Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	Hauser Security
Contact Name	Devin Duesler
Contact Title	SOC Analyst

Document History

Version	Date	Author(s)	Comments
001			

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

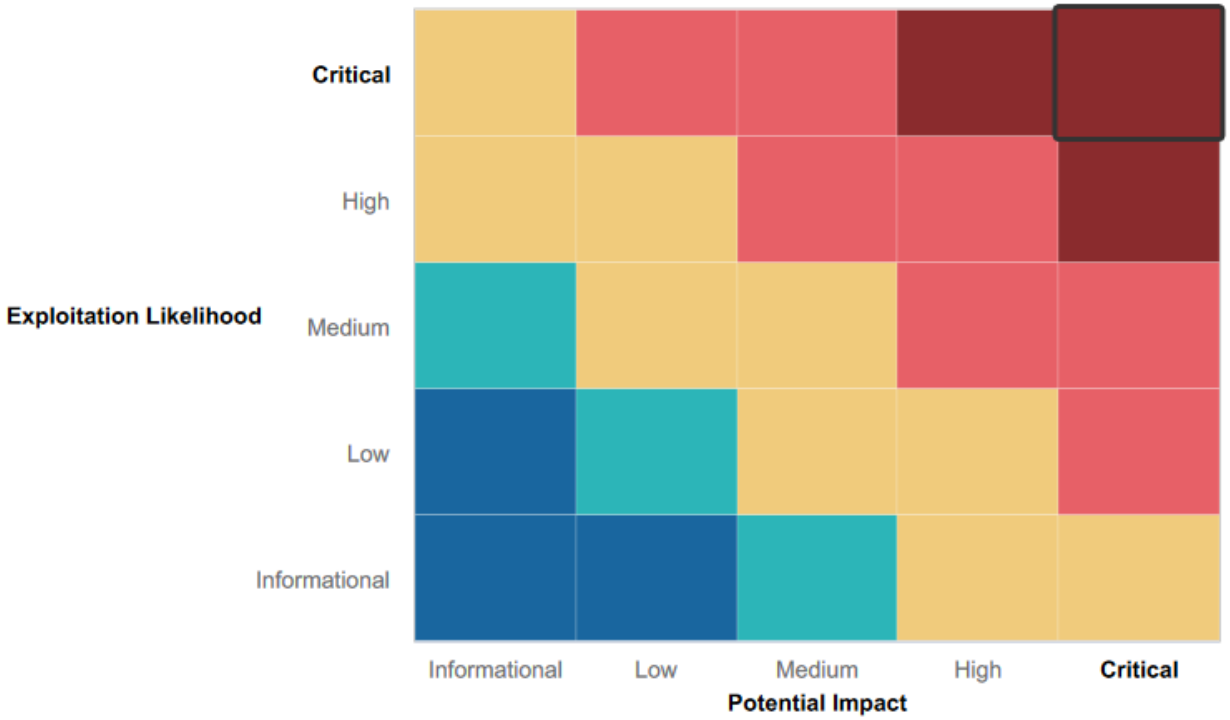
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Strong Login and Password credentials used for website access.
- Several features allow for cross site scripting protection on web app.
- Protection found for several known windows and linux server exploits

Summary of Weaknesses

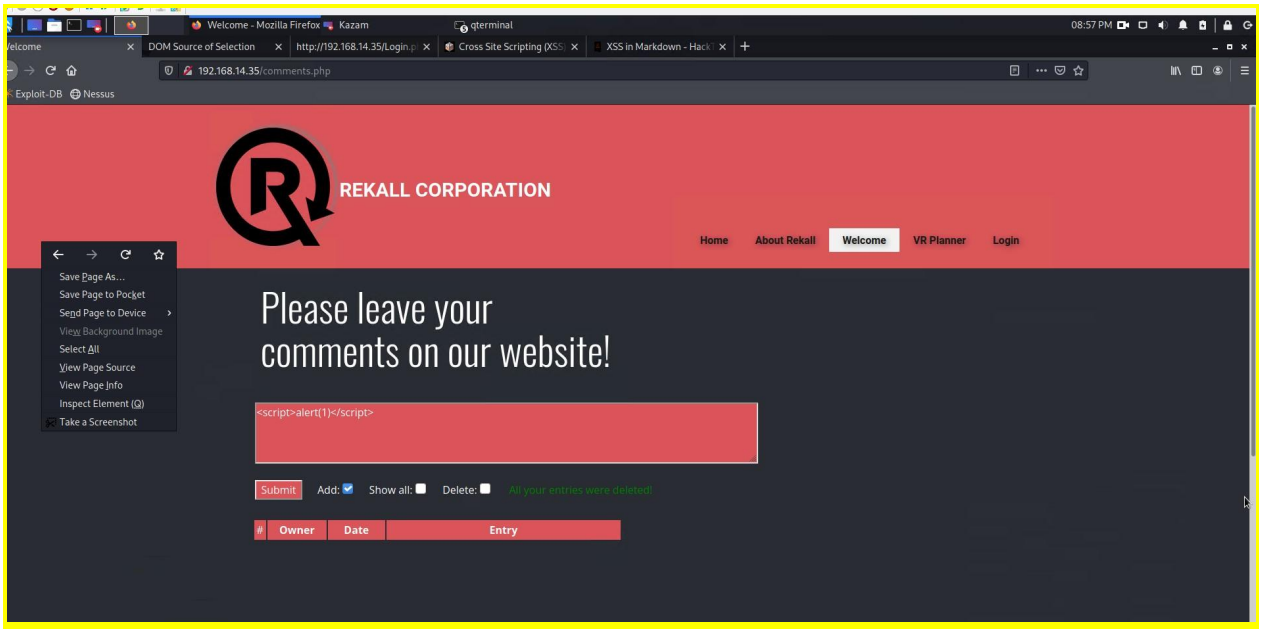
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

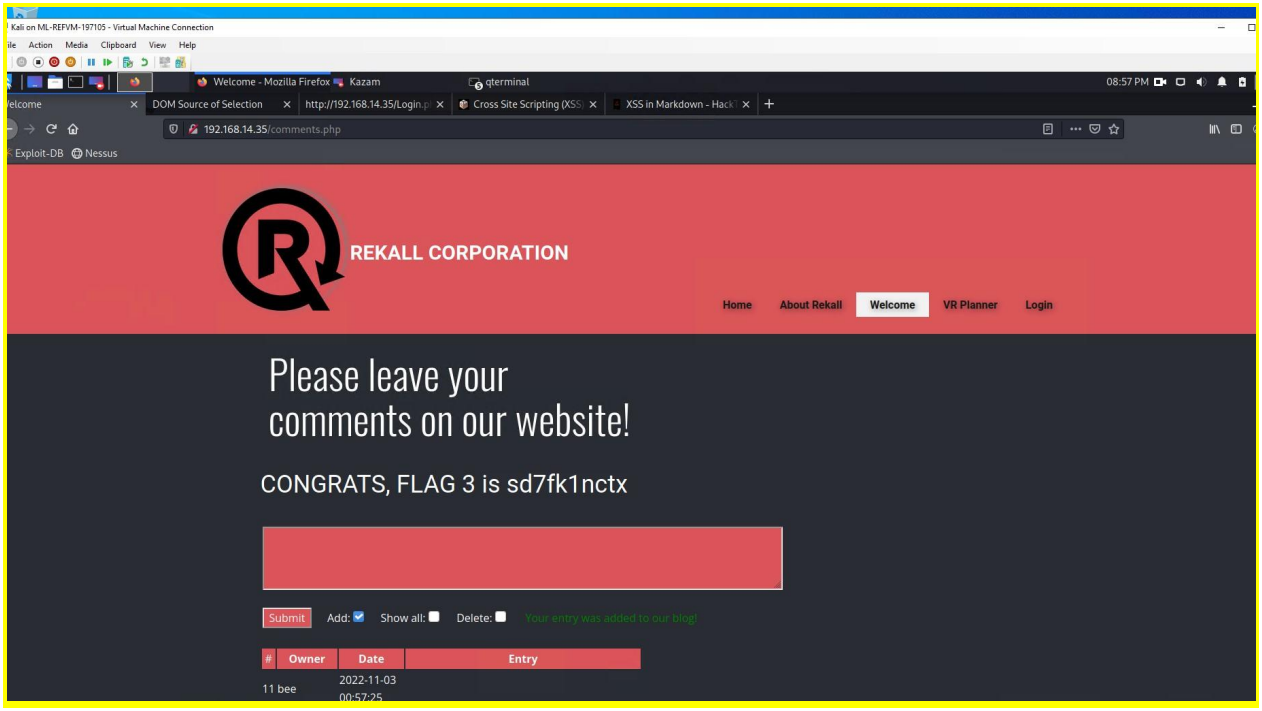
- Web site name entry and comment box tools vulnerable to Cross Site Scripting
- Login information found on login screen and github repository for site.
- Both Windows and Linux web servers were found to be exploitable

Executive Summary

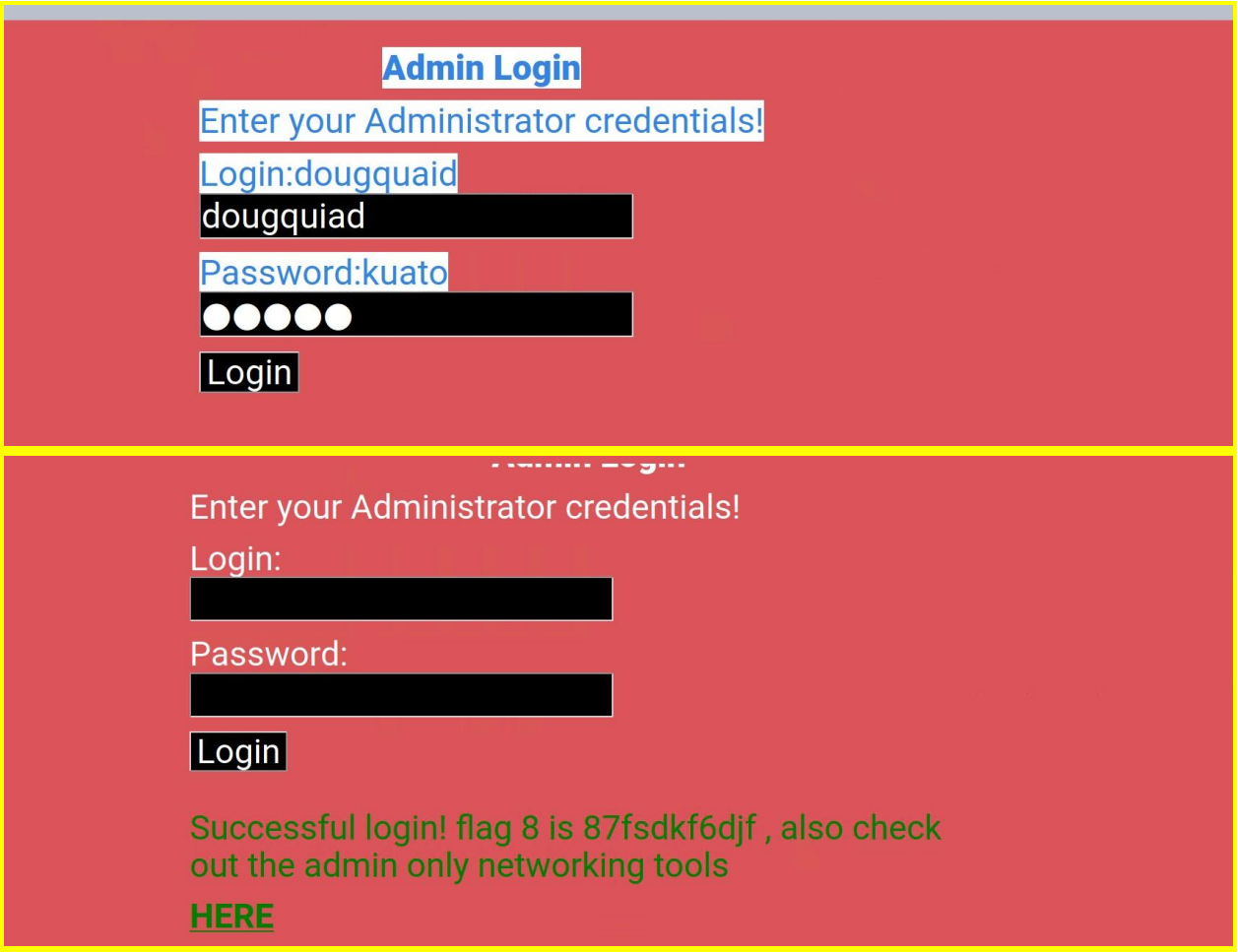
Upon initial inspection of the website, an examination of possible scripting exploits began. The first exploit discovered with the name input tool, an input of a simple script yielded information regarding the file structure of the web applications server.

The next vulnerability located on the site was discovered by using the comment box tool on the website. Similarly to the name input tool listed previously, use of a simple script yielded web application server information that can be exploited to gain information/access to the site's data.



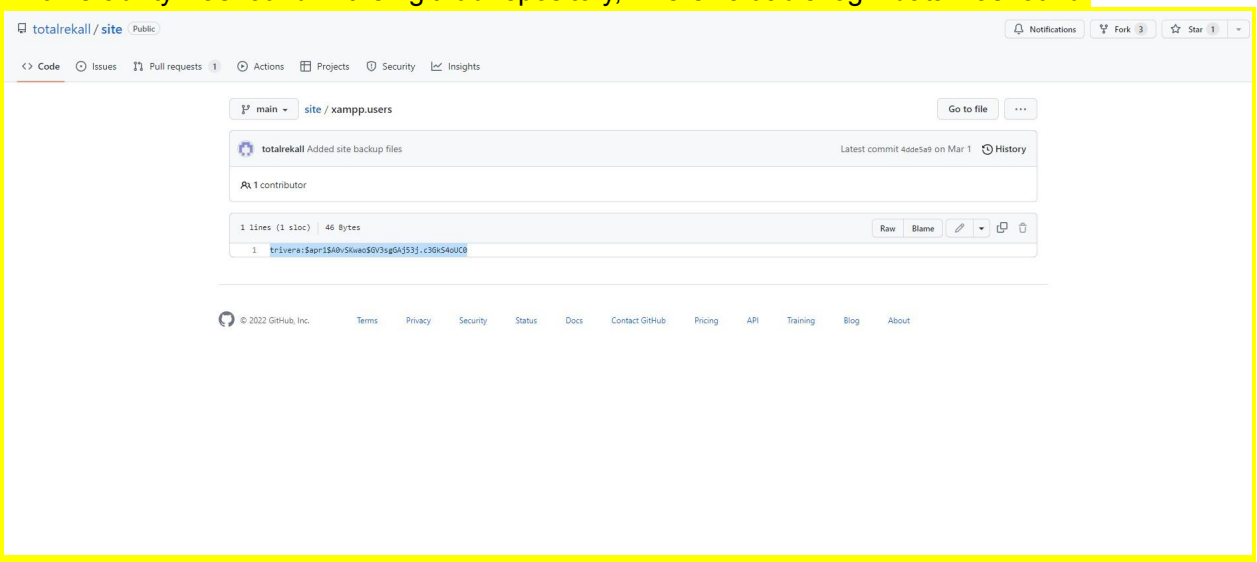


An additional vulnerability was found when examining the login input fields. When highlighting the details on the webpage, login credentials are found for the user, Doug Quaid.



Once found, the credentials were entered in and confirmed to provide a successful log in.

A vulnerability was found in their github repository, where valuable login data was found.



Before going further, some additional reconnaissance was completed, data was gathered on the domain by pulling a domain dossier and a whois record to gain additional information for Rekall.

Domain Whois record

Queried **whois.nic.xyz** with "**totalrekall.xyz**"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2022-03-11T15:12:32.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2023-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2022-11-03T22:43:25.0Z <<<
```

Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-02-02T19:16:19Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2023-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s83zhakasd flag1
Registrant City: Atlanta
```

Domain Dossier Investigate domains and IP addresses

domain or IP address: totalrekall.xyz

☑ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan go

user: anonymous [104.58.114.73]
balance: 48 units
log in | account info

CentralOps.net

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

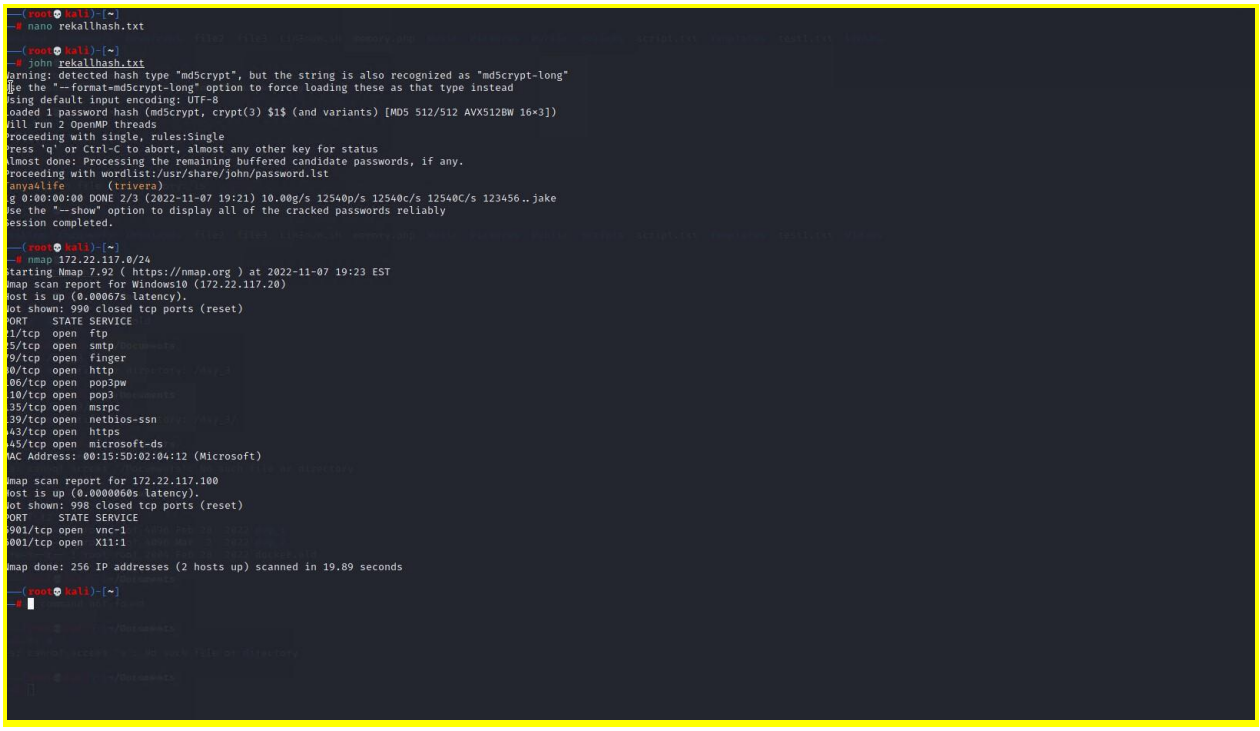
canonical name **totalrekall.xyz.**
aliases
addresses **34.102.136.180**

Domain Whois record

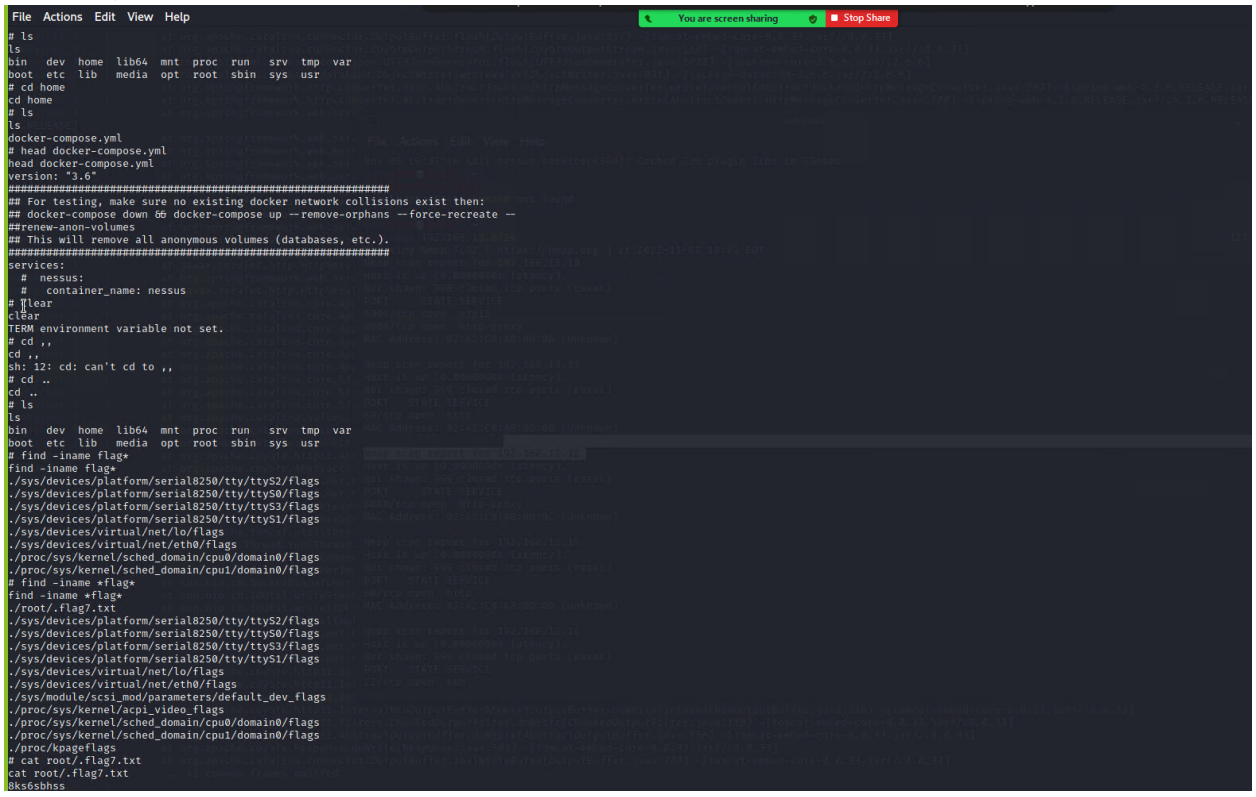
Queried **whois.nic.xyz** with "**totalrekall.xyz**"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2022-03-11T15:12:32.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2023-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2022-11-03T22:43:25.0Z <<<
```

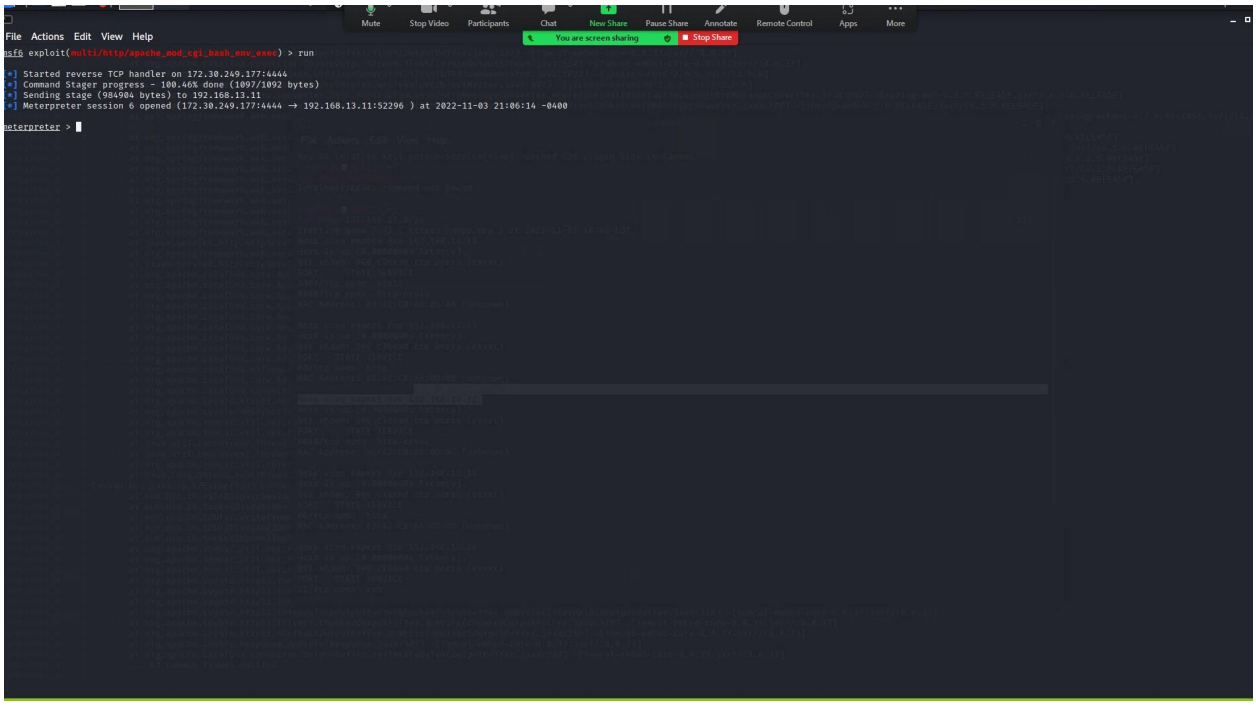
Additionally, an NMAP scan was completed to see what ports were open and what services were using them.

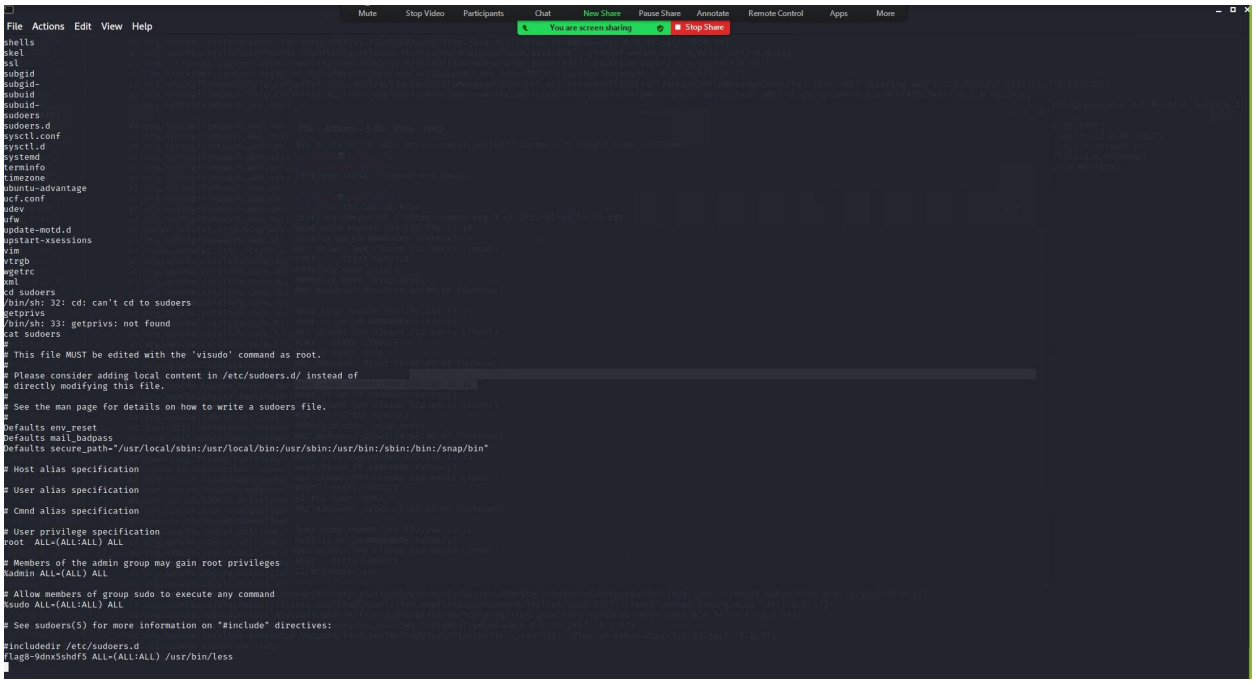


Using Metasploit, a RCE exploit was used to access the linux web server running the site, revealing potentially valuable data.



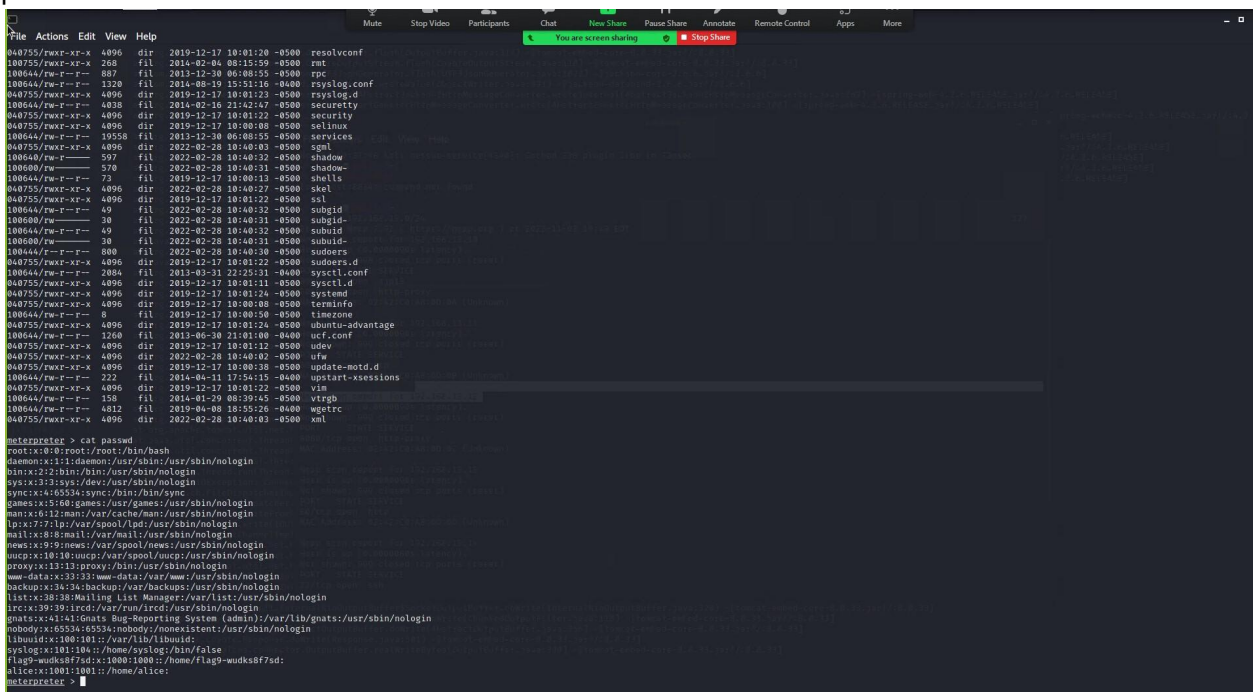
From there, metasploit was used to run a separate RCE exploit and a Meterpreter shell was created.



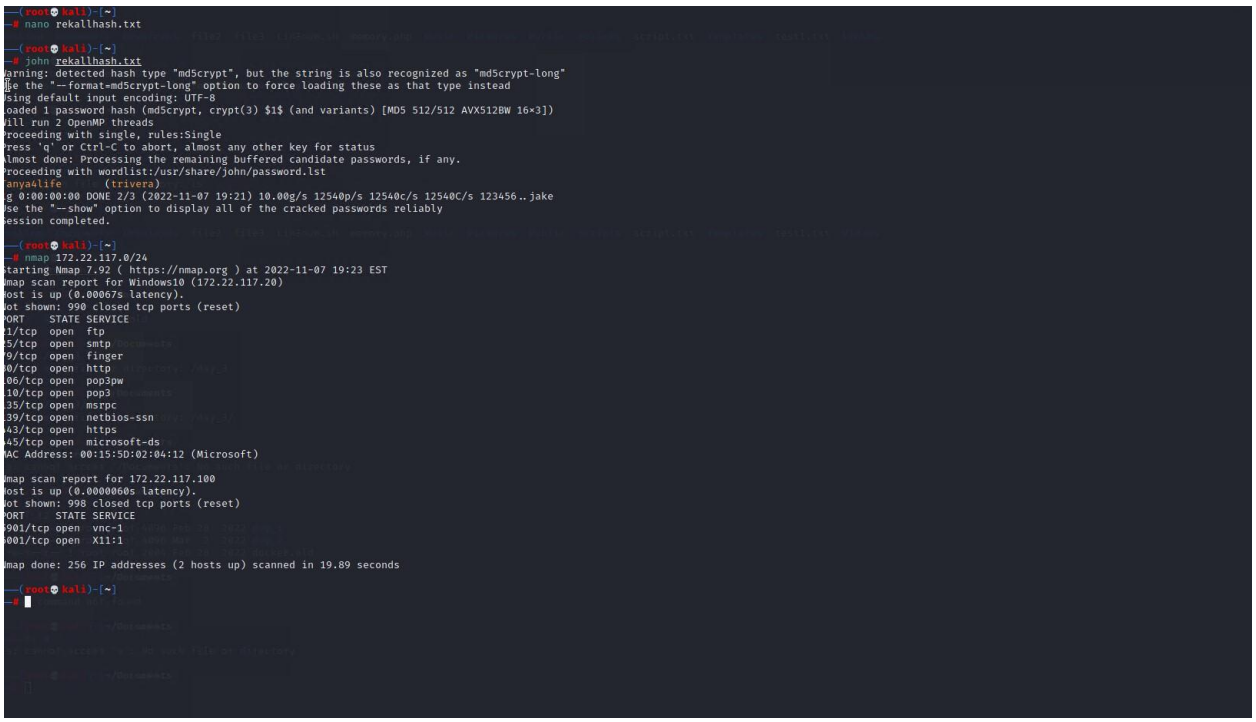


From here, it was discovered that the “SUDOERS” directory was not actually a directory, but actually a file revealing sensitive information once a concatenate command was done on the file. Additionally, while this shell was open, access was found to the etc/shadow folder, providing username and

password information.

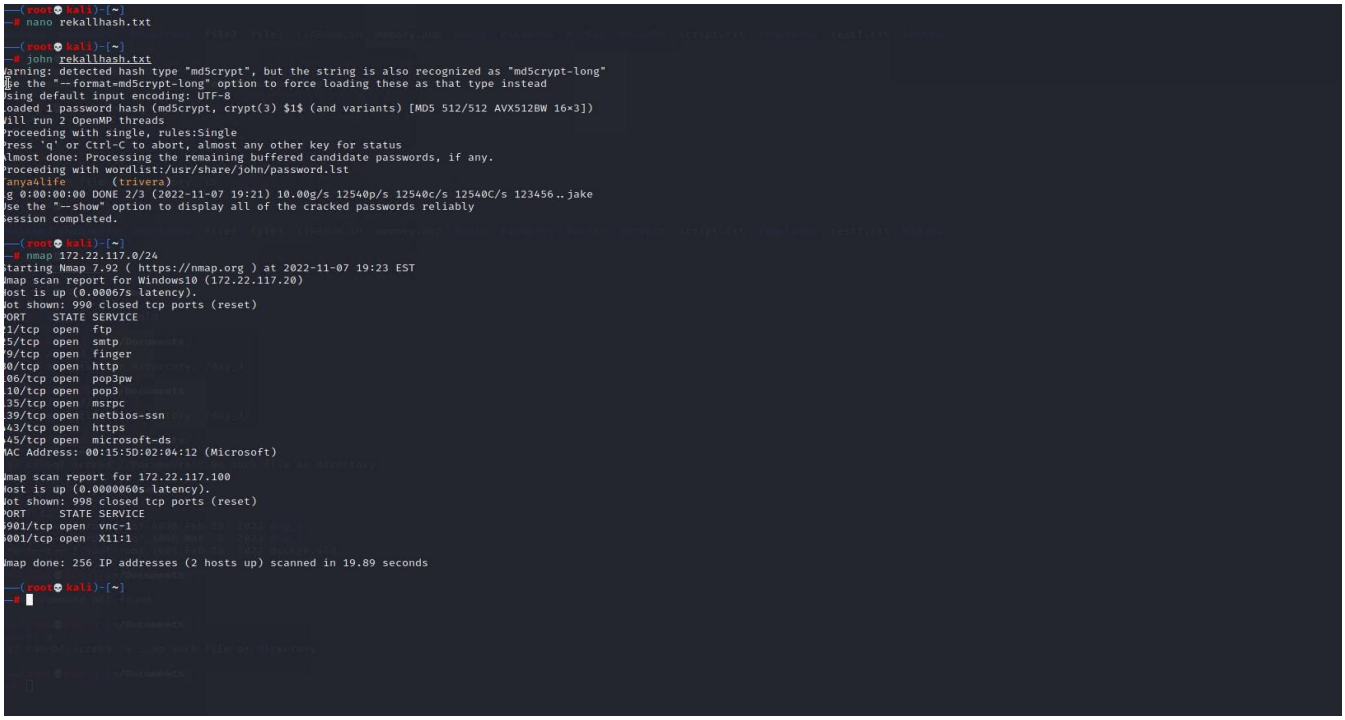


From Here, Recon began on the Windows web app server, and an nmap scan was completed.

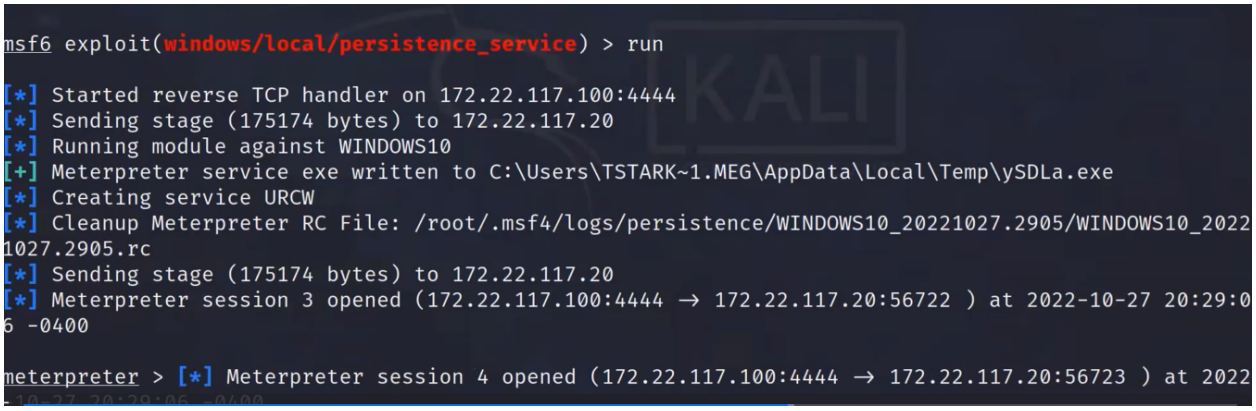


Seeing a POP3 survive, running a pop3 exploit was run via metasploit to gain access to the system. Once the password hash was found, an exploit was found to get the password hash and then was

cracked with john the ripper.



Additionally, using metasploit, an exploit was found allowing for persistence on the windows server.



Summary Vulnerability Overview

Vulnerability	Severity
Name entry tool vulnerable to scripting attacks on web app.	CRITICAL
Comment Box tool vulnerable to scripting attacks on web app.	CRITICAL
Linux server susceptible to RCE exploits	CRITICAL
Windows Server susceptible to pop3 exploit.	CRITICAL
Login Credentials found in text on their web app.	CRITICAL
Persistence exploit successfully performed on windows server	HIGH
Login info found in github repository	HIGH

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20, 192.168.10.13
Ports	21.80,443

Exploitation Risk	Total
Critical	6
High	1
Medium	0
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	Name entry tool vulnerable to scripting attacks on web app.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**CRITICAL**
Description	basic cross site scripting revealed server information
Images	Pages 10-11
Affected Hosts	192.168.10.13
Remediation	Use cross site scripting blacking letters by blocking likely search terms.

Vulnerability 2	Findings

Title	Post comment tool vulnerable to scripting attacks on web app.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	CRITICAL
Description	basic cross site scripting revealed server information
Images	Pages 10-11
Affected Hosts	192.168.10.13
Remediation	Use cross site scripting blacking letters by blocking likely search terms.

Vulnerability 3	Findings
Title	Linux Web App server susceptible to RCE exploits
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	CRITICAL
Description	Remote code execution allowed for Command and Control of linux server/
Images	Pages 13,14,15
Affected Hosts	177.22.117.20
Remediation	Updating to most current linux kernel, enhanced monitoring of server activity.

Vulnerability 4	Findings
Title	Windows Server susceptible to pop3 exploit.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	CRITICAL
Description	SL Mail Windows exploit allows for access to system.
Images	Pages 16 and 17
Affected Hosts	192.168.10.13
Remediation	Update to most updated version of SL Mail,create a lockout if attempted passwords are over the length needed to exploit same,

Vulnerability 5	Findings
Title	User's login in credentials found on web app log in page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	CRITICAL
Description	When page text is highlighted, login credentials are found
Images	page 12
Affected Hosts	177.22.117.20
Remediation	Remove text from the site.

Vulnerability 6	Findings
Title	Login information found in github repository.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	HIGH
Description	Details on user's login information found in github repository
Images	Page 12
Affected Hosts	177.22.117.20
Remediation	Remove from repository.

Vulnerability 7	Findings
Title	Persistence exploit performed successfully
Type (Web app / Linux OS / WIndows OS)	Windows Server
Risk Rating	HIGH
Description	A persistence exploit was enabled on
Images	page 17
Affected Hosts	192.168.10.13
Remediation	Use windows enhanced mitigation toolkit, update windows to most recent version.