controls, and conduct regular scans to maintain a secure network environment.

Screenshots

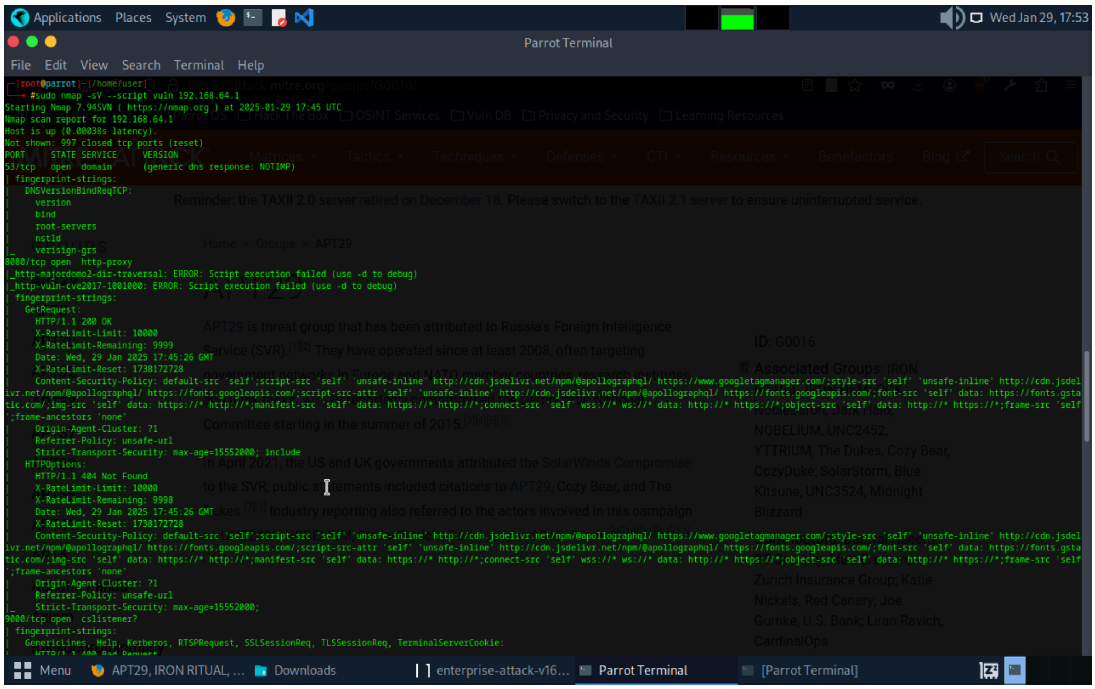
Vulnerability Scan

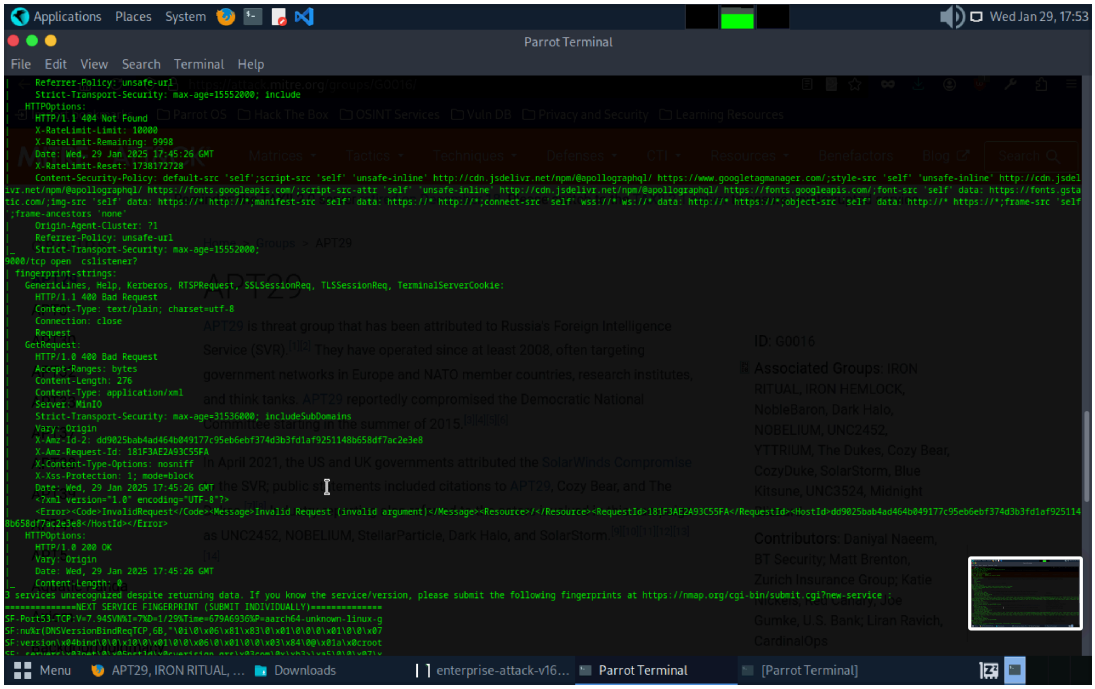


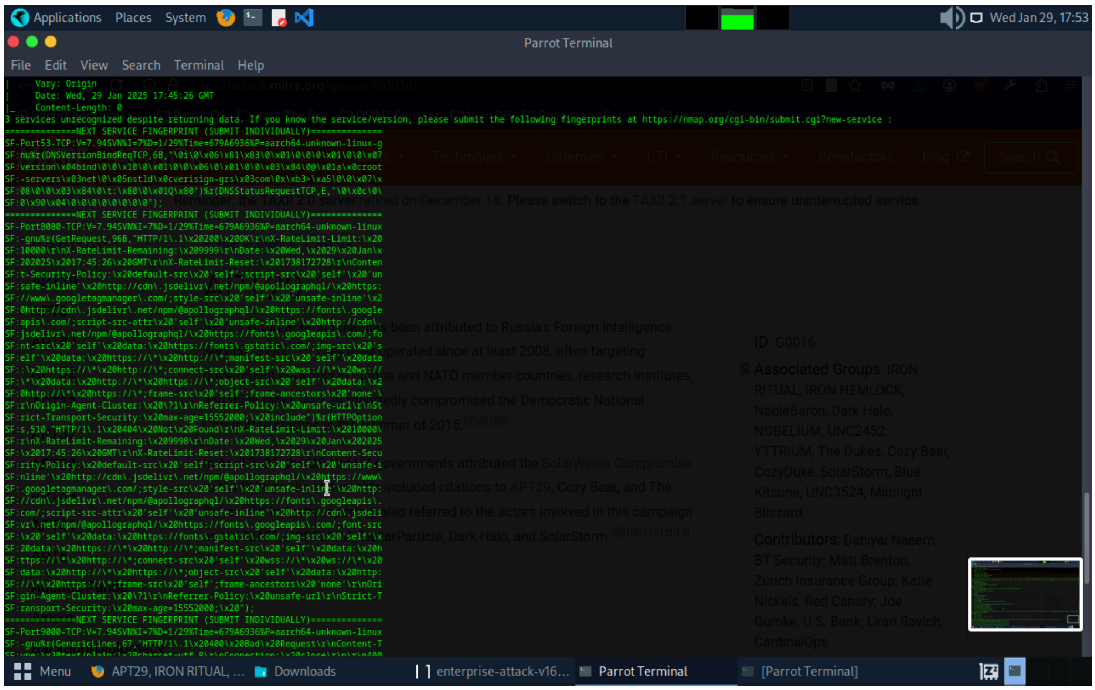

Applications Places System
Wed Jan 29, 17:45
Parrot Terminal
File Edit View Search Terminal Help
SF:t-Security-Policy:\x20default-src\x20'self';script-src\x20'self'\x20'un
SF:safe-inline'\x20http://cdn\.jsdelivr\.net/npm/@apollographql/\x20https:
SF://www\.googletagmanager\.com/;style-src\x20'self'\x20'unsafe-inline'\x2
SF:0http://cdn\.jsdelivr\.net/npm/@apollographql/\x20https://fonts\.google
SF:apis\.com/;script-src-attr\x20'self'\x20'unsafe-inline'\x20http://cdn\.
SF:jsdelivr\.net/npm/@apollographql/\x20https://fonts\.googleapis\.com/;fo
SF:nt-src\x20'self'\x20data:\x20https://fonts\.gstatic\.com/;img-src\x20's
SF:elf'\x20data:\x20https://*\x20http://*;manifest-src\x20'self'\x20data
SF:\x20https://*\x20http://*;connect-src\x20'self'\x20wss://*\x20ws://
SF:*\x20data:\x20http://*\x20https://*;object-src\x20'self'\x20data:\x2
SF:0http://*\x20https://*;frame-src\x20'self';frame-ancestors\x20'none'\
SF:r\nOrigin-Agent-Cluster:\x20\?1\r\nReferrer-Policy:\x20unsafe-url\r\nSt
SF:rict-Transport-Security:\x20max-age=15552000;\x20include")%r(HTTPOption
SF:s,510,"HTTP/1\.1\x20404\x20Not\x20Found\r\nX-RateLimit-Limit:\x2010000\
SF:r\nX-RateLimit-Remaining:\x209998\r\nDate:\x20Wed,\x2029\x20Jan\x202025
SF:\x2017:41:50\x20GMT\r\nX-RateLimit-Reset:\x201738172512\r\nContent-Secu
SF:rity-Policy:\x20default-src\x20'self';script-src\x20'self'\x20'unsafe-i
SF:nline'\x20http://cdn\.jsdelivr\.net/npm/@apollographql/\x20https://www\
SF:.googletagmanager\.com/;style-src\x20'self'\x20'unsafe-inline'\x20http:
SF://cdn\.jsdelivr\.net/npm/@apollographql/\x20https://fonts\.googleapis\.
SF:com/;script-src-attr\x20'self'\x20'unsafe-inline'\x20http://cdn\.jsdeli
SF:vr\.net/npm/@apollographql/\x20https://fonts\.googleapis\.com/;font-src
SF:\x20'self'\x20data:\x20https://fonts\.gstatic\.com/;img-src\x20'self'\x
SF:20data:\x20https://*\x20http://*;manifest-src\x20'self'\x20data:\x20h
SF:ttps://*\x20http://*;connect-src\x20'self'\x20wss://*\x20ws://*\x20
SF:data:\x20http://*\x20https://*;object-src\x20'self'\x20data:\x20http:
SF://*\x20https://*;frame-src\x20'self';frame-ancestors\x20'none'\r\nOri
SF:gin-Agent-Cluster:\x20\?1\r\nReferrer-Policy:\x20unsafe-url\r\nStrict-T
SF:ransport-Security:\x20max-age=15552000;\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9000-TCP:V=7.94SVN%I=7%D=1/29%Time=679A685E%P=aarch64-unknown-linux
SF:-gnu%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(GetRequest,2B0,"HTTP/1\.0\x20400\x20Bad\x20Reque
SF:st\r\nAccept-Ranges:\x20bytes\r\nContent-Length:\x20276\r\nContent-Type
SF::\x20application/xml\r\nServer:\x20MinIO\r\nStrict-Transport-Security:\
SF:x20max-age=31536000;\x20includeSubDomains\r\nVary:\x20Origin\r\nX-Amz-I
SF:d-2:\x20dd9025bab4ad464b049177c95eb6ebf374d3b3fd1af9251148b658df7ac2e3e
SF:8\r\nX-Amz-Request-Id:\x20181F3AB07093B22C\r\nX-Content-Type-Options:\x
SF:20nosniff\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Wed,\x20
Menu
APT29, IRON RITUAL, ...
Downloads
enterprise-attack-v16...
Parrot Terminal
[Parrot Terminal]

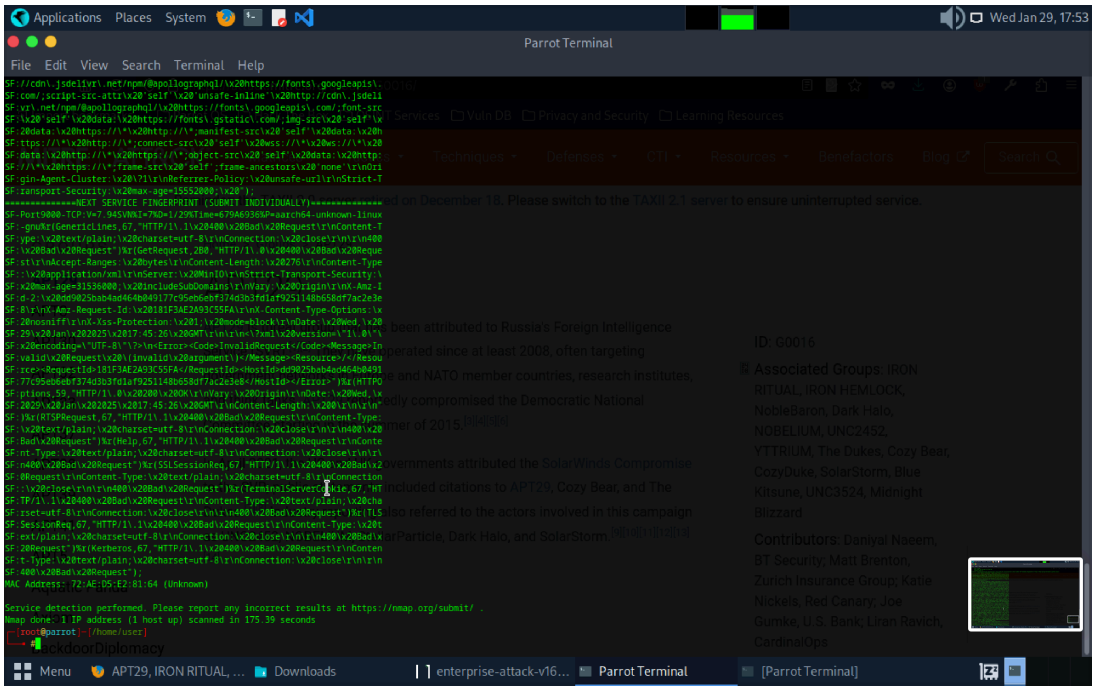

Applications Places System
Wed Jan 29, 17:45
Parrot Terminal
File Edit View Search Terminal Help
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9000-TCP:V=7.94SVN%I=7%D=1/29%Time=679A685E%P=aarch64-unknown-linux
SF:-gnu%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(GetRequest,2B0,"HTTP/1\.0\x20400\x20Bad\x20Reque
SF:st\r\nAccept-Ranges:\x20bytes\r\nContent-Length:\x20276\r\nContent-Type
SF::\x20application/xml\r\nServer:\x20MinIO\r\nStrict-Transport-Security:\
SF:x20max-age=31536000;\x20includeSubDomains\r\nVary:\x20Origin\r\nX-Amz-I
SF:d-2:\x20dd9025bab4ad464b049177c95eb6ebf374d3b3fd1af9251148b658df7ac2e3e
SF:8\r\nX-Amz-Request-Id:\x20181F3AB07093B22C\r\nX-Content-Type-Options:\x
SF:20nosniff\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Wed,\x20
SF:29\x20Jan\x202025\x2017:41:50\x20GMT\r\n\r\n<\?xml\x20version=\"1\.0\"\
SF:x20encoding=\"UTF-8\"\?>\n<Error><Code>InvalidRequest</Code><Message>In
SF:valid\x20Request\x20\(invalid\x20argument\)</Message><Resource>/</Resou
SF:rce><RequestId>181F3AB07093B22C</RequestId><HostId>dd9025bab4ad464b0491
SF:77c95eb6ebf374d3b3fd1af9251148b658df7ac2e3e8</HostId></Error>")%r(HTTPO
SF:ptions,59,"HTTP/1\.0\x20200\x20OK\r\nVary:\x20Origin\r\nDate:\x20Wed,\x
SF:2029\x20Jan\x202025\x2017:41:50\x20GMT\r\nContent-Length:\x200\r\n\r\n"
SF:)%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:
SF:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20
SF:Bad\x20Request")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConte
SF:nt-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\
SF:n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection
SF::\x20close\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TLS
SF:SessionReq,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(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n
SF:400\x20Bad\x20Request");
MAC Address: 72:AE:D5:E2:81:64 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 457.22 seconds
┌──(root@parrot)-[/home/user]
└─# sudo nmap -sV --script vuln 192.168.64.1
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-29 17:45 UTC
Menu
APT29, IRON RITUAL, ...
Downloads
enterprise-attack-v16...
Parrot Terminal
[Parrot Terminal]


Applications Places System
Wed Jan 29, 17:53
Parrot Terminal
File Edit View Search Terminal Help
#sudo nmap -sV --script vuln 192.168.64.1
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-29 17:45 UTC
Nmap scan report for 192.168.64.1
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: NOTIMP)
| fingerprint-strings:
| DNSVersionBindReqTCP:
| version
| bind
| root-servers
| nstld
| verisign-grs
8080/tcp open http-proxy
| http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
| http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
| GetRequest:
| HTTP/1.1 200 OK
| X-RateLimit-Limit: 10000
| X-RateLimit-Remaining: 9999
| Date: Wed, 29 Jan 2025 17:45:26 GMT
| X-RateLimit-Reset: 1738172728
| Content-Security-Policy: default-src 'self';script-src 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://www.googletagmanager.com/;style-src 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://fonts.googleapis.com/;script-src-attr 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://fonts.googleapis.com/;font-src 'self' data: https://fonts.gstatic.com/;img-src 'self' data: https://* http://*;manifest-src 'self' data: https://* http://*;connect-src 'self' wss://* ws://* data: http://* https://*;object-src 'self' data: http://* https://*;frame-src 'self';frame-ancestors 'none'
| Origin-Agent-Cluster: ?1
| Referrer-Policy: unsafe-url
| Strict-Transport-Security: max-age=15552000; include
| HTTPOptions:
| HTTP/1.1 404 Not Found
| X-RateLimit-Limit: 10000
| X-RateLimit-Remaining: 9998
| Date: Wed, 29 Jan 2025 17:45:26 GMT
| X-RateLimit-Reset: 1738172728
| Content-Security-Policy: default-src 'self';script-src 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://www.googletagmanager.com/;style-src 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://fonts.googleapis.com/;script-src-attr 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://fonts.googleapis.com/;font-src 'self' data: https://fonts.gstatic.com/;img-src 'self' data: https://* http://*;manifest-src 'self' data: https://* http://*;connect-src 'self' wss://* ws://* data: http://* https://*;object-src 'self' data: http://* https://*;frame-src 'self';frame-ancestors 'none'
| Origin-Agent-Cluster: ?1
| Referrer-Policy: unsafe-url
|_ Strict-Transport-Security: max-age=15552000;
9000/tcp open cslistener?
| fingerprint-strings:
| GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
| HTTP/1.1 400 Bad Request
Menu
APT29, IRON RITUAL, ...
Downloads
enterprise-attack-v16...
Parrot Terminal
[Parrot Terminal]


Applications Places System
Wed Jan 29, 17:53
Parrot Terminal
File Edit View Search Terminal Help
Referrer-Policy: unsafe-url
Strict-Transport-Security: max-age=15552000; include
HTTPOptions:
HTTP/1.1 404 Not Found
X-RateLimit-Limit: 10000
X-RateLimit-Remaining: 9998
Date: Wed, 29 Jan 2025 17:45:26 GMT
X-RateLimit-Reset: 1738172728
Content-Security-Policy: default-src 'self';script-src 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://www.googletagmanager.com/;style-src 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://fonts.googleapis.com/;script-src-attr 'self' 'unsafe-inline' http://cdn.jsdelivr.net/npm/@apollographql/ https://fonts.googleapis.com/;font-src 'self' data: https://fonts.gstatic.com/;img-src 'self' data: https://* http://*;manifest-src 'self' data: https://* http://*;connect-src 'self' wss://* ws://* data: http://* https://*;object-src 'self' data: http://* https://*;frame-src 'self';frame-ancestors 'none'
Origin-Agent-Cluster: ?1
Referrer-Policy: unsafe-url
Strict-Transport-Security: max-age=15552000;
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: 181F3AE2A93C55FA
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Date: Wed, 29 Jan 2025 17:45:26 GMT
<?xml version="1.0" encoding="UTF-8"?>
<Error><Code>InvalidRequest</Code><Message>Invalid Request (invalid argument)</Message><Resource>/</Resource><RequestId>181F3AE2A93C55FA</RequestId><HostId>dd9025bab4ad464b049177c95eb6ebf374d3b3fd1af925114
8b658df7ac2e3e8</HostId></Error>
HTTPOptions:
HTTP/1.0 200 OK
Vary: Origin
Date: Wed, 29 Jan 2025 17:45:26 GMT
Content-Length: 0
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.94SVN%I=7%D=1/29%Time=679A6936%P=aarch64-unknown-linux-g
SF:nu%r(DNSVersionBindReqTCP,6B,"\0i\0\x06\x81\x83\0\x01\0\0\0\0\x01\0\0\x07
SF:version\x04bind\0\0\x10\0\x01\0\0\x06\0\x01\0\0\x83\x84\0@\x01a\x0Croot
Menu
APT29, IRON RITUAL, ...
Downloads
enterprise-attack-v16...
Parrot Terminal
[Parrot Terminal]





Asset Discovery Scan

Appendix

Nmap Commands Used

- **sudo nmap -sV --script vuln 192.168.64.1**
- **sudo nmap -sn 192.168.64.0/24**

Additional Information

- Operating System: Parrot OS
- Tools: Nmap

This report provides a comprehensive overview of the vulnerability assessment conducted on the target network. The findings and recommendations should be used to enhance the security posture of the network.