Vulnerability Overview

Vulnerability	Severity
Apache Struts Exploit (CVE-2019-14287)--	Critical
SLMail Service Exploit Port 110	Critical
Drupal CVE 2019-6340 on Port 80–	Critical
Apache Tomcat Exploit	Critical
Privilege Escalation via CVE-2019-14287–	Critical
SQL Injection–	Critical
Weak Password Policies–	High
Brute Force Attack	High
Sensitive Data Exposure	Critical
Command Injection–	High
Exposed Administrative Credentials in Plain Text–	High
Open Port 80 with Website Access–	High
Public Exposure of User Credentials in GitHub Repository–	High
Exposed WHOIS Documentation and TXT/DNS Records–	High
LLMNR Protocol Weaknesses	Medium
Insecure File Transfers due to Open Port 21	Medium
Robots.txt File Exposure	Medium
XSS Reflected	Medium
XSS Stored	Medium
Directory Traversal	High

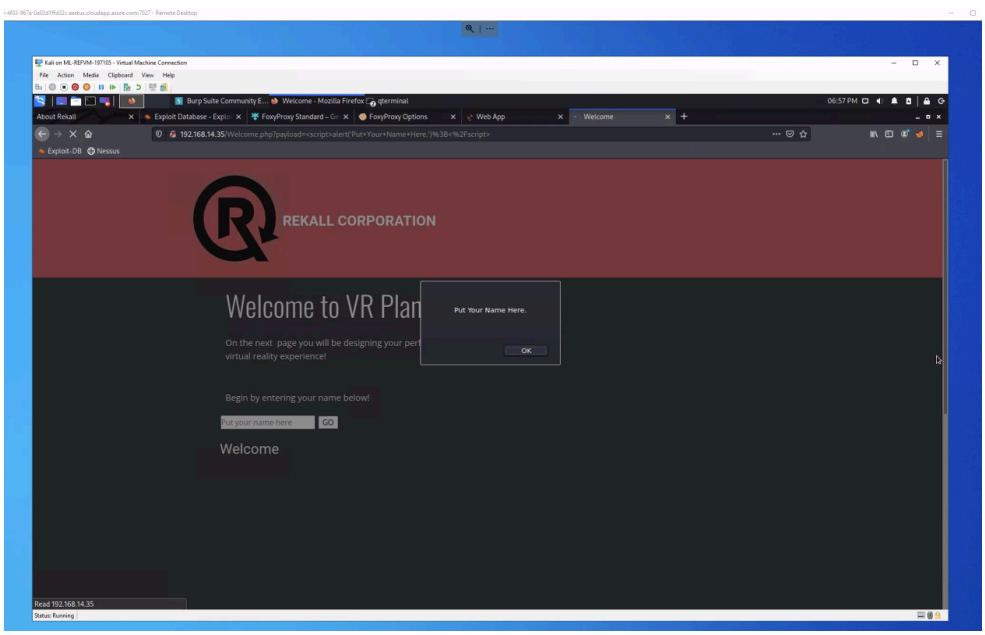
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	10
Ports	5

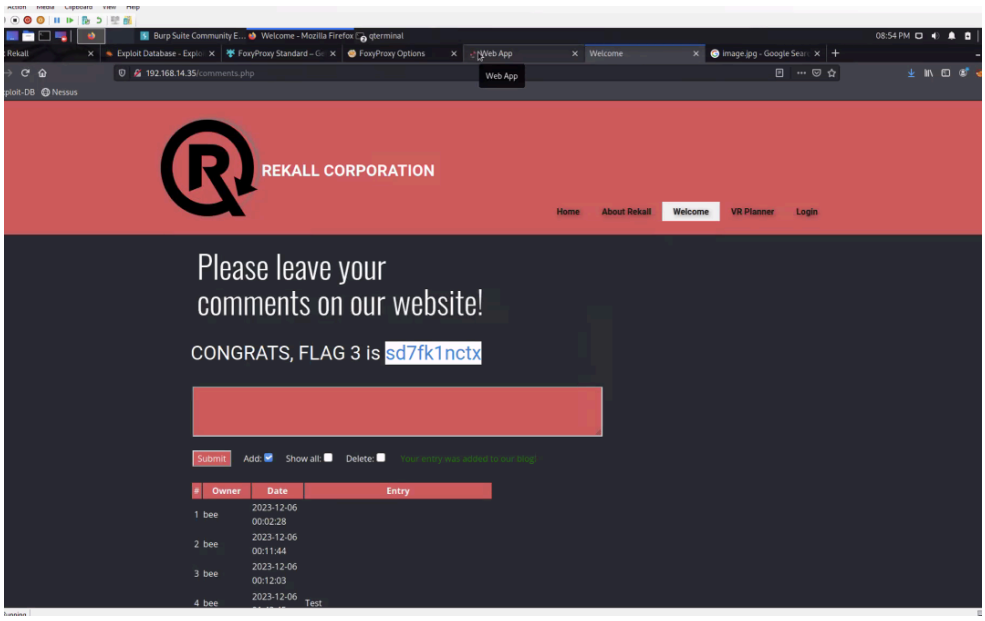
Exploitation Risk	Total
Critical	7

High	8
Medium	5
Low	0

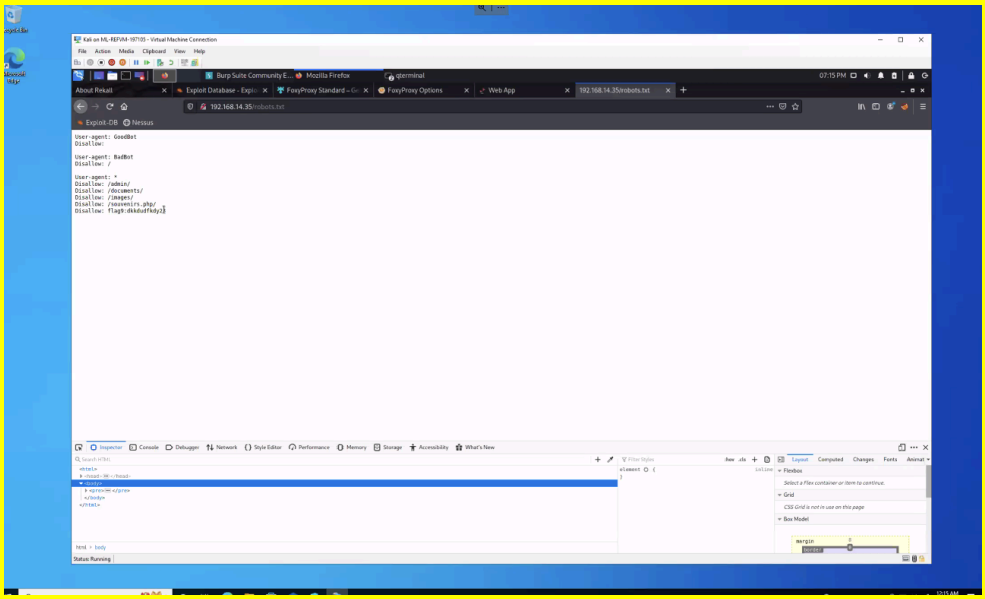
Vulnerability Findings

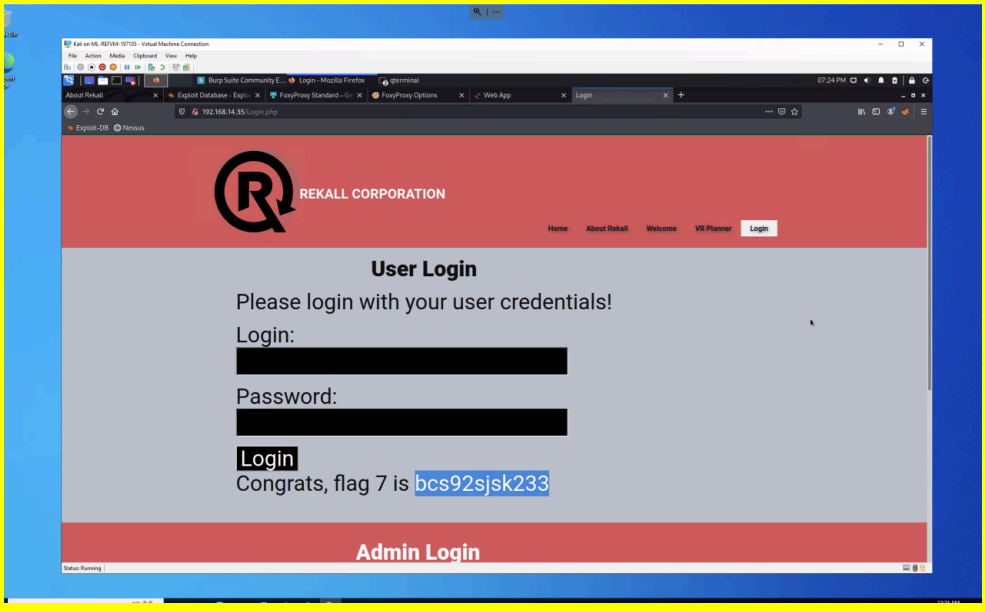
Vulnerability 1	Findings
Title	XSS Refelected
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Malicious script reflected on home page
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App

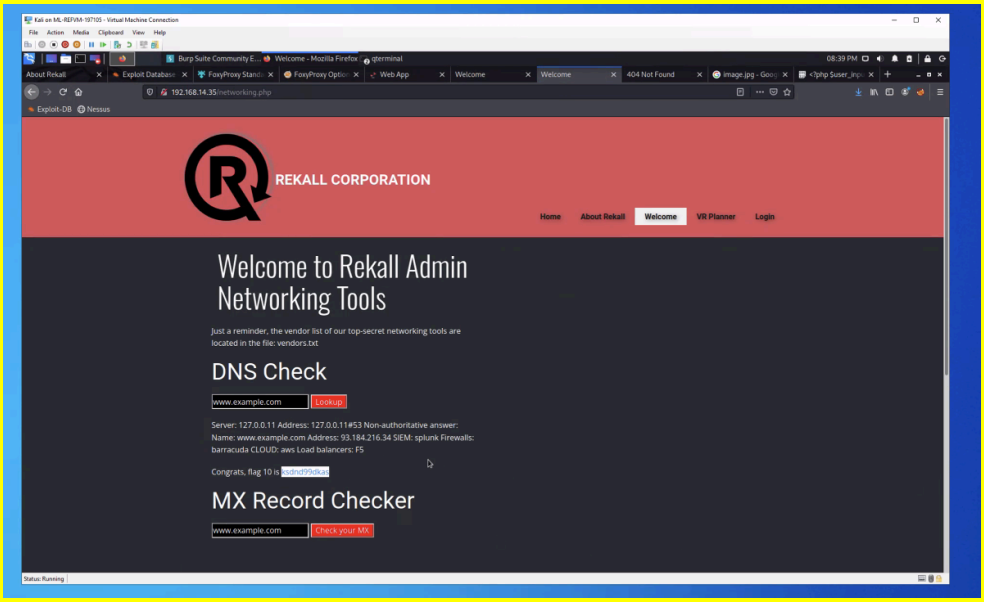
Risk Rating	Medium
Description	Comments.php directory allows user to input scripts/paylods into the the stored data fields
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 3	Findings
Title	Robots.txt File Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Sensitive Information stored in the Robots.txt file

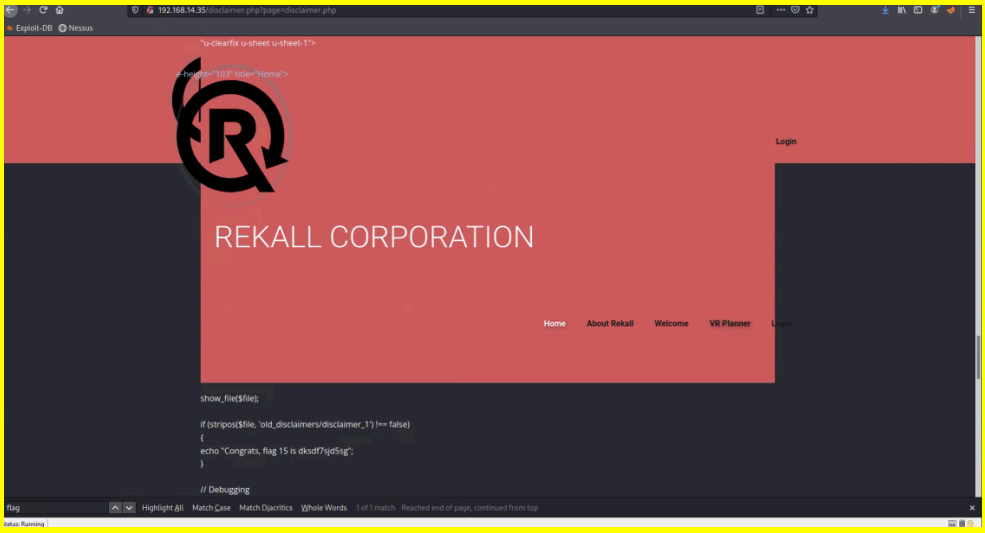
Images	
Affected Hosts	192.168.14.35
Remediation	Examine the robots.txt file to ensure it doesn't reveal sensitive information about the website's structure or directories

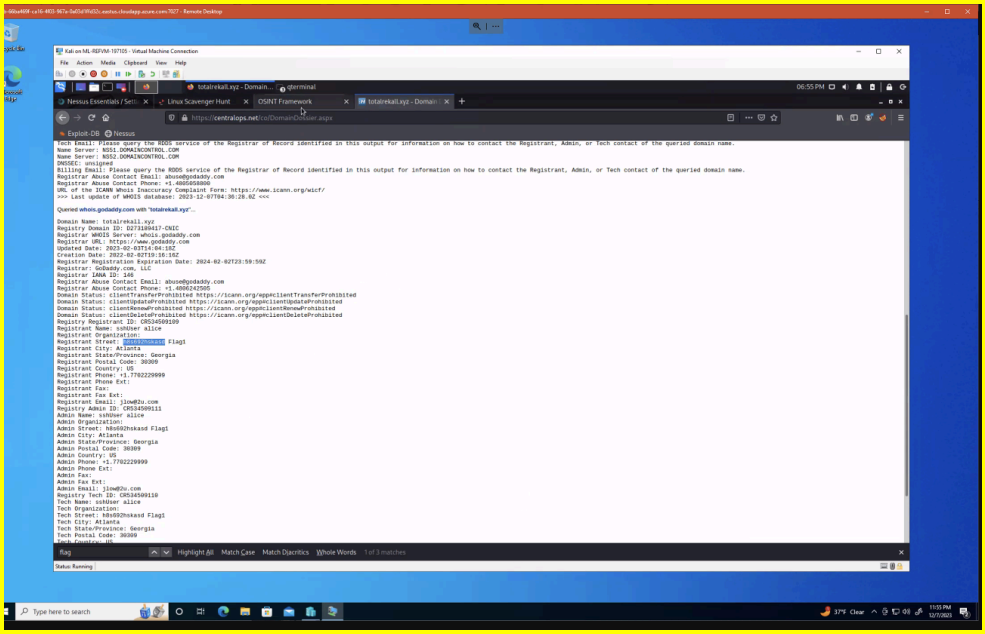
Vulnerability 4	**Findings**
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Inputting SQL query ‘ OR ‘1’=’1 displays sensitive information
Images	

Affected Hosts	192.168.14.35
Remediation	Validate and Santize Input

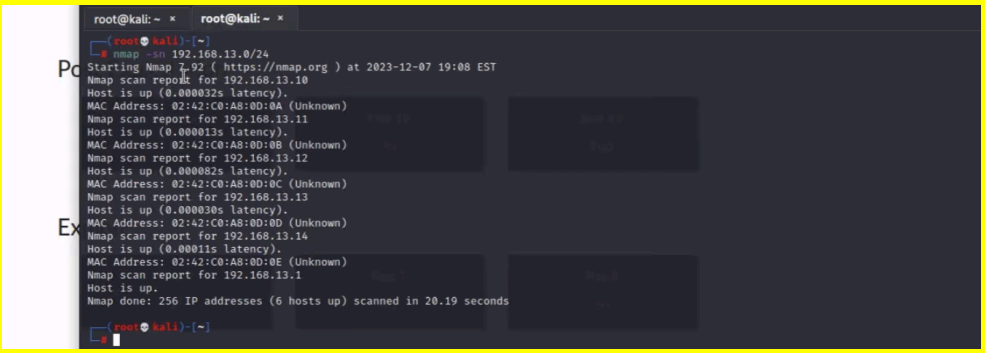
Vulnerability 5	**Findings**
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Injecting commands to view files and structure. Able to view sensitive files via commands inside DNS scheck search bar
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitization:

Vulnerability 6	**Findings**
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Was able to view directory through command injection on DNS Search input. Then used directory traversal to view .php disclaimer file

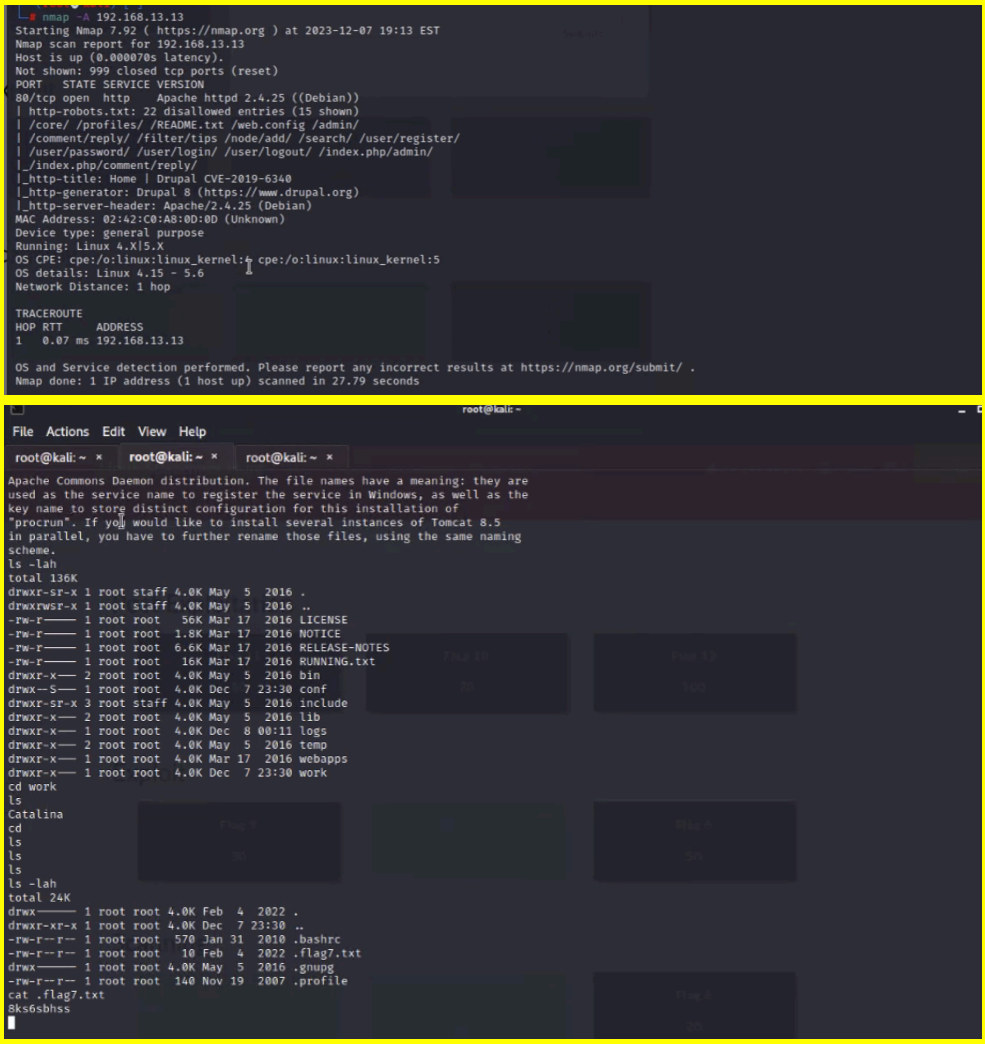
Images	
Affected Hosts	192.168.14.35
Remediation	Limit File access, Least Privilege Principle, Input Validation

Vulnerability 8	**Findings**
Title	Exposed WHOIS Documentation and TXT/DNS Records
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Was able to find sensitive information in the WHOIS and TXT/DNS Record
Images	
Affected Hosts	

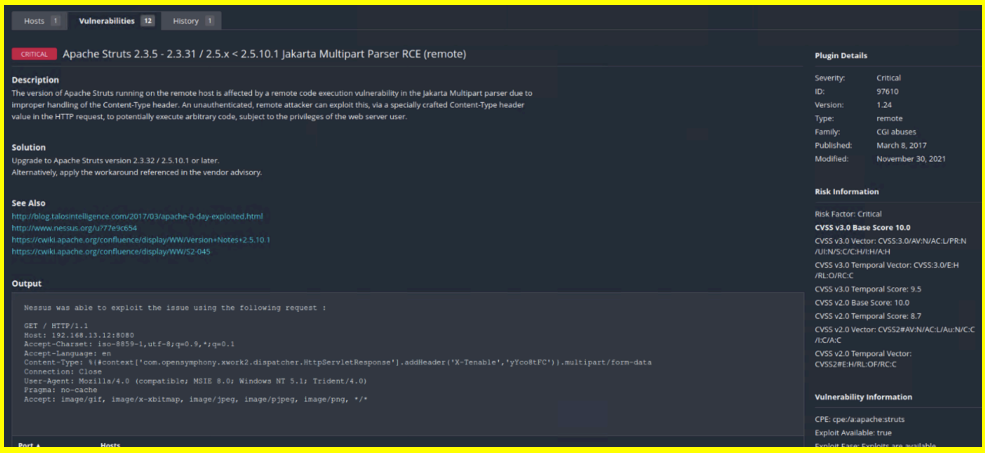
Remediation	Review and Restrict Public Information. Use Domain Privacy Services

Vulnerability 9	Findings
Title	NMAP Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	NMAP Scan against 192.168.13.0/24. Resulted in 6 available hosts
Images	
Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Block IP scanning from unauthorized users

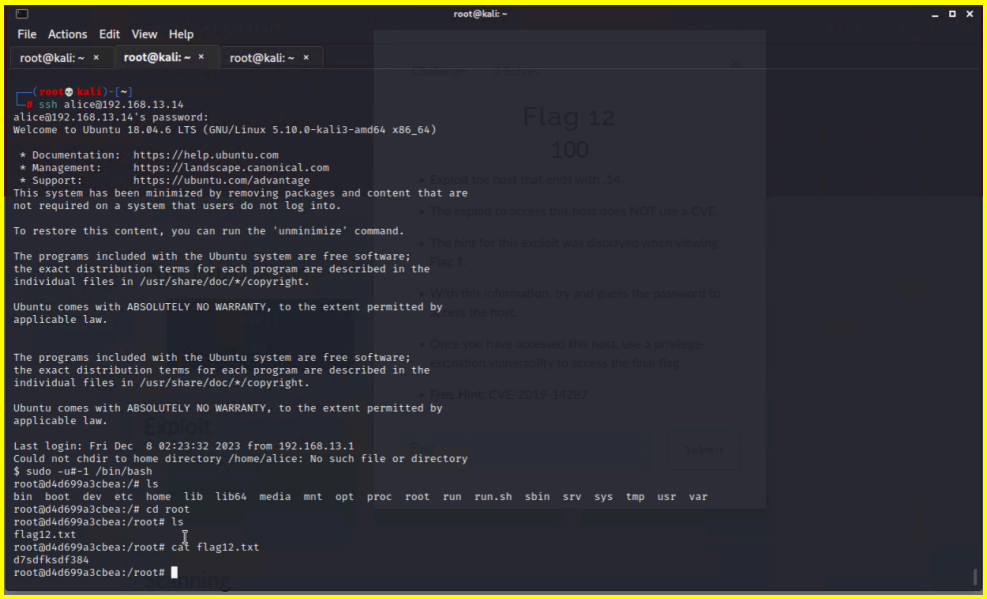
Vulnerability 10	Findings
Title	Drupal CVE 2019-6340 on Port 80
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used Aggressive NMAP scan -A and discovered Drupal running.

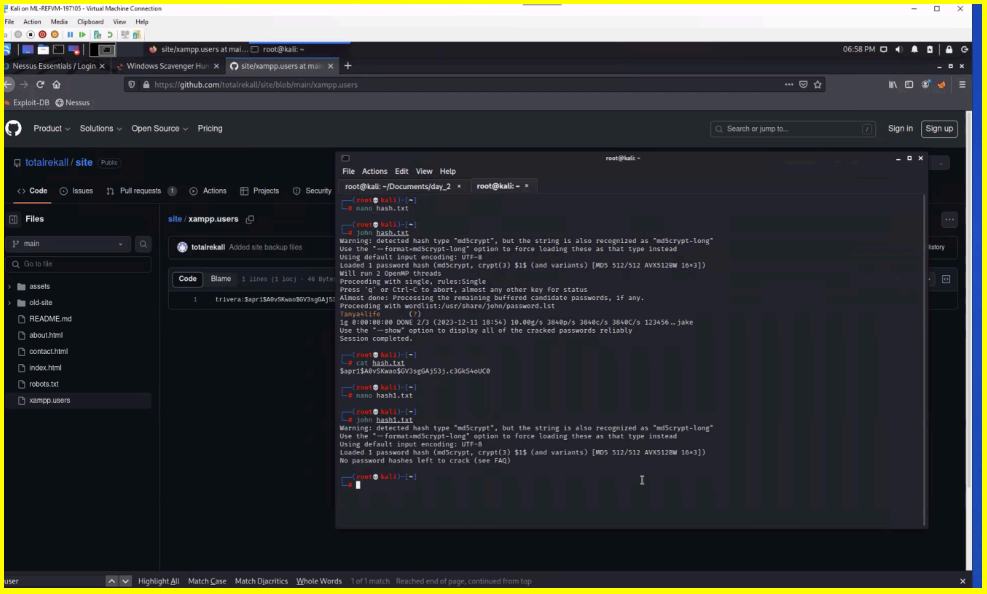
Images	
Affected Hosts	192.168.13.13
Remediation	Apply Patches, Review Drupal Configs and Secure Port 80

Vulnerability 11	Findings
Title	Apache Struts Exploit (CVE-2019-14287)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Scanned 192.168.13.12 using Nessus. Revealed Apache Struts Exploit (CVE-2019-14287). Used metasploit to gain access using exploit

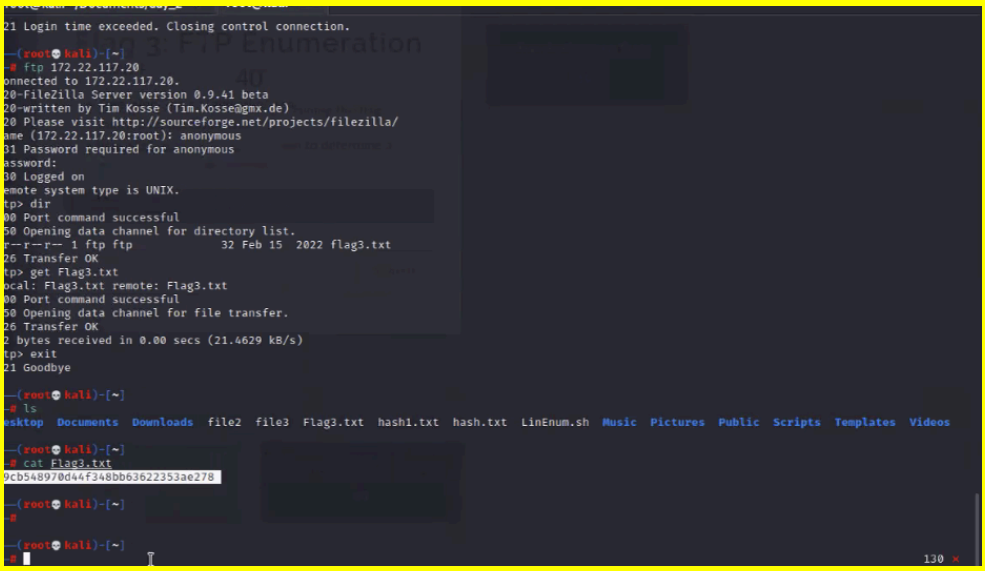
Images	 
Affected Hosts	192.168.13.12
Remediation	Apply Latest Patches to server and regularly update the software/server

Vulnerability 12	Findings
Title	Privilege Escalation via CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	User SSH information stored in plain text on WHOIS documentation. Weak password used to access. Privilege was escalated using “sudo -u#-1 /bin/bash”

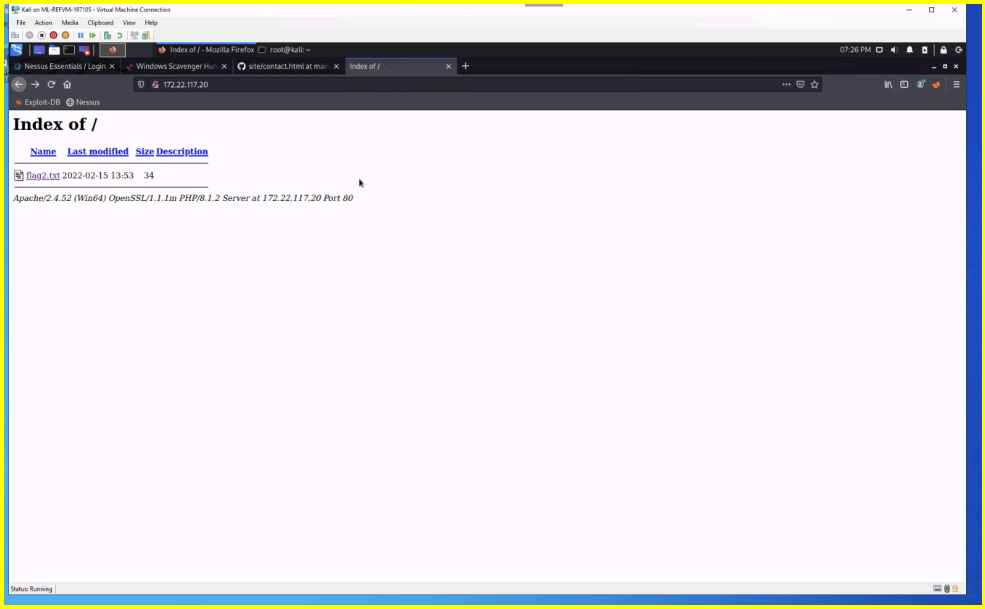
Images	
Affected Hosts	192.168.13.14
Remediation	Apply Security Patches. Audit User Permissions. Use an IDS/IPS

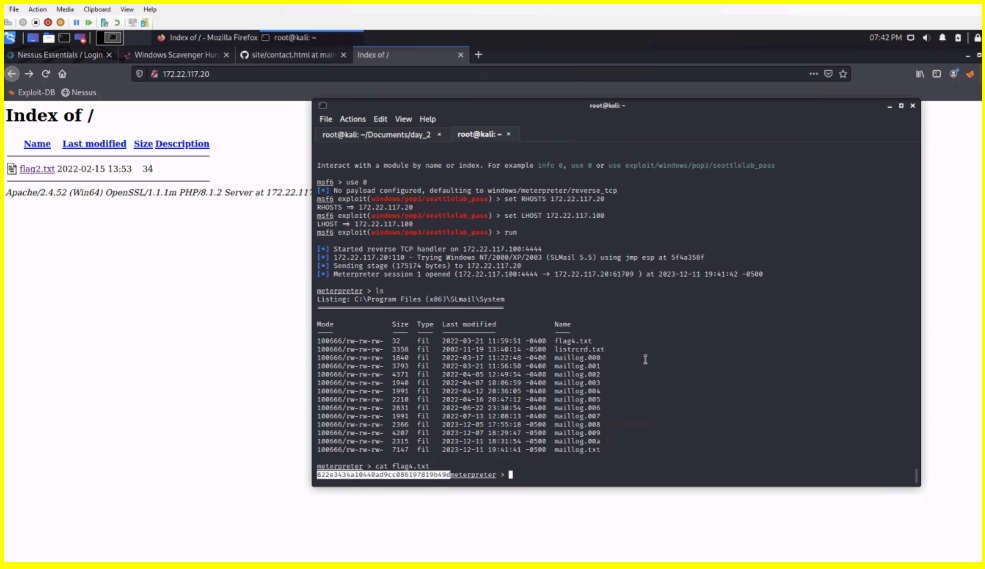
Vulnerability 13	Findings
Title	Public Exposure of User Credentials in GitHub Repository:
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Username and hash stored on publicly available github repo. Hash was cracked using John the Ripper
Images	

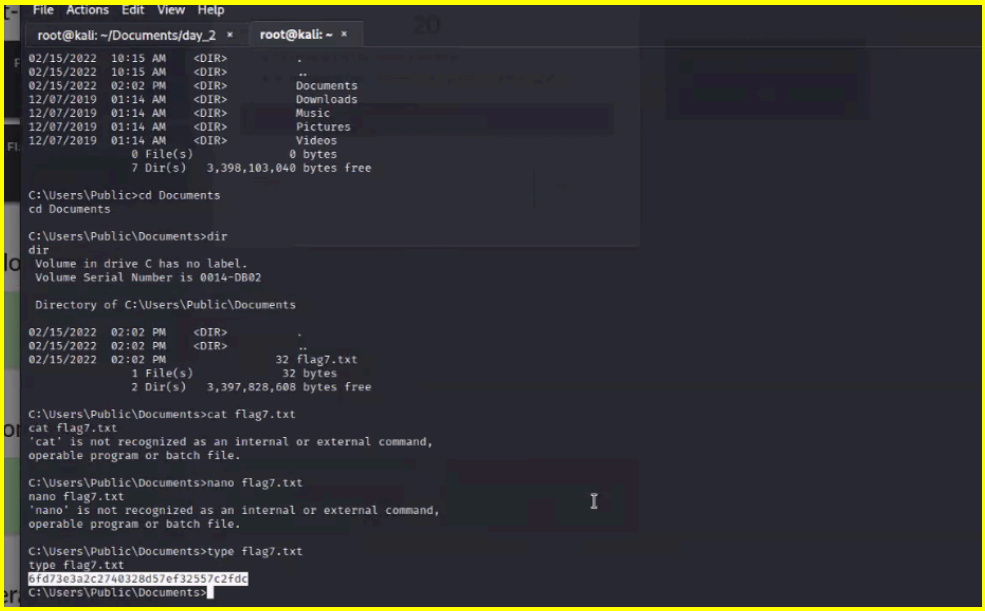
Affected Hosts	Catna Web Server
Remediation	Restrict access to Repo and remove credentials

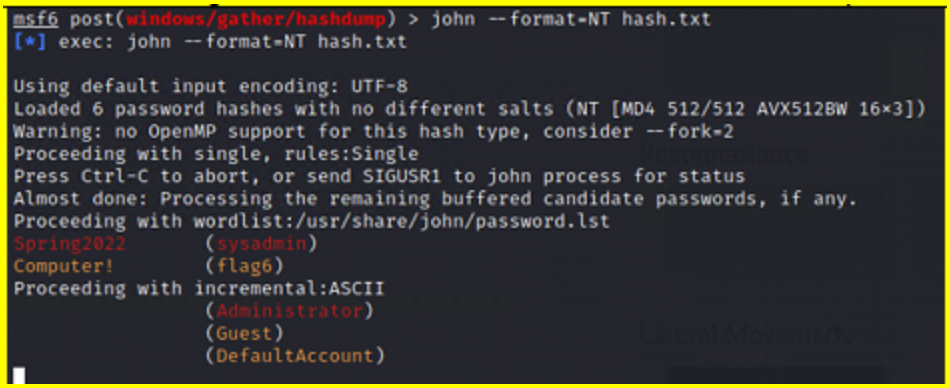
Vulnerability 14	**Findings**
Title	Insecure File Transfers due to Open Port 21
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Access the insecure FTP server
Images	
Affected Hosts	172.22.117.20
Remediation	Use protocol SFTP. Close or restrict access to port 21. Use stronger authentication processes for access via port 21

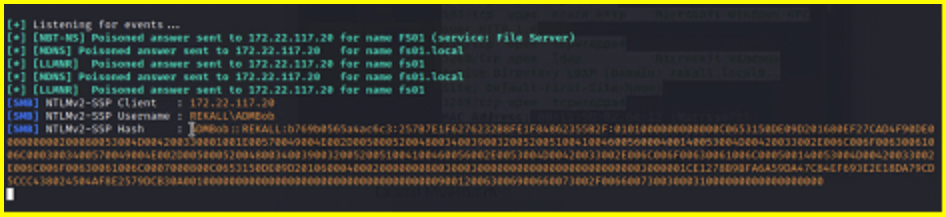
Vulnerability 15	**Findings**
Title	Open Port 80 with Website Access–
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Used credentials from Github Repo to access 172.22.117.20

Images	
Affected Hosts	172.22.117.20
Remediation	Enhance policy for User password complexity, history and length

Vulnerability 16	Findings
Title	SLMail Service Exploit Port 110
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Metasploit exploit/windows/pop3/seattlelab_pass exploit used to gain access to machine
Images	

	
Affected Hosts	172.22.117.20
Remediation	Apply Security Patches. Migrate to Secure Email Protocols IMAPS or POPS. CLose or restrict access to port 110

Vulnerability 17	Findings
Title	Weak Password Policies
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Used hashdump module in Metasploit to capture hashes and used John the Ripper to get password
Images	
Affected Hosts	172.22.117.20
Remediation	Enhance policy for User password complexity, history and length

Vulnerability 18	Findings
Title	LLMNR Protocol Weaknesses
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Captured LLMNR broadcasts to listen and discover credentials
Images	
Affected Hosts	172.22.117.20
Remediation	Disable LLMNR broadcasts