Hacking ético e Test de intrusión
Máster Inter-Universitario en Ciberseguridad (MUNICS)
Universidade da Coruña (UDC) y Universidade de Vigo (UVigo)
Curso 2024-2025

Práctica 2 - Identificación de vulnerabilidades

Nuria Codesido Iglesias

Índice

1 Identificación de CVE

En este apartado, se realizará un análisis exhaustivo de las vulnerabilidades encontradas en las máquinas Windows y Linux, utilizando herramientas especializadas para el escaneo de vulnerabilidades como `NESSUS` y `NMAP/NSE`. Para la máquina Linux, además, se empleará `NIKTO`.
Para cada vulnerabilidad identificada, se presentará una descripción detallada, el nivel de riesgo asociado, las soluciones recomendadas y los posibles exploits que podrían ser utilizados, tanto de forma manual como automática. Si se encuentra un exploit, se proporcionará una breve descripción (en color azul). En caso de que el exploit pertenezca a una categoría de alto riesgo, como aquellos que pueden causar daños graves al sistema, se destacará en color rojo. Cabe destacar que cada exploit se buscó con la herramienta `SearchSploit` y cada búsqueda está debidamente referenciada con una imagen en el apartado 2.

1.1 Análisis CVE - Máquina Windows(192.168.56.6)

CVE	Vulnerabilidad	Herramienta	Descripción	Riesgo	Solución	Exploit	
						Manual	Automático
CVE-2017-0143	ETERNALBLUE (MS17-010)	NESSUS/ NMAP/NSE	Vulnerabilidad en SMBv1 que permite a un atacante remoto no autenticado ejecutar código malicioso al enviar un paquete especialmente diseñado.	High	Instalar parches específicos y deshabilitar el servicio SMBv1.	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) 3 **Consiste:** en aprovechar una vulnerabilidad en SMB para ejecutar código remoto en Windows Server 2008 R2. Sí, supone un peligro grave. Si el exploit se usa incorrectamente o en un sistema sin parchear, puede causar un BSOD debido a la ejecución de código en el kernel, ya que la vulnerabilidad afecta cómo SMB maneja las solicitudes de red.	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) 3 **Consiste:** en permitir a un atacante ejecutar código de forma remota en sistemas Windows a través de vulnerabilidades en SMBv1. Sí, es grave. No causa BSOD, pero tiene mayor impacto por control y propagación.
CVE-2017-0144	ETERNALBLUE (MS17-010)	NESSUS	Vulnerabilidad en SMBv1 que permite a un atacante remoto no autenticado ejecutar código malicioso al enviar un paquete especialmente diseñado.	High	Instalar parches específicos y deshabilitar el servicio SMBv1.	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) 4 **Consiste:** en aprovechar una vulnerabilidad en SMB para ejecutar código remoto en Windows Server 2008 R2. Sí, supone un peligro grave. Si el exploit se usa incorrectamente o en un sistema sin parchear, puede causar un BSOD debido a la ejecución de código en el kernel, ya que la vulnerabilidad afecta cómo SMB maneja las solicitudes de red.	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) 4 **Consiste:** en permitir a un atacante ejecutar código de forma remota en sistemas Windows a través de vulnerabilidades en SMBv1. Sí, es grave. No causa BSOD, pero tiene mayor impacto por control y propagación.
CVE-2017-0145	ETERNALBLUE (MS17-010)	NESSUS	Vulnerabilidad en SMBv1 que permite a un atacante remoto no autenticado ejecutar código malicioso al enviar un paquete especialmente diseñado.	High	Instalar parches específicos y deshabilitar el servicio SMBv1.	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) 5 **Consiste:** en aprovechar una vulnerabilidad en SMB para ejecutar código remoto en Windows Server 2008 R2. Sí, supone un peligro grave. Si el exploit se usa incorrectamente o en un sistema sin parchear, puede causar un BSOD debido a la ejecución de código en el kernel, ya que la vulnerabilidad afecta cómo SMB maneja las solicitudes de red.	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) 5 **Consiste:** en permitir a un atacante ejecutar código de forma remota en sistemas Windows a través de vulnerabilidades en SMBv1. Sí, es grave. No causa BSOD, pero tiene mayor impacto por control y propagación.
CVE-2017-0146	ETERNALBLUE (MS17-010)	NESSUS	Vulnerabilidad en SMBv1 que permite a un atacante remoto no autenticado ejecutar código malicioso al enviar un paquete especialmente diseñado.	High	Instalar parches específicos y deshabilitar el servicio SMBv1.	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) 6 **Consiste:** en aprovechar una vulnerabilidad en SMB para ejecutar código remoto en Windows Server 2008 R2. Sí, supone un peligro grave. Si el exploit se usa incorrectamente o en un sistema sin parchear, puede causar un BSOD debido a la ejecución de código en el kernel, ya que la vulnerabilidad afecta cómo SMB maneja las solicitudes de red.	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) 6 **Consiste:** en permitir a un atacante ejecutar código de forma remota en sistemas Windows a través de vulnerabilidades en SMBv1. Sí, es grave. No causa BSOD, pero tiene mayor impacto por control y propagación.
CVE-2017-0147	ETERNALBLUE (MS17-010)	NESSUS	Vulnerabilidad en SMBv1 que permite a un atacante remoto no autenticado revelar información sensible mediante un paquete especialmente diseñado.	High	Instalar parches específicos y deshabilitar el servicio SMBv1.	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) 7 **Consiste:** en aprovechar una vulnerabilidad en SMB para ejecutar código remoto en Windows Server 2008 R2. Sí, supone un peligro grave. Si el exploit se usa incorrectamente o en un sistema sin parchear, puede causar un BSOD debido a la ejecución de código en el kernel, ya que la vulnerabilidad afecta cómo SMB maneja las solicitudes de red.	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) 7 **Consiste:** en permitir a un atacante ejecutar código de forma remota en sistemas Windows a través de vulnerabilidades en SMBv1. Sí, es grave. No causa BSOD, pero tiene mayor impacto por control y propagación.

Table 1: Identificación de CVE - Windows(192.168.56.6)

CVE	Vulnerabilidad	Herramienta	Descripción	Riesgo	Solución	Exploit	
						Manual	**Automático**
CVE-2017-0148	ETERNALBLUE (MS17-010)	NESSUS	Vulnerabilidad en SMBv1 que permite a un atacante remoto no autenticado ejecutar código malicioso al enviar un paquete especialmente diseñado.	High	Instalar parches específicos y deshabilitar el servicio SMBv1.	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) 8 **Consiste:** en aprovechar una vulnerabilidad en SMB para ejecutar código remoto en Windows Server 2008 R2. Aunque no causa un BSOD, permite tomar control del sistema y puede ser utilizado para propagar malware Sí, supone un peligro grave. Si el exploit se usa incorrectamente o en un sistema sin parchear, puede causar un BSOD debido a la ejecución de código en el kernel, ya que la vulnerabilidad afecta cómo SMB maneja las solicitudes de red.	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) 8 **Consiste:** en permitir a un atacante ejecutar código de forma remota en sistemas Windows a través de vulnerabilidades en SMBv1. Sí, es grave. No causa BSOD, pero tiene mayor impacto por control y propagación.
CVE-2016-0128	Elevación de privilegios en SAM y LSAD (MS16-047)	NESSUS	Vulnerabilidad en los protocolos SAM y LSAD que permite la elevación de privilegios mediante la manipulación de la autenticación sobre RPC, permitiendo el acceso al SAM.	Medium	Aplicar los parches de seguridad de Microsoft para las versiones afectadas de Windows.	No Results 9	No Results 9
CVE-2010-2730	Desbordamiento de búfer	NMAP	Vulnerabilidad en Outlook que permite ejecución remota de código	High	Aplicar parche de seguridad de Microsoft	No Results 9	No Results 9
CVE-2010-3972	Ejecución remota de código	NMAP	Fallo en el motor de script de IE que permite ejecución arbitraria de código	High	Actualizar Internet Explorer	Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (PoC) 11 **Consiste** en aprovechar un desbordamiento de búfer en el servicio FTP al procesar ciertos comandos FTP, lo que puede hacer que el servicio deje de responder	No Results 11
CVE-2010-1899	Corrupción de memoria	NMAP	Fallo en OpenType Font Driver que permite ejecución de código	Medium	Aplicar actualizaciones de seguridad	Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065) 12 **Consiste** en aprovechar un desbordamiento de pila al procesar solicitudes POST con muchos parámetros, lo que hace que el servidor se vuelva no responsivo hasta que se reinicie manualmente	No Results 12
CVE-2020-1113	Elevación de privilegios	NMAP	Fallo en el servicio de actualización que permite escalación de privilegios	High	Instalar parches de seguridad de Microsoft	No Results 13	No Results 13
CVE-2018-7445	Desbordamiento de memoria	NMAP	Vulnerabilidad en VLC que puede provocar ejecución de código malicioso	Critical	Actualizar VLC a la última versión	MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow 14 **Consiste** en aprovechar un desbordamiento de búfer al procesar mensajes de solicitud de sesión NetBIOS, permitiendo la ejecución de código sin autenticación Sí, es un peligro grave, ya que permite ejecución remota de código. No provoca un BSOD, pero puede tomar control del enrutador, afectando la red.	No Results 14

Table 2: Identificación de CVE 2 - Windows(192.168.56.6)

1.2 Análisis CVE - Máquina Linux (192.168.56.9)

CVE	Vulnerabilidad	Herramienta	Descripción	Riesgo	Solución	Exploit	
						Manual	Automático
CVE-2008-0166	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	NESSUS	El generador de números aleatorios de OpenSSL en Debian/Ubuntu es débil, permitiendo la predicción de claves privadas y ataques MITM.	Critical	Regenerar todas las claves criptográficas SSH, SSL y OpenVPN.	OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH (Ruby) 15 **Consiste** en permitir a un atacante predecir números aleatorios generados por OpenSSL, facilitando un ataque de fuerza bruta contra claves SSH en servidores vulnerables	No results 15
CVE-2008-0166	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	NESSUS	Claves SSH generadas en Debian/Ubuntu pueden ser fácilmente descubiertas y usadas para ataques.	Critical	Regenerar todas las claves SSH en el host afectado.	OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH (Ruby) 15 **Consiste** en permitir a un atacante predecir números aleatorios generados por OpenSSL, facilitando un ataque de fuerza bruta contra claves SSH en servidores vulnerables	No results 15
CVE-2020-1745	Apache Tomcat AJP Connector Request Injection (Ghostcat)	NESSUS	Un atacante remoto puede leer archivos de aplicaciones web y ejecutar código si el servidor permite la carga de archivos.	High	Configurar autorización en el conector AJP y actualizar Tomcat a 7.0.100, 8.5.51 o 9.0.31 o posterior.	Seowon SLR-120 Router - Remote Code Execution (Unauthenticated) 16 **Consiste** en afectar a los enrutadores Seowon SLR-120 y permite ejecución remota de código sin autenticación	No Results 16
CVE-2020-1938	Apache Tomcat AJP Connector Request Injection (Ghostcat)	NESSUS/NMAP	Similar a CVE-2020-1745, permite la lectura de archivos y ejecución de código en servidores vulnerables.	High	Configurar autorización en el conector AJP y actualizar Tomcat.	No Results 17	Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit) 17 **Consiste** en permitir a un atacante remoto y no autenticado leer archivos de aplicaciones web o incluir archivos maliciosos para ejecutar código en el servido.
CVE-2016-2183	SSL Medium Strength Cipher Suites Supported (SWEET32)	NESSUS	El servicio remoto permite el uso de cifrados SSL de fortaleza media (3DES), lo que facilita ataques criptográficos.	Medium	Reconfigurar la aplicación para evitar el uso de estos cifrados.	No Results 18	No Results 18
CVE-2013-2566	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	NESSUS	Uso del cifrado RC4, que tiene sesgos predecibles y puede ser descifrado si se capturan suficientes datos.	Medium	Deshabilitar el uso de RC4 y configurar TLS 1.2 con AES-GCM.	No Results 19	No Results 19
CVE-2015-2808	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	NESSUS	Similar a CVE-2013-2566, afecta la seguridad de los datos transmitidos.	Medium	Reconfigurar la aplicación para evitar el uso de RC4.	No Results 20	No Results 20
CVE-1999-0651	rlogin Service Detection	NESSUS/NMAP	El servicio rlogin está en ejecución en el host remoto, transmitiendo datos en texto plano, lo que permite ataques Man-in-the-Middle y posibles accesos no autenticados.	High	Comentar la línea 'login' en `/etc/inetd.conf` y reiniciar inetd, o deshabilitar rlogin y usar SSH.	No Results 21	No Results 21
CVE-2016-0800	SSL DROWN Attack	NESSUS	El host admite SSLv2, lo que permite un ataque de oracle de relleno Bleichenbacher para descifrar tráfico TLS capturado.	Medium	Deshabilitar SSLv2 y cifrados de grado de exportación, asegurando que las claves privadas no se usen con servidores SSLv2.	No Results 22	No Results 22
CVE-2016-2118	Samba Badlock Vulnerability	NESSUS	Vulnerabilidad en Samba que permite a un atacante interceptar y degradar la autenticación en el protocolo RPC, pudiendo modificar datos sensibles en Active Directory.	Medium	Actualizar Samba a la versión 4.2.11 / 4.3.8 / 4.4.2 o posterior.	No Results 23	No Results 23
CVE-2020-8616	ISC BIND Service Downgrade / Reflected DoS	NESSUS	ISC BIND 9 permite realizar demasiadas búsquedas al procesar una respuesta de referencia, lo que puede ser explotado para degradar el rendimiento del servidor o para ataques de reflexión.	Medium	Actualizar ISC BIND a la versión recomendada por el proveedor.	No Results 24	No Results 24
CVE-2003-1567	HTTP TRACE / TRACK Methods Allowed	NESSUS	El servidor web remoto permite los métodos TRACE y TRACK, lo que puede ser utilizado para ataques de cross-site tracing (XST).	Medium	Deshabilitar los métodos TRACE y TRACK en la configuración del servidor web.	No Results 25	No Results 25
CVE-2004-2320	HTTP TRACE / TRACK Methods Allowed	NESSUS	El servidor web remoto permite los métodos TRACE y TRACK, lo que puede ser utilizado para ataques de cross-site tracing (XST).	Medium	Deshabilitar los métodos TRACE y TRACK en la configuración del servidor web.	No Results 26	No Results 26
CVE-2010-0386	HTTP TRACE / TRACK Methods Allowed	NESSUS	El servidor web remoto permite los métodos TRACE y TRACK, lo que puede ser utilizado para ataques de cross-site tracing (XST).	Medium	Deshabilitar los métodos TRACE y TRACK en la configuración del servidor web.	No Results 27	No Results 27

Table 3: Identificación de CVE - Linux(192.168.56.9)

CVE	Vulnerabilidad	Herramienta	Descripción	Riesgo	Solución	Exploit	
						Manual	Automático
CVE-2007-1858	SSL Anonymous Cipher Suites Supported	NESSUS	El servicio remoto admite cifrados SSL anónimos, lo que permite ataques de Man-in-the-Middle debido a la falta de autenticación.	Low	Reconfigurar la aplicación para evitar el uso de cifrados débiles.	No Results 28	No Results 28
CVE-2011-0411	SMTP Service STARTTLS Plaintext Command Injection	NESSUS	Implementación defectuosa de STARTTLS en el servicio SMTP permite a un atacante inyectar comandos en la fase de texto plano y ejecutarlos en la fase cifrada, lo que puede llevar al robo de correos electrónicos o credenciales SASL.	Medium	Contactar al proveedor para obtener una actualización.	No Results 28	No Results 28
CVE-2011-1430	SMTP Service STARTTLS Plaintext Command Injection	NESSUS	Implementación defectuosa de STARTTLS en el servicio SMTP permite a un atacante inyectar comandos en la fase de texto plano y ejecutarlos en la fase cifrada, lo que puede llevar al robo de correos electrónicos o credenciales SASL.	Medium	Contactar al proveedor para obtener una actualización.	No Results 28	No Results 28
CVE-2011-1431	SMTP Service STARTTLS Plaintext Command Injection	NESSUS	Implementación defectuosa de STARTTLS en el servicio SMTP permite a un atacante inyectar comandos en la fase de texto plano y ejecutarlos en la fase cifrada, lo que puede llevar al robo de correos electrónicos o credenciales SASL.	Medium	Contactar al proveedor para obtener una actualización.	No Results 28	No Results 28
CVE-2011-1432	SMTP Service STARTTLS Plaintext Command Injection	NESSUS	Implementación defectuosa de STARTTLS en el servicio SMTP permite a un atacante inyectar comandos en la fase de texto plano y ejecutarlos en la fase cifrada, lo que puede llevar al robo de correos electrónicos o credenciales SASL.	Medium	Contactar al proveedor para obtener una actualización.	No Results 28	No Results 28
CVE-2011-1506	SMTP Service STARTTLS Plaintext Command Injection	NESSUS	Implementación defectuosa de STARTTLS en el servicio SMTP permite a un atacante inyectar comandos en la fase de texto plano y ejecutarlos en la fase cifrada, lo que puede llevar al robo de correos electrónicos o credenciales SASL.	Medium	Contactar al proveedor para obtener una actualización.	No Results 28	No Results 28
CVE-2011-2165	SMTP Service STARTTLS Plaintext Command Injection	NESSUS	Implementación defectuosa de STARTTLS en el servicio SMTP permite a un atacante inyectar comandos en la fase de texto plano y ejecutarlos en la fase cifrada, lo que puede llevar al robo de correos electrónicos o credenciales SASL.	Medium	Contactar al proveedor para obtener una actualización.	Watchguard XCS 10.0 - Multiple Vulnerabilities 29 **Consiste** en permitir inyección de SQL, ejecución de comandos y escalada de privilegios.	No Results 29
CVE-2015-0204	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	NESSUS	El host admite cifrados EXPORT_RSA con claves de 512 bits o menos, lo que permite a un atacante factorizar la clave y descifrar el tráfico SSL/TLS.	High	Deshabilitar los cifrados EXPORT_RSA y actualizar la configuración de TLS	No Results 30	No Results 30
CVE-2020-8617	ISC BIND Denial of Service	NESSUS	Vulnerabilidad en ISC BIND que permite un ataque DoS mediante un mensaje especialmente diseñado.	Medium	Actualizar a la versión corregida más cercana a la versión actual de BIND.	BIND - 'TSIG' Denial of Service 31 **Consiste** en provocar un Denial of Service (DoS) en servidores BIND al enviar consultas DNS manipuladas con TSIG malformadas.	No Results 31
CVE-2020-8622	ISC BIND DoS (TSIG-signed request)	NESSUS	DoS en ISC BIND al verificar una respuesta truncada a una solicitud TSIG, permitiendo el cierre del servidor.	Medium	Actualizar a BIND 9.11.22, 9.16.6, 9.17.4 o posterior.	No Results 32	No Results 32
CVE-2014-3566	SSLv3 POODLE Vulnerability	NESSUS/ NMAP/NSE	Vulnerabilidad en SSLv3 que permite ataques MitM para descifrar información confidencial.	Medium	Deshabilitar SSLv3 y habilitar el mecanismo TLS Fallback SCSV.	No Results 32	No Results 32

Table 4: Identificación de CVE 2 - Linux(192.168.56.9)

CVE	Vulnerabilidad	Herramienta	Descripción	Riesgo	Solución	Exploit	
						Manual	Automático
CVE-1999-0524	ICMP Timestamp Request Remote Date Disclosure	NESSUS	Permite a un atacante conocer la fecha y hora del sistema, útil para evadir autenticación basada en tiempo.	Low	Filtrar solicitudes ICMP timestamp (13) y respuestas (14).	No Results 32	No Results 32
CVE-2008-5161	SSH Server CBC Mode Ciphers Enabled	NESSUS/NMAP	Uso de cifrados CBC en SSH, lo que puede permitir la recuperación de texto en claro.	Low	Deshabilitar CBC y habilitar modos CTR o GCM.	No Results 32	No Results 32
CVE-2015-4000	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites (Logjam)	NESSUS/NMAP	Uso de claves Diffie-Hellman débiles en SSL/TLS, permitiendo ataque de downgrade.	Low	Eliminar soporte para EXPORT_DHE en la configuración del servicio.	No Results 32	No Results 32
CVE-2015-4000	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	NESSUS/NMAP	Uso de claves Diffie-Hellman de 1024 bits, permitiendo ataque de fuerza bruta en corto tiempo.	Low	Usar módulos Diffie-Hellman de al menos 2048 bits.	No Results 32	No Results 32
CVE-1999-0678	Exposición de directorios sensibles	NIKTO	(puerto 80) - vulnerabilidad que permite a los atacantes exploren directorios sensibles (como /usr/doc) a través de la indexación de directorios en un servidor web.	Medium	Deshabilitar la indexación de directorios en el servidor web, asegurándose de que no haya directorios sensibles accesibles sin autenticación. También es recomendable restringir el acceso a archivos sensibles en el servidor.	Debian 2.1 - HTTPd 33 **Consiste** en permitir a un atacante remoto ejecutar comandos arbitrarios en el servidor debido a una incorrecta configuración del servidor web. Sí, supone un peligro grave.No provoca un BSOD, pero permite ejecución remota de comandos.	No Results 33
CVE-2003-1418	Tomcat Directory Traversal	NIKTO	(puerto 80) - vulnerabilidad de directory traversal en Apache Tomcat que permite a un atacante acceder a archivos arbitrarios fuera del directorio web.	Medium	Limitar el acceso a archivos sensibles y asegurarse de que las rutas solicitadas no sean manipulables y actualizar Apache.	No Results 34	No Results 34
CVE-2000-0672	Tomcat Arbitrary File Reading	NIKTO	(puerto 8180) - vulnerabilidad de Apache Tomcat que permite a un atacante acceder y leer archivos arbitrarios en el servidor.	Medium	Actualizar a versiones de Tomcat que no presenten esta vulnerabilidad y restringir el acceso a las rutas sensibles.	No Results 34	No Results 34
CVE-2011-2523	Backdoor en vsftpd 2.3.4	NMAP/NSE	Shell abierto en puerto 6200/tcp.	Critical	Actualizar vsftpd a versión segura.	vsftpd 2.3.4 - Backdoor Command Execution 35 **Consiste** en permitir a un atacante ejecute comandos arbitrarios en el sistema mediante un backdoor presente en una versión específica de vsftpd. Sí, supone un peligro grave.No provoca un BSOD, pero permite ejecución remota de comandos.	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) 35 **Consiste** en permitir a un atacante ejecute comandos arbitrarios en el sistema mediante un backdoor presente en una versión específica de vsftpd. Sí, supone un peligro grave.No provoca un BSOD, pero permite ejecución remota de comandos.
CVE-2007-6750	Denegación de servicio en Apache HTTP Server (Slowloris)	NMAP/NSE	Ataque que mantiene conexiones abiertas con solicitudes HTTP parciales, agotando recursos del servidor.	Medium	Actualizar Apache a la versión 2.2.15 o superior.	No Results 36	No Results 36
CVE-2005-2040	Desbordamiento de búfer	NMAP	Vulnerabilidad en Samba que permite ejecución remota de código	Medium	Actualizar Samba	No Results 37	No Results 37
CVE-2008-0122	Desbordamiento de búfer	NMAP	Vulnerabilidad en Flash Player que permite ejecución de código	High	Actualizar o eliminar Flash Player	No Results 37	No Results 37
CVE-2017-3167	Autenticación débil	NMAP	Fallo en la autenticación de Apache que permite ataques de fuerza bruta	Critical	Aplicar parches y reforzar autenticación	No Results 37	No Results 37
CVE-2017-8779	Desbordamiento de pila	NMAP	Fallo en Putty que permite ejecución de código malicioso	High	Actualizar Putty	RPCBind / libtirpc - Denial of Service 38 **Consiste** en permitir a un atacante enviar paquetes UDP al puerto 111, lo que puede causar el consumo excesivo de memoria y la interrupción de servicios.	No Results 38
CVE-2023-42670	Cross-Site Scripting (XSS)	NMAP	Falta de validación en entrada permite inyección de scripts	Medium	Aplicar filtros de validación y escape de caracteres	No Results 39	No Results 39
CVE-1999-0502	Contraseña débil	NMAP	Uso de contraseñas predeterminadas o débiles en sistemas	High	Aplicar políticas de contraseñas seguras	No Results 40	SSH - User Code Execution (Metasploit) 40 **Consiste** en permitir la ejecución de código de usuario a través de SSH. Sí, supone un peligro grave, pero no causa un BSOD. En cambio, permite a un atacante obtener acceso no autorizado al sistema.
CVE-1999-1126	Inyección de comandos	NMAP	Uso de caracteres especiales en entradas no validadas	Low	Implementar validaciones de entrada	No Results 41	No Results 41
CVE-2011-3556	Desbordamiento de memoria	NMAP	Vulnerabilidad en Java que permite ejecución remota de código	High	Actualizar Java Runtime	No Results 42	Java RMI - Server Insecure Default Configuration Java Code Execution (Metasploit)42 **Consiste** en permitir a un atacante ejecutar código remoto en el servidor afectado sin autenticación. Sí, supone un peligro grave, pero no causa un BSOD. En cambio, permite la ejecución remota de código.
CVE-2009-0543	Denegación de servicio (DoS)	NMAP	Falla en IIS que permite ataques de denegación de servicio	Medium	Aplicar actualizaciones de seguridad	ProFTPd - 'mod_mysql' Authentication Bypass 42 **Consiste** en permitir eludir la autenticación mediante una inyección SQL.	No Results 43
CVE-2008-4097	Desbordamiento de pila	NMAP	Vulnerabilidad en VLC que permite ejecución de código arbitrario	Medium	Actualizar VLC a la última versión	No Results 44	No Results 44
CVE-2010-1447	Corrupción de memoria	NMAP	Fallo en el kernel de Windows que permite escalación de privilegios	High	Aplicar parches de seguridad	No Results 44	No Results 44
CVE-2002-1511	Inyección SQL	NMAP	Falta de validación en entradas permite inyección SQL	Medium	Aplicar validaciones en consultas SQL	No Results 44	No Results 44
CVE-2010-2075	Cross-Site Scripting (XSS)	NMAP	Vulnerabilidad en WordPress que permite inyección de scripts maliciosos	High	Aplicar actualizaciones de seguridad	UnrealIRCd 3.2.8.1 - Remote Downloader/Execute 45 **Consiste** en permitir la ejecución de comandos a través de una puerta trasera (backdoor)	UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit) 45 **Consiste** en permitir la ejecución de comandos a través de una puerta trasera (backdoor)
CVE-2005-2090	Desbordamiento de búfer	NMAP	Vulnerabilidad en PHP que permite ejecución de código remoto	Medium	Actualizar PHP a una versión segura	No Results 46	No Results 46

Table 5: Identificación de CVE 3 - Linux(192.168.56.9)

La heramienta NIKTO permite detectar gran cantidad de vulnerabilidades en servidores web. En base a los resultados del escaneo de Nmap de la práctica 1, los puertos relevantes que hay que analizar son:

- **Puerto 80**. Este puerto está asociado con el servidor Apache HTTPD 2.2.8.

  En la siguiente imagen, se muestra la salida de la herramienta NIKTO al escanear la máquina de Linux 192.168.56.9 a través del puerto 80. Una de las vulnerabilidades destacadas en la imagen es OSVDB-12184, que hace referencia a una vulnerabilidad en PHP que puede revelar información sensible a través de cadenas de consulta HTTP específicas. Sin embargo, no se encontró un CVE asociado a este OSVDB, tampoco en la tabla de relaciones del MITRE [1]. También se encontró una debilidad CWE-552 asociada a la página phpinfo.php, lo que implica que este script puede estar revelando información sensible del sistema.

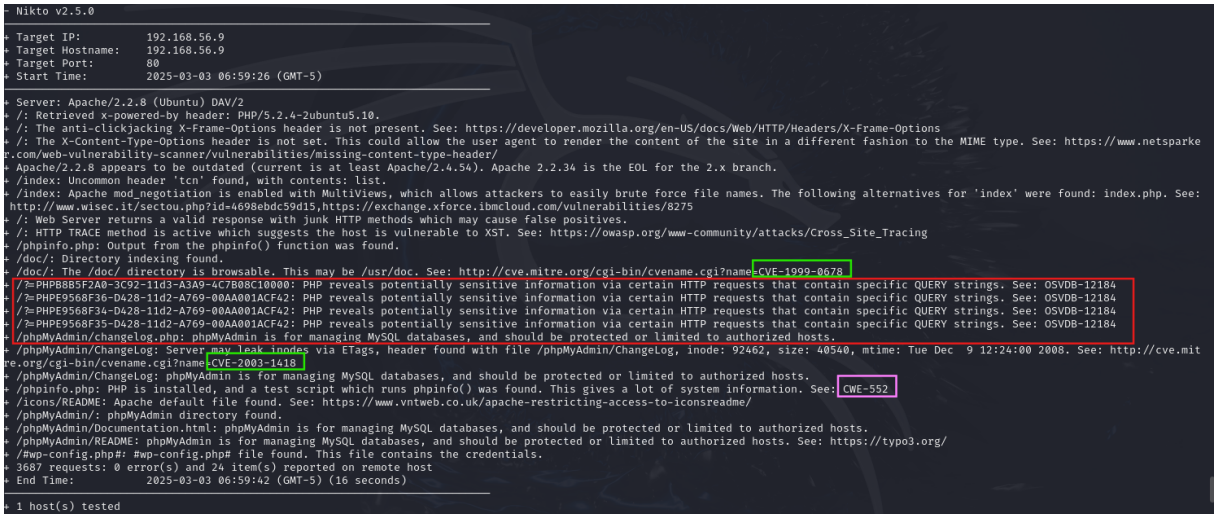

Figure 1: Herramienta NIKTO - puerto 80

- **Puerto 8180**. Este puerto está asociado con Apache Tomcat (Apache Tomcat/Coyote JSP engine 1.1).

Figure 2: Herramienta NIKTO - puerto 8180

2 Identificación de Exploits

En primer lugar, se usa la herramienta `SearchSploit` para encontrar los exploits relacionados con cada `CVE`, se realiza tanto para la máquina de Windows como la de Linux. A continuación, basándonos en los resultados anteriores, se debe identificar al menos dos exploits para cada `CVE`, uno de ellos manual.

2.1 Identificación de Exploits - Máquina Windows (192.168.56.6)

```
nuria@nci:~$ searchsploit --cve CVE-2017-0143
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)              | windows/remote/47456.rb
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Co | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (M | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 3: searchsploit –cve CVE-2017-0143

```
nuria@nci:~$ searchsploit --cve CVE-2017-0144
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)              | windows/remote/47456.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execu | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17 | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (M | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 4: searchsploit –cve CVE-2017-0144

```
nuria@nci:~$ searchsploit --cve CVE-2017-0145
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)              | windows/remote/47456.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (M | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 5: searchsploit –cve CVE-2017-0145

```
nuria@nci:~$ searchsploit --cve CVE-2017-0146
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)              | windows/remote/47456.rb
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Co | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (M | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 6: searchsploit –cve CVE-2017-0146

```
nuria@nci:~$ searchsploit --cve CVE-2017-0147
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)              | windows/remote/47456.rb
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Co | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (M | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 7: searchsploit –cve CVE-2017-0147

```
nuria@nci:~$ searchsploit --cve CVE-2017-0148
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)              | windows/remote/47456.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) | windows/dos/41891.rb
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (M | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 8: searchsploit –cve CVE-2017-0148

```
nuria@nci:~$ searchsploit --cve CVE-2016-0128
Exploits: No Results
Shellcodes: No Results
```

Figure 9: searchsploit –cve CVE-2016-0128

```
nuria@nci:~$ searchsploit --cve CVE-2010-2730
Exploits: No Results
Shellcodes: No Results
```

Figure 10: searchsploit –cve CVE-2010-2730

```
nuria@nci:~$ searchsploit --cve CVE-2010-3972
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (PoC) | windows/dos/15803.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 11: searchsploit –cve CVE-2010-3972

```
nuria@nci:~$ searchsploit --cve CVE-2010-1899
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065 | windows/dos/15167.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 12: searchsploit –cve CVE-2010-1899

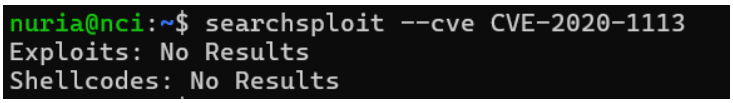

Figure 13: searchsploit –cve CVE-2020-1113

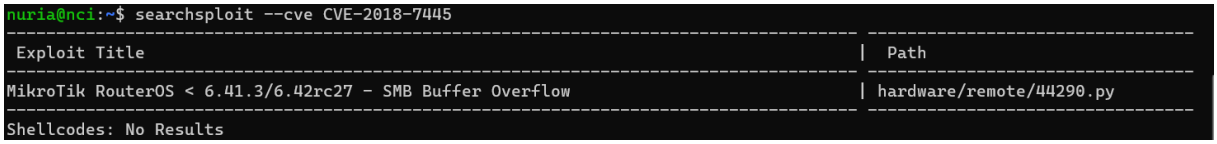

Figure 14: searchsploit –cve CVE-2018-7445

2.1.1 Peligrosidad - exploits.

Para cada exploit propuesto se debe indicar, en caso de que así sea, si el exploit supone algún peligro durante su ejecución (tipo BSOD) y en qué consiste. A partir de los exploits identificados en las vulnerabilidades listadas en las tablas 1 y 2 (principalmente relacionadas con el protocolo SMBv1 y otros fallos de software),en general, ninguno de los exploits detallados provoca directamente un BSOD en el sistema afectado, excepto en el caso de los relacionados con la vulnerabilidad CVE-2017-0143 (ETERNALBLUE). En este último caso, el exploit (`Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)`) puede provocar un BSOD debido a la ejecución de código malicioso en el núcleo del sistema, afectando la forma en que el protocolo SMB maneja las solicitudes de red.

2.2 Identificación de Exploits - Máquina Linux (192.168.56.9)

```
nuria@nci:~$ searchsploit --cve CVE-2008-0166
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force S | linux/remote/5622.txt
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force S | linux/remote/5632.rb
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force S | linux/remote/5720.py
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 15: searchsploit –cve CVE-2008-0166

```
nuria@nci:~$ searchsploit --cve CVE-2020-1745
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Seowon SLR-120 Router - Remote Code Execution (Unauthenticated)                           | hardware/remote/50821.py
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 16: searchsploit –cve CVE-2020-1745

```
nuria@nci:~$ searchsploit --cve CVE-2020-1938
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Apache Tomcat - AJP 'Ghostcat File Read/Inclusion                                         | multiple/webapps/48143.py
Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)                           | multiple/webapps/49039.rb
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 17: searchsploit –cve CVE-2020-1938

```
nuria@nci:~$ searchsploit --cve CVE-2016-2183
Exploits: No Results
Shellcodes: No Results
```

Figure 18: searchsploit –cve CVE-2016-2183

```
nuria@nci:~$ searchsploit --cve CVE-2013-2566
Exploits: No Results
Shellcodes: No Results
```

Figure 19: searchsploit –cve CVE-2013-2566

```
nuria@nci:~$ searchsploit --cve CVE-2015-2808
Exploits: No Results
Shellcodes: No Results
```

Figure 20: searchsploit –cve CVE-2015-2808

```
nuria@nci:~$ searchsploit --cve CVE-1999-0651
Exploits: No Results
Shellcodes: No Results
```

Figure 21: searchsploit –cve CVE-1999-0651

```
nuria@nci:~$ searchsploit --cve CVE-2016-0800
Exploits: No Results
Shellcodes: No Results
```

Figure 22: searchsploit –cve CVE-2016-0800

```
nuria@nci:~$ searchsploit --cve CVE-2016-2118
Exploits: No Results
Shellcodes: No Results
```

Figure 23: searchsploit –cve CVE-2016-2118

```
nuria@nci:~$ searchsploit --cve CVE-2020-8616
Exploits: No Results
Shellcodes: No Results
```

Figure 24: searchsploit –cve CVE-2020-8616

```
nuria@nci:~$ searchsploit --cve CVE-2003-1567
Exploits: No Results
Shellcodes: No Results
```

Figure 25: searchsploit –cve CVE-2003-1567

```
nuria@nci:~$ searchsploit --cve CVE-2004-2320
Exploits: No Results
Shellcodes: No Results
```

Figure 26: searchsploit –cve CVE-2004-2320

```
nuria@nci:~$ searchsploit --cve CVE-2010-0386
Exploits: No Results
Shellcodes: No Results
```

Figure 27: searchsploit –cve CVE-2010-0386

```
nuria@nci:~$ searchsploit --cve CVE-2007-1858
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2011-0411
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2011-1430
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2011-1431
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2011-1432
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2011-1506
Exploits: No Results
Shellcodes: No Results
```

Figure 28: searchsploit –cve ...

```
nuria@nci:~$ searchsploit --cve CVE-2011-2165
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Watchguard XCS 10.0 - Multiple Vulnerabilities                                | php/webapps/37440.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 29: searchsploit –cve CVE-2011-2165

```
nuria@nci:~$ searchsploit --cve CVE-2015-0204
Exploits: No Results
Shellcodes: No Results
```

Figure 30: searchsploit –cve CVE-2015-0204

```
nuria@nci:~$ searchsploit --cve CVE-2020-8617
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
BIND - 'TSIG' Denial of Service                                               | multiple/dos/48521.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 31: searchsploit –cve CVE-2020-8617

```
nuria@nci:~$ searchsploit --cve CVE-2020-8622
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2014-3566
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-1999-0524
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2008-5161
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2015-4000
Exploits: No Results
Shellcodes: No Results
```

Figure 32: searchsploit –cve ...

```
nuria@nci:~$ searchsploit --cve CVE-1999-0678
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Debian 2.1 - HTTPd                                                            | linux/remote/19253.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 33: searchsploit –cve CVE-1999-0678

```
nuria@nci:~$ searchsploit --cve CVE-2003-1418
Exploits: No Results
Shellcodes: No Results
nuria@nci:~$ searchsploit --cve CVE-2000-0672
Exploits: No Results
Shellcodes: No Results
```

Figure 34: searchsploit –cve ...

```
nuria@nci:~$ searchsploit --cve CVE-2011-2523
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Figure 35: searchsploit –cve CVE-2011-2523

```
nuria@nci:~$ searchsploit --cve CVE-2007-6750
Exploits: No Results
Shellcodes: No Results
```

Figure 36: searchsploit –cve CVE-2007-6750

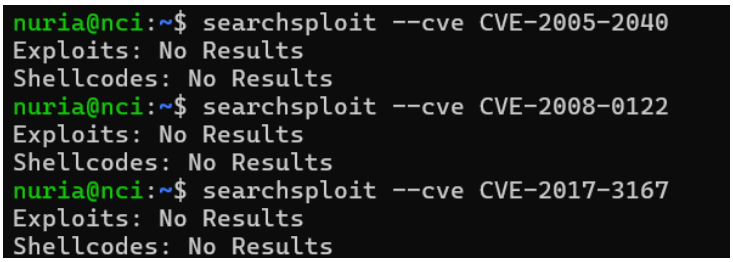

Figure 37: searchsploit –cve ...

Figure 38: searchsploit –cve CVE-2017-8779

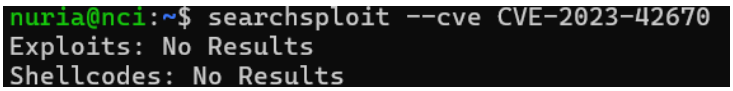

Figure 39: searchsploit –cve CVE-2023-42670

Figure 40: searchsploit –cve CVE-1999-0502

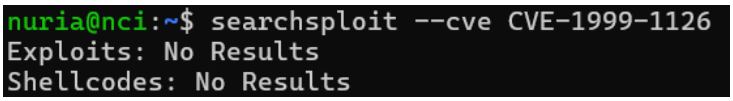

Figure 41: searchsploit –cve CVE-1999-1126

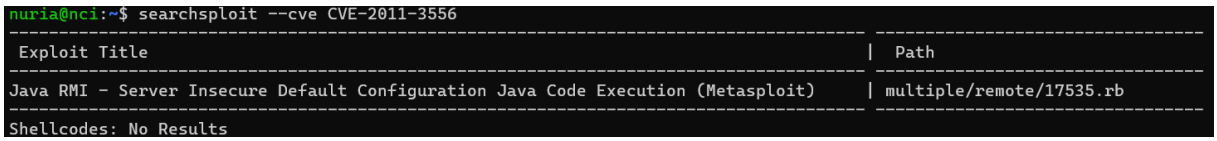

Figure 42: searchsploit –cve CVE-2011-3556

Figure 43: searchsploit –cve CVE-2009-0543

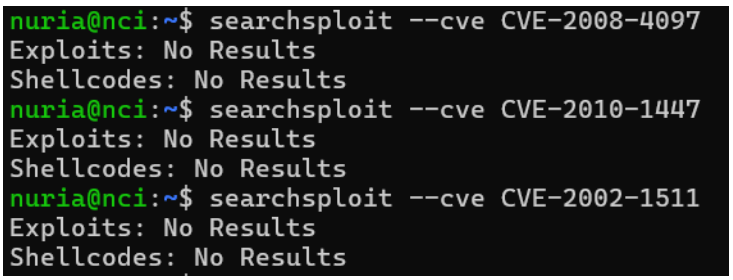

Figure 44: searchsploit –cve ...

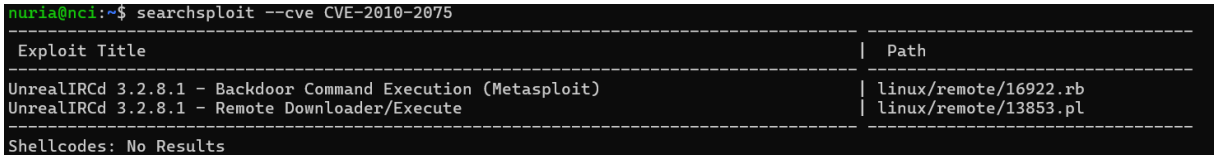

Figure 45: searchsploit –cve CVE-2010-2075

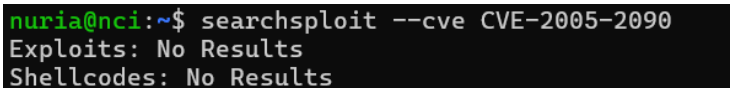

Figure 46: searchsploit –cve CVE-2005-2090

2.2.1 Peligrosidad - exploits.

Para cada exploit propuesto se debe indicar, en caso de que así sea, si el exploit supone algún peligro durante su ejecución (tipo BSOD) y en qué consiste. A partir de los exploits identificados en las vulnerabilidades listadas en las tablas 3, 4 y 5 (principalmente relacionadas con ejecución remota de código, ataques de denegación de servicio (DoS), y exposiciones de datos), ninguno de los exploits detallados en relación al S.O. Linux, provoca directamente un BSOD en el sistema afectado. En cambio, estos exploits comprometen principalmente la seguridad a nivel de software, lo que significa que pueden permitir la ejecución remota de código, la exposición de datos sensibles o ataques de denegación de servicio (DoS), pero no afectan directamente la estabilidad del sistema operativo.

3 Referencias

[1] *Cve reference map for source osvdb*. [Online]. Available: `https://cve.mitre.org/data/refs/refmap/source-OSVDB.html`.