Comprehensive Vulnerability Assessment and Risk Management 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. Additionally, the report includes risk management practices, identification of critical risks, treatment recommendations, mitigation steps, and a risk monitoring procedure.

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

Risk Management

Identification of Critical Risks

Critical Risk 1: Unauthorized Access via HTTP Proxy (Port 8080)

- Description: The HTTP Proxy service running on port 8080 is susceptible to unauthorized access, which can lead to data leakage and potential misuse of the proxy for malicious activities.
- Impact: High. Unauthorized access can result in data breaches, loss of sensitive information, and potential legal implications.
- Likelihood: Medium. The service is accessible and could be targeted by

attackers.
- Risk Level: High (Impact: High, Likelihood: Medium)

Critical Risk 2: Unknown Service on Port 9000

- Description: The service running on port 9000 is unidentified and could be a custom service (cslistener). This unknown service poses a risk of unauthorized access and data leakage.
- Impact: High. Unauthorized access to an unknown service can lead to data breaches and potential exploitation of the service for malicious activities.
- Likelihood: Medium. The service is accessible and could be targeted by attackers.
- Risk Level: High (Impact: High, Likelihood: Medium)

Treatment Recommendations

Unauthorized Access via HTTP Proxy (Port 8080)

- Recommendation: Implement strict access controls to limit exposure of the HTTP Proxy service.
- Mitigation Steps:
  1. Access Control: Restrict access to the HTTP Proxy service to trusted IPs only.
  2. Authentication: Implement strong authentication mechanisms to ensure only authorized users can access the service.
  3. Monitoring: Set up logging and monitoring to detect and respond to unauthorized access attempts.

Unknown Service on Port 9000

- Recommendation: Identify the service and ensure proper configuration and access controls.
- Mitigation Steps:
  1. Service Identification: Conduct further investigation to identify the service running on port 9000.
  2. Access Control: Implement strict access controls to limit exposure of the service.
  3. Configuration Review: Ensure the service is configured securely and patched regularly.
  4. Monitoring: Set up logging and monitoring to detect and respond to unauthorized access attempts.

Risk Monitoring Procedure

Procedure: Regular Vulnerability Scans and Access Log Review

- Objective: To track identified risks and ensure timely detection and response to potential security incidents.
- Frequency: Monthly
- Steps:
  1. Vulnerability Scan: Conduct a vulnerability scan using Nmap to

identify new vulnerabilities and changes in the network.
2. Access Log Review: Review access logs for the HTTP Proxy service and the unknown service on port 9000 to detect unauthorized access attempts.
3. Incident Response: Investigate and respond to any detected security incidents promptly.
4. Reporting: Document the findings of the vulnerability scan and access log review, and report to the relevant stakeholders.
5. Patch Management: Ensure all software and services are up-to-date with the latest security patches.

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.

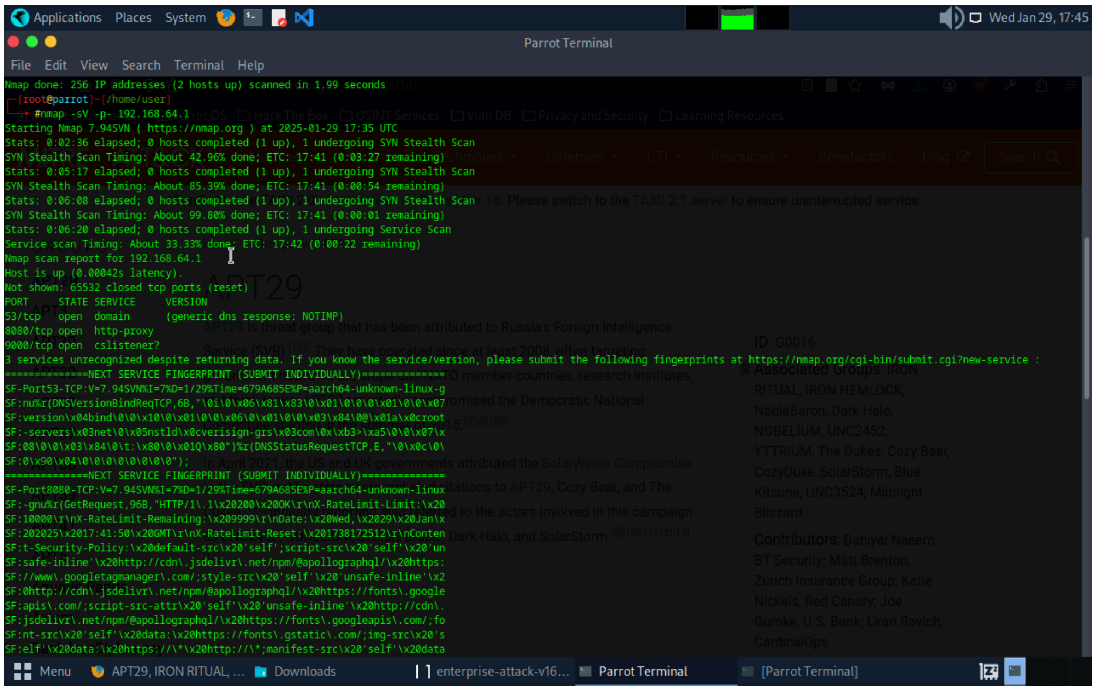
Recommendations

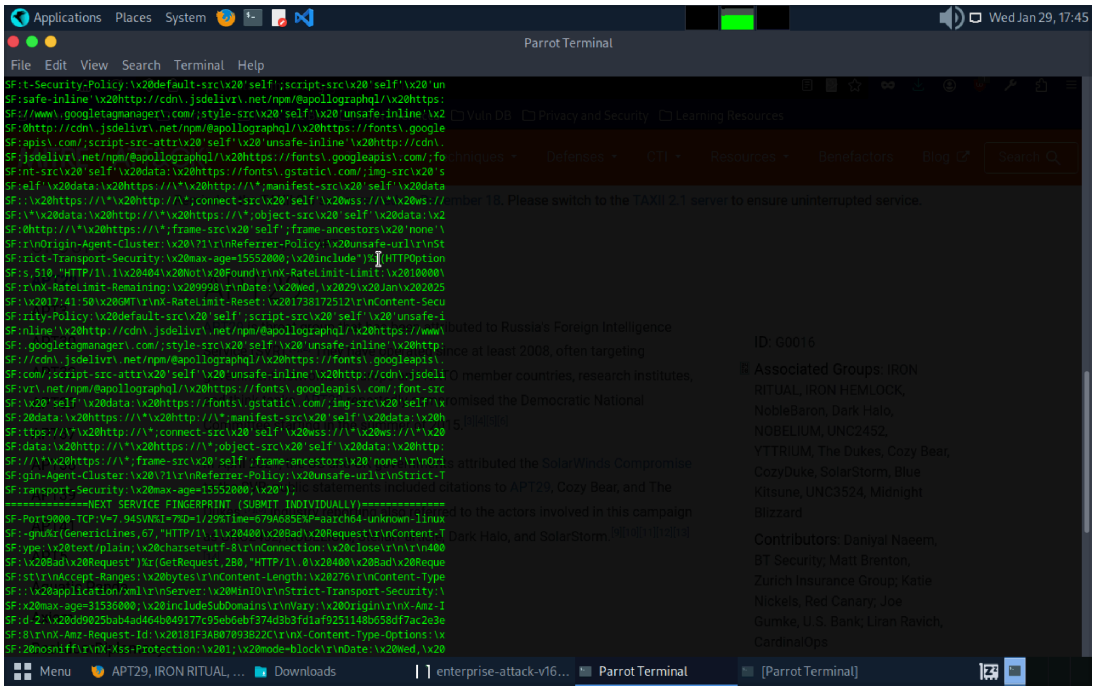
- Patch Management: Ensure all software and services are up-to-date with the latest security patches.
- Access Control: Implement strict access controls to limit exposure of critical services.
- Network Segmentation: Segment the network to isolate critical assets and reduce the attack surface.
- Regular 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.

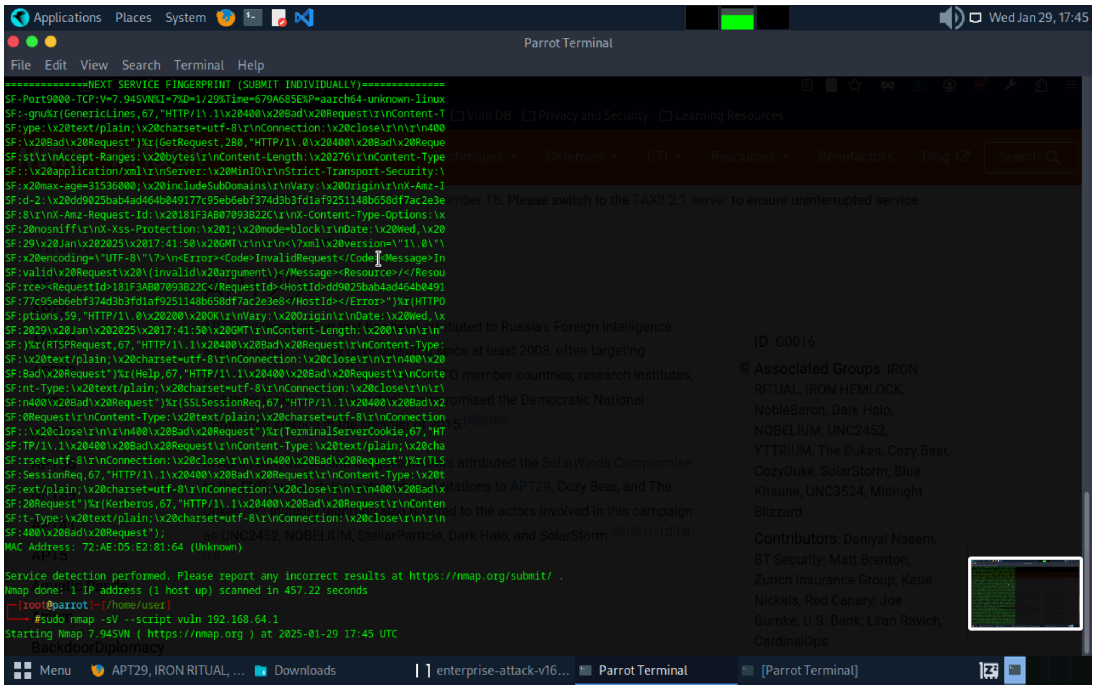
Conclusion

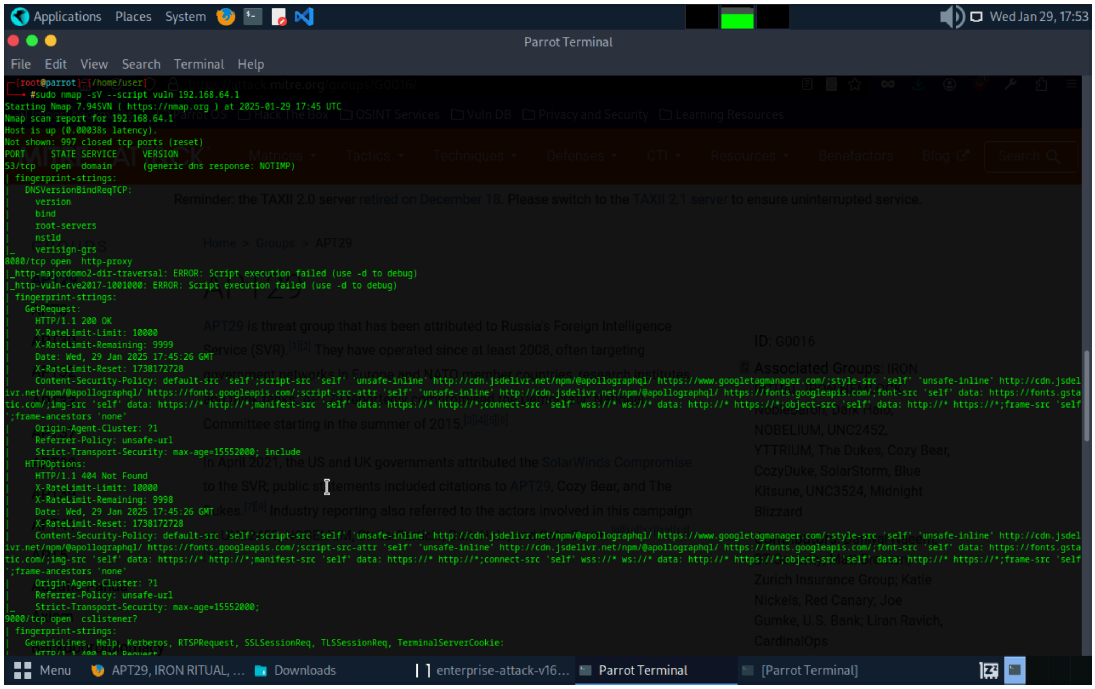
The vulnerability assessment identified several medium and high-severity vulnerabilities in the target network. Immediate action is recommended to patch vulnerabilities, implement access controls, and conduct regular scans to maintain a secure network environment. The risk management procedures outlined in this report will help track identified risks and ensure timely detection and response to potential security incidents.

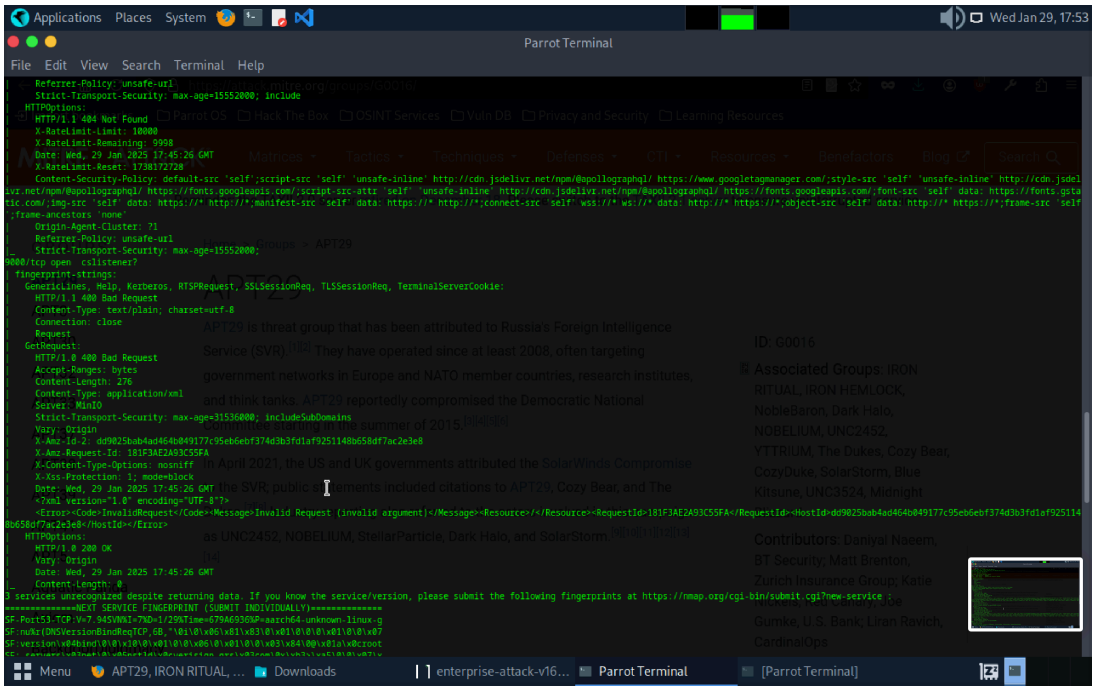
Screenshots

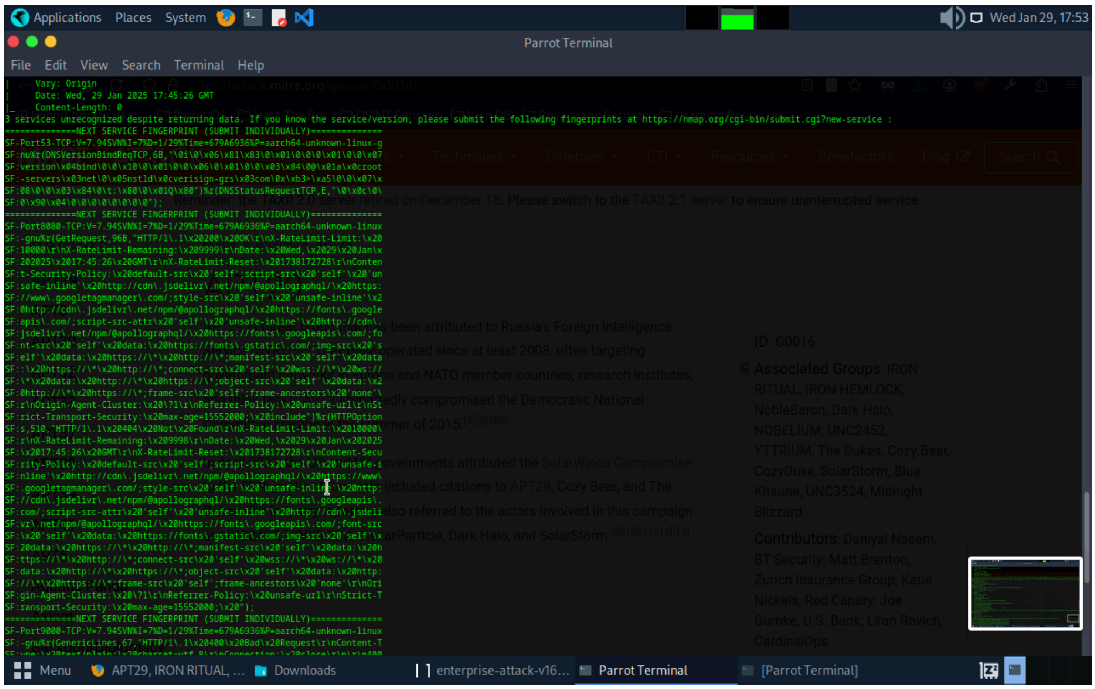

Applications Places System
Wed Jan 29, 17:45
Parrot Terminal
File Edit View Search Terminal Help
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.99 seconds
[root@parrot]~[/home/user]
#nmap -sV -p- 192.168.64.1
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-29 17:35 UTC
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.96% done; ETC: 17:41 (0:03:27 remaining)
Stats: 0:05:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.39% done; ETC: 17:41 (0:00:54 remaining)
Stats: 0:06:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.80% done; ETC: 17:41 (0:00:01 remaining)
Stats: 0:06:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 17:42 (0:00:22 remaining)
Nmap scan report for 192.168.64.1
Host is up (0.00042s latency).
Not shown: 65532 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: NOTIMP)
8080/tcp open http-proxy
9000/tcp open cslistener?
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=679A685E%P=aarch64-unknown-linux-g
SF:nu%r(DNSVersionBindReqTCP,6B,"\0i\0\x06\x81\x83\0\x01\0\0\0\x01\0\0\x07
SF:version\x04bind\0\0\x10\0\x01\0\0\x06\0\x01\0\0\x03\x84\0@\x01a\x0croot
SF:-servers\x03net\0\x05nstld\x0cverisign-grs\x03com\0x\xb3>\xa5\0\0\x07\x
SF:08\0\0\x03\x84\0t:\x80\0\x01Q\x80")%r(DNSStatusRequestTCP,E,"\0\x0c\0\
SF:0\x90\x04\0\0\0\0\0\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.94SVN%I=7%D=1/29%Time=679A685E%P=aarch64-unknown-linux
SF:-gnu%r(GetRequest,96B,"HTTP/1\.1\x20200\x20OK\r\nX-RateLimit-Limit:\x20
SF:10000\r\nX-RateLimit-Remaining:\x209999\r\nDate:\x20Wed,\x2029\x20Jan\x
SF:202025\x2017:41:50\x20GMT\r\nX-RateLimit-Reset:\x201738172512\r\nConten
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
Menu APT29, IRON RITUAL, ... Downloads enterprise-attack-v16... Parrot Terminal [Parrot Terminal]

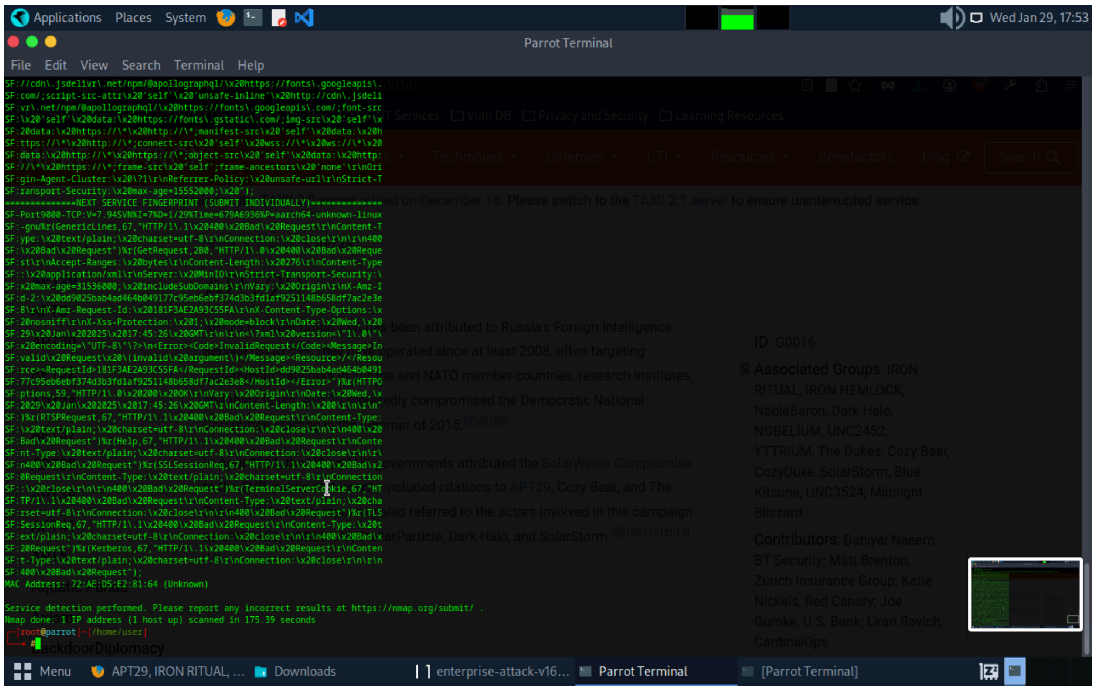

Applications Places System
Wed Jan 29, 17:45
Parrot Terminal
File Edit View Search Terminal Help
SF:t-Security-Policy:\x20default-src\x20'self';script-src\x20'self'\x20'un
SF:safe-inline'\x20http://cdn\.jsdelivr\.net/npm/@apollographql/\x20https:
SF://www\.googletagmanager\.com/;style-src\x20'self'\x20'unsafe-inline'\x2
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:\x2181F3AB07093B22C\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,280,"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
[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
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
| nstid
|_ version-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: 1730172728
| 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: 1730172728
| 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;
9080/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
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
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
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.39 seconds
[root@parrot]~[/home/user]
#
Menu
APT29, IRON RITUAL, ...
Downloads
enterprise-attack-v16...
Parrot Terminal
[Parrot Terminal]