



Universidad Carlos III
Curso Ingeniería del Software 2020-21
Práctica
Curso 2020-21

Descubrimiento de vulnerabilidades

Fecha: **12/04/2021** - ENTREGA: **2**

GRUPO: **82** EQUIPO: **06**

Alumnos: **Alfonso Serrano Corbelle, Alberto Morcillo Villa**

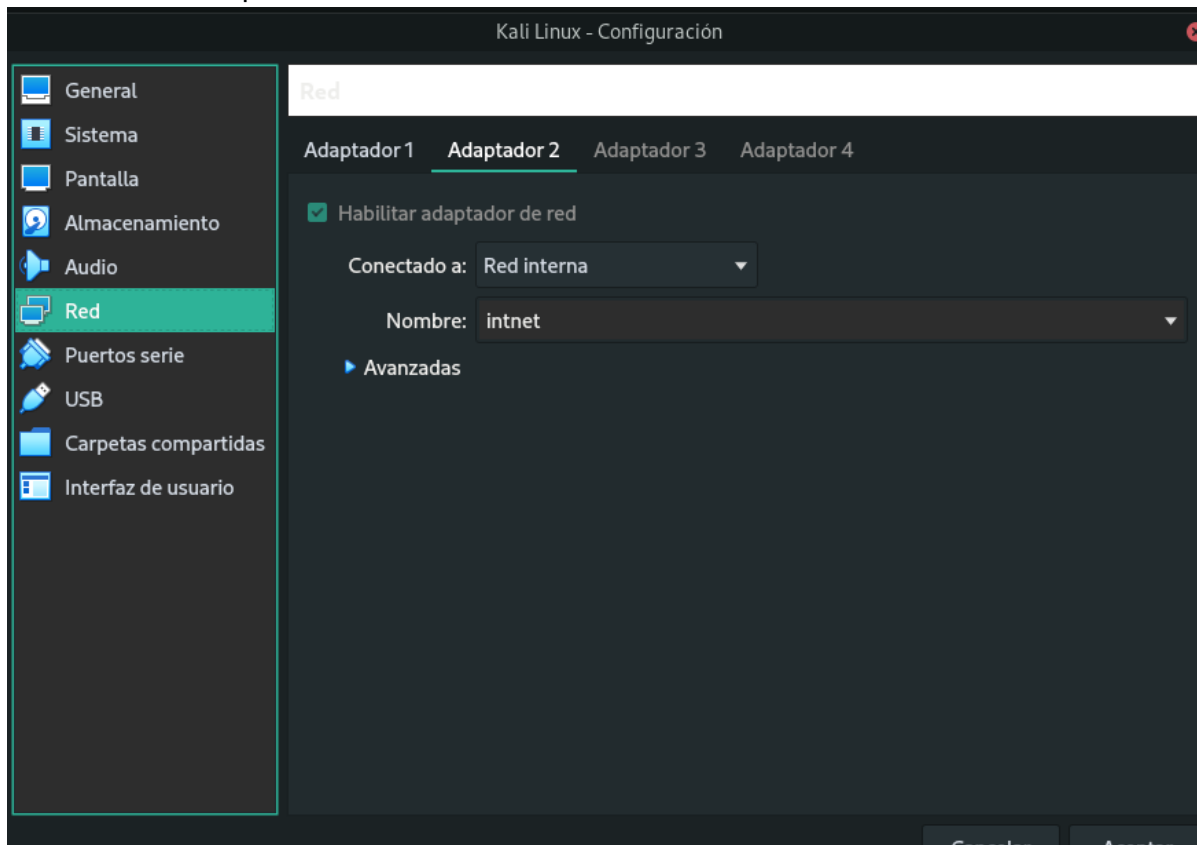
Índice

1. Proceso de configuración y uso de las herramientas	2
2. Listado de los servicios abiertos descubiertos en cada máquina	3
3. Resumen Ejecutivo	4
3.1. Linux.....	4
3.2. Windows XP	9
3.3. Windows 7	12
3.4. Recomendaciones para la corrección de vulnerabilidades.....	16
4. Estudio de las Vulnerabilidades	16
4.1. MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)	16
4.2. MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING)	17
4.3. MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	18
4.4. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	18
4.5. rexecd Service Detection	19
4.6. Bind Shell Backdoor Detection.....	20
4.7. VNC Server 'password' Password.....	21
4.8. MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)	21
4.9. MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	23
4.10. Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	24
5. Bibliografía.....	26

1. Proceso de configuración y uso de las herramientas

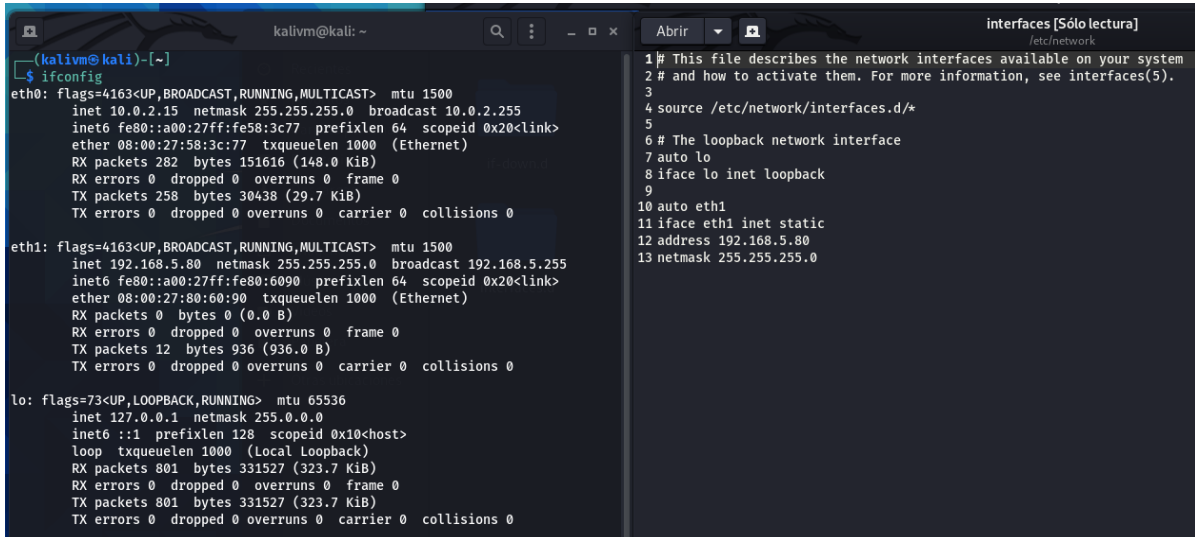
Se han importado las máquinas correspondientes a Virtualbox mediante el fichero OVA proporcionado.

Para conectar la VM de Kali en Opciones se ha conectado un adaptador de red hacia la red interna de las máquinas dadas



Después se ha configurado la máquina para que el la eth1 se pueda conectar a la red interna editando el fichero `/etc/network/interfaces` y se le asigna una IP en el rango 192.168.5.0/24, en este caso ha sido 192.168.5.80

Y usando ifconfig en la terminal se ve como está bien configurada, usando Nessus detecta a las VM buscadas



```
(kalivm@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe58:3c77 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:58:3c:77 txqueuelen 1000 (Ethernet)
    RX packets 282 bytes 151616 (148.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 258 bytes 30438 (29.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.5.80 netmask 255.255.255.0 broadcast 192.168.5.255
    inet6 fe80::a00:27ff:fe80:6090 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:80:60:90 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 936 (936.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 801 bytes 331527 (323.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 801 bytes 331527 (323.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
3
4 source /etc/network/interfaces.d/*
5
6 # The loopback network interface
7 auto lo
8 iface lo inet loopback
9
10 auto eth1
11 iface eth1 inet static
12 address 192.168.5.80
13 netmask 255.255.255.0
```

2. Listado de los servicios abiertos descubiertos en cada máquina

Servicios Linux (192.168.5.20)

FTP Server, SSH Server, Telnet Server, SMTP Server, Web Server, Shell Server, VNC Server, IRC Server

Servicios Windows XP (192.168.5.40)

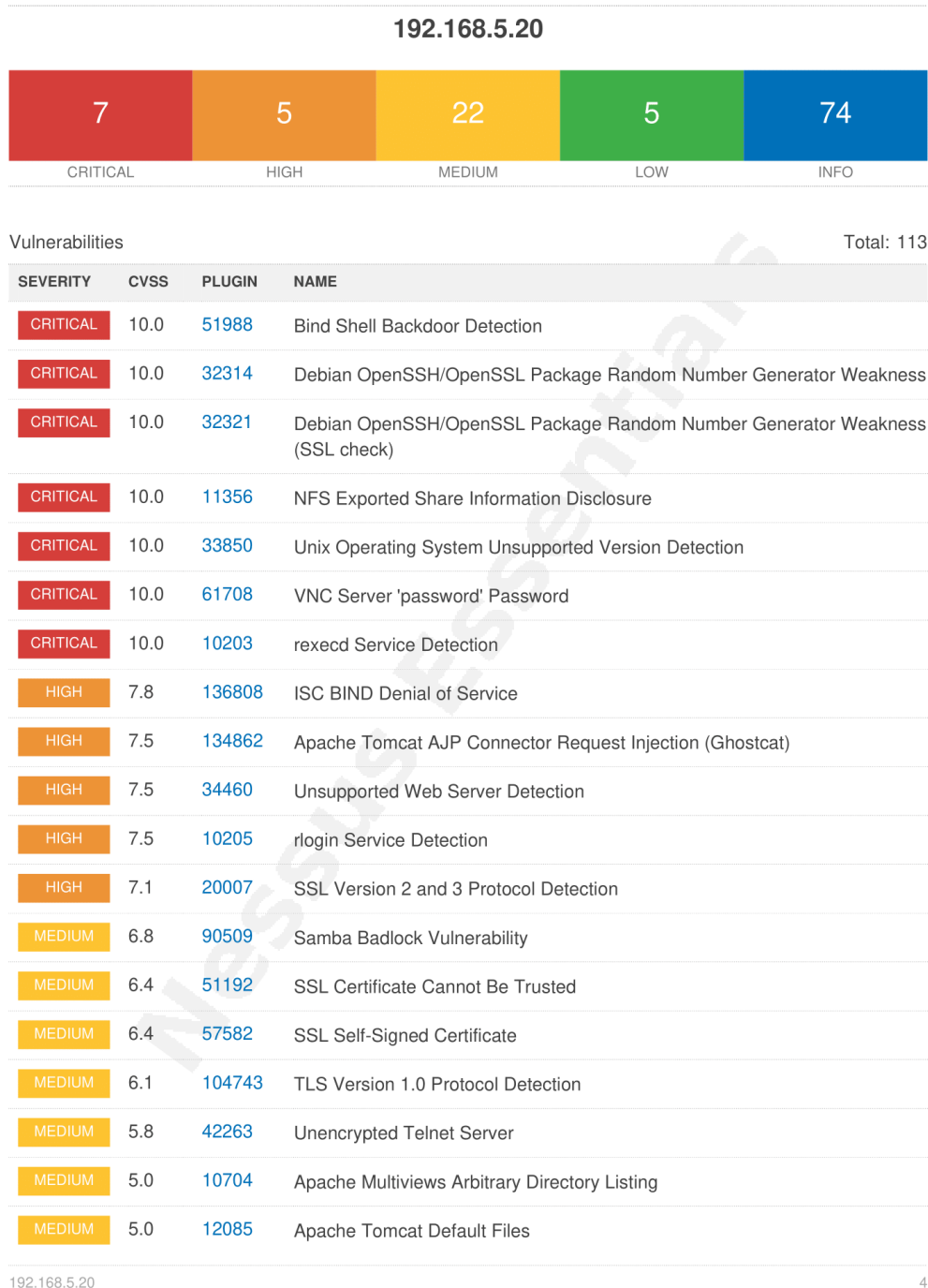
SNP Server, SMB Server

Servicios Windows 7 (192.168.5.60)

TCP Wrapper, Web Server, TLS 1.2

3. Resumen Ejecutivo

3.1. Linux



MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	5.0	42256	NFS Shares World Readable
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	4.0	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6	10407	X Server Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	21186	AJP Connector Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure

INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	39519	Backported Security Patch Detection (FTP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	10719	MySQL Server Detection

INFO	N/A	10437	NFS Share Export List
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	10919	Open Port Re-check
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	118224	PostgreSQL STARTTLS Support
INFO	N/A	26024	PostgreSQL Server Detection
INFO	N/A	22227	RMI Registry Detection
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	53335	RPC portmapper (TCP)
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	42088	SMTP Service STARTTLS Command Support
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported

INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	19288	VNC Server Security Type Detection
INFO	N/A	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	10342	VNC Software Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	11424	WebDAV Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	52703	vsftpd Detection

3.2. Windows XP

192.168.5.40				
6	4	1	1	30
CRITICAL	HIGH	MEDIUM	LOW	INFO
Vulnerabilities				Total: 42
SEVERITY	CVSS	PLUGIN	NAME	
CRITICAL	10.0	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)	
CRITICAL	10.0	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)	
CRITICAL	10.0	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)	
CRITICAL	10.0	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection	
CRITICAL	10.0	108797	Unsupported Windows OS (remote)	
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	
HIGH	7.5	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)	
HIGH	7.5	26920	Microsoft Windows SMB NULL Session Authentication	
HIGH	7.5	41028	SNMP Agent Default Community Name (public)	
MEDIUM	5.0	57608	SMB Signing not required	
LOW	3.3	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure	
INFO	N/A	45590	Common Platform Enumeration (CPE)	
192.168.5.40				4

INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	14274	Nessus SNMP Scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	35296	SNMP Protocol Version Detection
INFO	N/A	34022	SNMP Query Routing Information Disclosure
INFO	N/A	10550	SNMP Query Running Process List Disclosure
INFO	N/A	10800	SNMP Query System Information Disclosure
INFO	N/A	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	40448	SNMP Supported Protocols Detection
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported

INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

3.3. Windows 7

192.168.5.60

5	4	19	6	43
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 77

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	97192	Tenable Nessus 6.x < 6.9 Multiple Vulnerabilities (TNS-2016-16) (SWEET32)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	8.5	128118	Tenable Nessus < 8.6.0 Denial of Service vulnerability (TNS-2019-05)
HIGH	7.5	34460	Unsupported Web Server Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.0	99440	Tenable Nessus 6.8.x < 6.10.2 Arbitrary File Upload (TNS-2017-06)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

192.168.5.60

MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	120198	Tenable Nessus < 7.1.4 Multiple Vulnerabilities (TNS-2018-17)
MEDIUM	4.3	123462	Tenable Nessus < 8.3.0 Multiple Vulnerabilities (TNS-2019-02)
MEDIUM	4.3	126627	Tenable Nessus < 8.5.0 Multiple Vulnerabilities (TNS-2019-04)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
MEDIUM	4.0	110096	Tenable Nessus < 7.1.0 Multiple Vulnerabilities (TNS-2018-05)
MEDIUM	4.0	130433	Tenable Nessus < 8.7.0 DoS (TNS-2019-06)
LOW	3.6	139910	Tenable Nessus < 8.11.1 Session Expiration (TNS-2020-06)
LOW	3.5	97193	Tenable Nessus 6.8.x and 6.9.x < 6.9.1 Stored XSS (TNS-2016-17)
LOW	3.5	96833	Tenable Nessus 6.x < 6.9.3 Multiple Stored XSS
LOW	3.5	138562	Tenable Nessus < 8.11.0 Stored XSS (TNS-2020-05)
LOW	3.5	121620	Tenable Nessus < 8.2.2 Stored XSS Vulnerability (TNS-2019-01)
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses

INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10147	Nessus Server Detection
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	66173	RDP Screenshot
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported

INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	135860	WMI Not Available
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

3.4. Recomendaciones para la corrección de vulnerabilidades

La mayoría de las vulnerabilidades pueden ser corregidas simplemente actualizando elementos desfasados que a día de hoy están ya corregidos, especialmente los más peligrosos y de más criticidad pues son los que más rápidamente son parcheados.

Aparte de mantener actualizado el sistema operativo y sus programas también es importante tomar precauciones. Algunas precauciones son hacer contraseñas seguras y arbitrarias, o dejar sesiones abiertas cuando pueden ser accedidas por otras personas, no permitir la ejecución de comandos del SO desde el código de la capa de aplicación, no entrar en URL's desconocidas, usar autenticación en dos pasos al iniciar sesión y no ejecutar archivos ejecutables (.exe) que hayamos descargado de sitios desconocidos o poco seguros.

También se recomienda bloquear puertos usados por servicios como SMB o RDP a las redes externas al entorno donde está el PC si no son usados estos servicios ya que suelen constituir problemas graves para la seguridad, lo mismo se aplica a VNC y en general programas que permitan controlar de forma remota el PC.

4. Estudio de las Vulnerabilidades

4.1. MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)ⁱ

Descripción del problema

Debido a un error en la implementación del Server Message Block (SMB), un atacante podría ejecutar un código arbitrario en el host remoto.

CVSS

Base Score = 10

CVSS: 3.1/ AV:N / AC:L / PR:N / UI:N / S:C / C:H / I:H / A:H

Exploit

Un atacante puede, sin necesidad de ser autenticado, explotar esta vulnerabilidad para instalar programas; ver, editar o borrar datos e incluso crear nuevas cuentas con permisos de administrador.

Solución

Windows sacó parches para arreglar estos problemas. Además de ello, un usuario podría intentar diferentes soluciones alternativas como utilizar un firewall con configuración predeterminada (en vez de la defectuosa), usar filtros avanzados de TCP/IP y bloquear los puertos TCP afectados, que en este caso normalmente son 139 y 445.

4.2. MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING)ⁱⁱ

Descripción del problema

ECLIPSEDWING es uno de los exploits descubiertos en 2017 por un grupo muy famoso de hackers llamado los "Shadow Brokers". Consiste en que un host remoto de Windows es afectado por una excepción de la ejecución remota de un código debido a un fallo en la gestión de RCP o llamada a procedimiento remoto.

CVSS

Base Score: 9.8

CVSS: 3.1/ AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H

Exploit

A través de una petición de SPC especialmente fabricada un atacante podría, sin necesidad de autenticarse, ejecutar un código aleatorio con privilegios de sistema. Hemos encontrado uno de los posibles códigos con los que se podría explotar tal vulnerabilidad y que permitiría a un atacante obtener privilegios de forma remota.ⁱⁱⁱ

Solución

Afortunadamente todos los exploits de los Shadow Brokers fueron solucionados por la propia Microsoft por medio de parches para Windows 2000, XP, 2003, Vista y 2008.

4.3. MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unauthenticated check)^{iv}

Descripción del problema

El host remoto de Windows tiene una vulnerabilidad de ejecución de código remoto debido a su procesamiento incorrecto de los paquetes por el Paquete de seguridad Secure Channel (Schannel).

CVSS

Base Score: 10

CVSS: 3.1/AV=N / AC=L / PR=N / UI=N / S=C / C=H / I=H / A=H

Exploit

Esto lo hace susceptible de sufrir un ataque por parte de un agresor que envíe un paquete especialmente fabricado que le permitiría ejecutar código en el ordenador de forma remota. El Schannel envía un mensaje para completar un handshake tipo certificado TLS, pero algunos hosts de Windows cortarían la conexión si reciben uno que no han pedido con un mensaje de CertificateRequest, por lo que el plugin no detectaría la vulnerabilidad.^v

Solución

Para solucionar este problema, debería instalar el parche que corrige cómo Schannel procesa los paquetes especialmente fabricados.

4.4. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness^{vi}

Descripción del problema

Uno de los certificados remotos SSL ha sido generado de forma incorrecta por la librería OpenSSL de generación de números aleatorios. Esto está provocado a un empaquetador de Debian, el CVE-2008-0166, que ha eliminado buena parte de los generadores de entropía, haciendo que los números aleatorios generados a la larga sean fáciles de adivinar.

CVSS

Base Score: 8.9

CVSS = 3.1 / AV=N / AC=H / PR=N / UI=N / S=C / C=L / I=H / A=H

Exploit

Debido a la falta de aleatoriedad de las claves privadas generadas, un atacante podría ser capaz de adivinar fácilmente la parte privada de una clave remota para así acceder de forma remota a la sesión o hacer un ataque Man In The Middle.^{vii}

Solución

Como solución no solo habría que actualizar la versión de OpenSSL, sino que sería necesario volver a generar, esta vez con una entropía más adecuada, las claves de SSL, SSH y OpenVPN que puedan haber sido generadas con este error, en concreto desde la 0.9.8c-1.

Además de ello, también se recomienda que todas las claves DSA que se hayan usado en el entorno Debian desde que el equipo ha estado comprometido se consideren como vulnerables y se vuelvan a generar también.

4.5. rexecd Service Detection^{viii ix}

Descripción del problema

El servicio rexecd está diseñado para proporcionar a usuarios remotos la posibilidad de ejecución remota por medio de una autenticación basada en nombres de usuario y contraseñas. Se inicia cuando inetd recibe una solicitud de servicio en el puerto indicado por un comando exec.

La vulnerabilidad da lugar cuando un atacante usa rexecd sin necesidad de ser autenticado.

CVSS

Base Score: 8.3

CVSS: 3.1 / AV=N / AC=L / PR=N / UI=N / S=C / C= L / I=L / A=L

Exploit

El problema de esta vulnerabilidad es que rexecd puede ser utilizado por un atacante sin necesidad de ser correctamente autenticado. De esa forma, el hacker podría hacer un escaneo completo del host.^x

Solución

Los "R Services" ya están en desuso debido a que son unos servicios de comandos de los 80 con un sistema de autenticación insuficientemente encriptado, de forma que han dado muchos problemas y han sido reemplazados por ssh y telnet.

Si el usuario aún así quisiera seguir usando rexecd podría quitar la línea de 'exec' en /etc/inetd.conf y reiniciar el proceso inetd.

4.6. Bind Shell Backdoor Detection^{xi}

Descripción del problema

Una Bind Shell es una terminal que está "escuchando" en un puerto en concreto de manera que se le pueden enviar comandos a través de la red para su ejecución sin necesidad de autenticación.

Normalmente es abierta por alguien que ha aprovechado otra vulnerabilidad para tomar de manera sencilla el control del PC atacado.

CVSS

Base Score : 9.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

(No tiene sentido hacer una temporal score ya que no es una vulnerabilidad del SO per se)

Exploit

Un atacante puede conectarse a la shell mediante Telnet o equivalente y enviar comandos hacia el PC comprometido

Solución

Verificar como ha sido comprometido el PC atacado y si es necesario reinstalar el SO

4.7. VNC Server 'password' Password^{xii}

Descripción del problema

VNC es un programa que nos permite controlar un ordenador de manera remota viendo la pantalla del mismo y manejando el ratón y teclado mediante el protocolo RFB.

Para conectarse a un ordenador se necesita una contraseña, "password" es una contraseña de diccionario de las más comunes en Internet y por lo tanto muy predecible y extremadamente débil.

CVSS

Base Score : 9.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

(No tiene sentido hacer una temporal score ya que no es una vulnerabilidad del SO per se)

Exploit

Para aprovechar esta vulnerabilidad un atacante sólo tiene que hacer un ataque de diccionario al servicio VNC y la contraseña debería salir en cuestión de segundos, dando control total al atacante sobre el PC.

O el propio escáner ya ha dado la contraseña así que solo sería loguearse usándola.

Solución

- Cambiar la contraseña a una más robusta.
- Desactivar el servicio VNC

4.8. MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (unauthenticated check)^{xiii xiv xv}

Descripción del problema

El servicio server ofrece una interfaz RPC (Llamadas a procedimientos remotos) que se puede usar para impresión, compartir archivos o compartición de pipes con nombre en entornos de red, el problema es que hay un desbordamiento de buffer en este servicio que permite ataques de denegación de servicio o la ejecución de código arbitrario.

(CVE-2006-3439)

Un desbordamiento de buffer consiste en un error de software que ocurre cuando un programa no controla la cantidad de datos que se escriben en la zona de memoria reservada con tal efecto, de manera que si supera la capacidad pre-asignada la información sobrante se almacena en zonas de memoria adyacentes las cuales pueden tener otros datos o código de otro programa almacenados en memoria.

Esto se puede usar para sobrescribir el funcionamiento de un programa y alterar su flujo de ejecución natural para realizar operaciones y procedimientos no previstos originalmente, constituye un fallo muy grave de seguridad cuando el programa en cuestión tiene privilegios de administrador.

CVSS

Base Score : 9.8

Temporal Score: 9.4

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Exploit

Un atacante sin necesidad de identificarse puede enviar un mensaje especialmente fabricado a la máquina vulnerable de forma remota y provocar el desbordamiento del buffer y de esta manera aprovechar la vulnerabilidad.^{xvi}

Solución

- Actualizar Windows
- Restringir el acceso SMB en los puertos 139/tcp y 445/tcp de redes desconocidas a través de internet
- Restringir el acceso anónimo de SMB, sin embargo esto no evita el ataque por parte de usuarios identificados

4.9. MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)^{xvii} xviii xix xx xxi xxii xxiii

Descripción del problema

- (EternalBlue)

Eternalblue funciona en todas las versiones anteriores a Windows 8, estas versiones tienen un interproceso de comunicación compartido (IPC\$) que permite una sesión “null” la cual puede ser establecida por un usuario anónimo.

Eternalblue usa 3 bugs para conseguir esto

Bug A “Wrong casting bug”

Un bug en el proceso de convertir FEA con estructura Os2 a estructura NT por parte de la implementación de SMB de Windows da lugar a un desbordamiento de buffer en la parte no paginada del kernel

Bug B “Wrong parsing bug”

Cuando se transmite un archivo por SMB hay varias funciones relacionadas con los datos

SMB_COM_TRANSACTION2 y SMB_COM_NT_TRANSACT (El cual extiende las funciones del anterior y permite transferir grandes cantidades de datos)

Cuando hay una transferencia de datos que excede el buffer inicial de cualquiera de estas dos funciones se usa el comando _SECONDARY

SMB_COM_TRANSACTION2 usa el tamaño Word
SMB_COM_NT_TRANSACT usa el tamaño Dword

El problema proviene de que no hay validación de qué función empezó la transacción y se parsea en función de la anterior, es decir, es posible hacer un SMB_COM_NT_TRANSACT seguido de SMB_COM_TRANSACTION2_SECONDARY lo cual da lugar al bug A

Bug C “Non-paged Pool Allocation Bug”

Hay un bug que permite localizar un “chunk” de memoria de un tamaño específico en la memoria no paginada del kernel, este chunk de memoria es posteriormente vaciado y

rellenado con datos creando un "out of bound" y escribiendo en el siguiente chunk de memoria.

Todo esto se lleva a cabo con el protocolo SMB

- (EternalChampion), (EternalRomance) y (EternalSynergy)

Funciona igual que EternalBlue pero usa una pipe con nombre en vez de solo necesitar el IPC\$, sin embargo, no hay posibilidad de crashear el sistema como hace Eternalblue

(CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148)

CVSS

Base Score: 8.1

Temporal Score: 7.7

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Exploit

Un atacante puede explotar estas vulnerabilidad para la ejecución de código arbitrario en el PC atacado y conseguir información confidencial.

Soluciones

- Actualizar el SO
- Desactivar SMBv1
- Bloquear el puerto TCP 445 en todas las redes exteriores

4.10. Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)^{xxiv xxv}

Descripción del Problema

La vulnerabilidad está relacionada con la solicitud "MCS Connect Initial and GCC Create" que contiene información relacionada con la seguridad, información de creación de canales virtuales y otras capacidades del cliente RDP.

El protocolo RDP soporta canales virtuales estáticos, que están destinados a ser utilizados como enlaces de comunicación para varios componentes RDP y extensiones de usuario.

Windows crea dos canales por defecto: MS_T120 (utilizado para el propio RDP) y CTXTW (utilizado en Citrix ICA). No se espera que el cliente los cree a través de la red, en su lugar

son inicializados internamente por el sistema RDP de Windows cuando se establece una conexión.

Los canales virtuales se crean mediante la función *IcaCreateChannel()* dentro del controlador del kernel termdd que primero comprueba si el canal específico existe. Si no existe, entonces asigna una "channel structure" para crearlo. Un puntero a la "channel structure", que llamamos *ChannelControlStructure*, se almacena dentro de una tabla, también conocida como *ChannelPointerTable*.

Todas las conexiones RDP comienzan con esta vista de la *ChannelPointerTable* (los primeros cinco slots no son controlados por el usuario y por lo tanto no se muestran. En su lugar, el slot 0 se toma como el primer canal escribible por el cliente)

Cada slot puede almacenar un puntero *ChannelControlStructure*. Cuando un cliente RDP se conecta y abre canales, las *ChannelControlStructures* correspondientes se crean y su puntero se almacena en la *ChannelPointerTable* comenzando por el slot 0. CTXTW siempre está presente en el slot 7, y MS_T120 en el slot 0x1F.

Si se especifica un canal con nombre "MS_T120\x00" (por ejemplo, en el slot 10), *IcaCreateChannel()* llama a *IcaFindChannelByName()* y devuelve la *ChannelControlStructure* apuntada por la estructura MS_T120 en el slot 0x1F. Este puntero (el mismo que el del slot 0x1F) se almacena en el slot especificado por el usuario.

Después, cuando se abren los canales mediante "MCS Channel Join Request", el canal MS_T120 también se abre con éxito.

Si un atacante envía datos falsos en el canal MS_T120, termdd.sys intenta responder al mensaje enviando un mensaje de error y cerrando el canal mediante *IcaCloseChannel()*, que a su vez llama a *IcaFreeChannel()*, liberando la MS_T120 *ChannelControlStructure* y borrando el puntero en la ranura controlada por el usuario en *ChannelPointerTable*.

Sin embargo, el mismo puntero en la ranura 0x1F no se borra.

Posteriormente, cuando la conexión termina, se invoca a *RDPWD!SignalBrokenConnection()* que a su vez llama a *IcaChannelInputInternal()* e intenta escribir en la estructura *ChannelControlStructure* utilizando el puntero del slot 0x1F. Esto lleva a una condición "use-after-free".

El use after free es similar a la estrategia usada en el bug C de EternalBlue, hacer referencia a una dirección de memoria después de haberla liberado para hacer que un programa se bloquee, utilice valores inesperados o ejecute código.

(CVE-2019-0708)

CVSS

Base Score: 9.8

Temporal Score: 9.4

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Exploit

Ataque DDOS o ejecución de código arbitrario con privilegios de SYSTEM de forma remota a través de un paquete especialmente fabricado.

Soluciones

- Actualizar el SO
- Desactivar el servicio RDP

5. Bibliografía

-
- ⁱ <https://www.tenable.com/plugins/nessus/18502>
 - ⁱⁱ <https://www.tenable.com/plugins/nessus/34477>.
 - ⁱⁱⁱ <https://www.exploit-db.com/exploits/7132>
 - ^{iv} <https://www.tenable.com/plugins/nessus/79638>
 - ^v <https://www.securitysift.com/exploiting-ms14-066-cve-2014-6321-aka-winshock/>
 - ^{vi} <https://www.tenable.com/plugins/nessus/32321>
 - ^{vii} <https://blog.segu-info.com.ar/2008/07/expotando-dsa-1571-cmo-romper-pfs-en.html>.
 - ^{viii} <https://www.tenable.com/plugins/nessus/10203>
 - ^{ix} http://www.qnx.com/developers/docs/qnx_4.25_docs/tcpip50/user_guide/utls/rexecd.html.
 - ^x https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/scanner/rservices/rexec_login.md
 - ^{xi} <https://www.tenable.com/plugins/nessus/51988>
 - ^{xii} <https://www.tenable.com/plugins/nessus/61708>
 - ^{xiii} <https://www.tenable.com/plugins/nessus/22194>
 - ^{xiv} <https://www.kb.cert.org/vuls/id/650769>
 - ^{xv} https://en.wikipedia.org/wiki/Buffer_overflow
 - ^{xvi} <https://www.exploit-db.com/exploits/2223>
 - ^{xvii} <https://www.tenable.com/plugins/nessus/97833>
 - ^{xviii} <https://research.checkpoint.com/2017/eternalblue-everything-know/>
 - ^{xix} <https://research.checkpoint.com/2017/eternalblue-everything-know/>
 - ^{xx} <https://msrc-blog.microsoft.com/2017/06/29/eternal-champion-exploit-analysis/>
 - ^{xxi} <https://msrc-blog.microsoft.com/2017/07/13/eternal-synergy-exploit-analysis/>
 - ^{xxii} https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_psexec/
 - ^{xxiii} <https://github.com/worawit/MS17-010>
 - ^{xxiv} <https://www.tenable.com/plugins/nessus/125313>
 - ^{xxv} <https://cyobs.ch/Dreamlab-The-Bluekeep-Threat-2019.pdf>