


Pobranie Metasploitable i uruchomienie maszyny wirtualnej

Home / Browse / Security & Utilities / Security / Metasploitable



Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine
Brought to you by: [rapid7user](#)

★★★★★ 6 Reviews

Downloads: 9,627 This Week

Oracle VM VirtualBox Menedżer

Plik Maszyna Pomoc

Tools

metasploitable Wyłączona

Nowa Ustawienia Odrzuć Uruchom

Ogólne

Nazwa: metasploitable
System operacyjny: Oracle (64-bit)

System

RAM: 1024 MB
Boot Order: Floppy, Napęd optyczny, Dysk twardy
Akceleracja: VT-x/AMD-V, Zagnieżdżone stronicowanie, PAE/NX, Parawirtualizacja KVM

Ekran

Pamięć wideo: 16 MB
Graphics Controller: VMSVGA
Serwer pulpitu zdalnego: Disabled
Recording: Disabled

Pamięć

Kontroler: IDE
IDE Secondary Master: [Napęd optyczny] Brak
Kontroler: SATA
Port SATA 0: Metasploitable.vmdk (Normalny, 8,00 GB)

Dźwięk

Sterownik gospodarza: Windows DirectSound
Controller: ICH AC97

Network

Karta 1: Intel PRO/1000 MT Desktop (NAT)

USB

Kontroler USB: OHCI, EHCI
Filtry urządzeń: 0 (aktywne: 0)

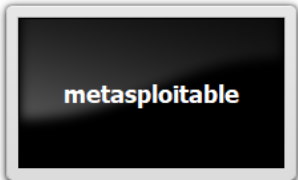
Udostępniane foldery

Brak

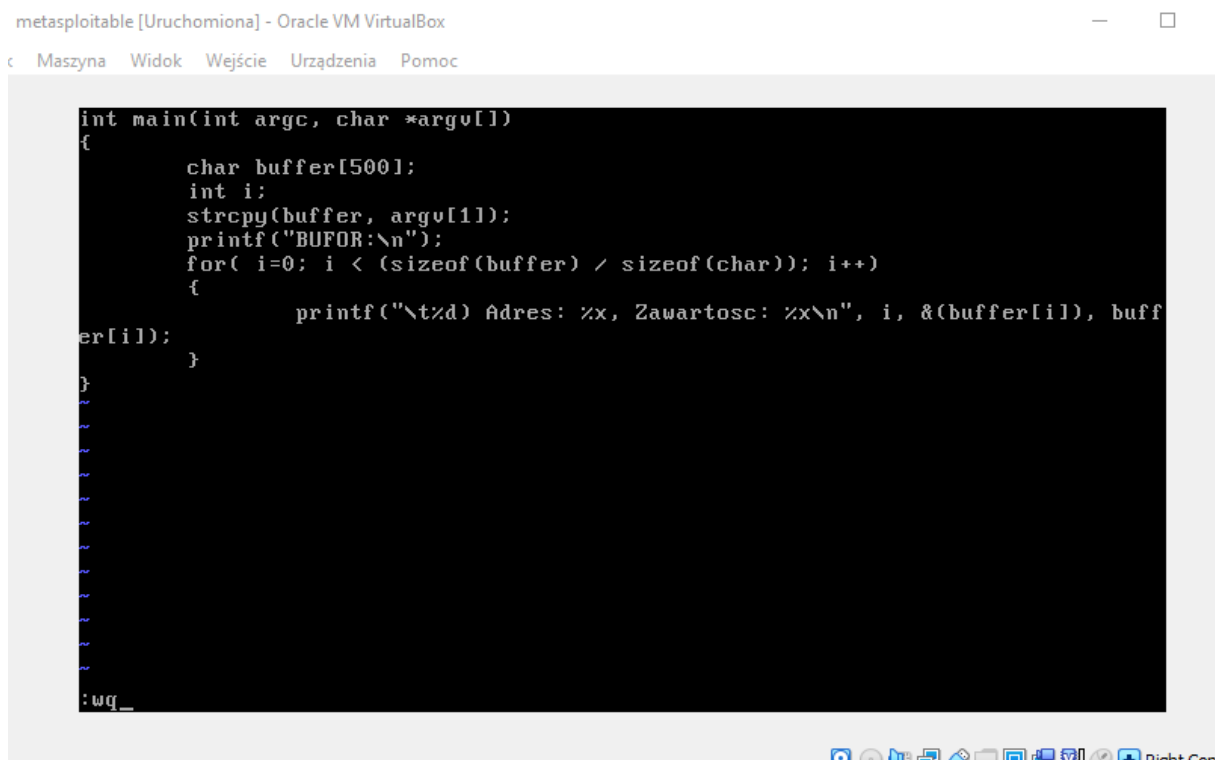
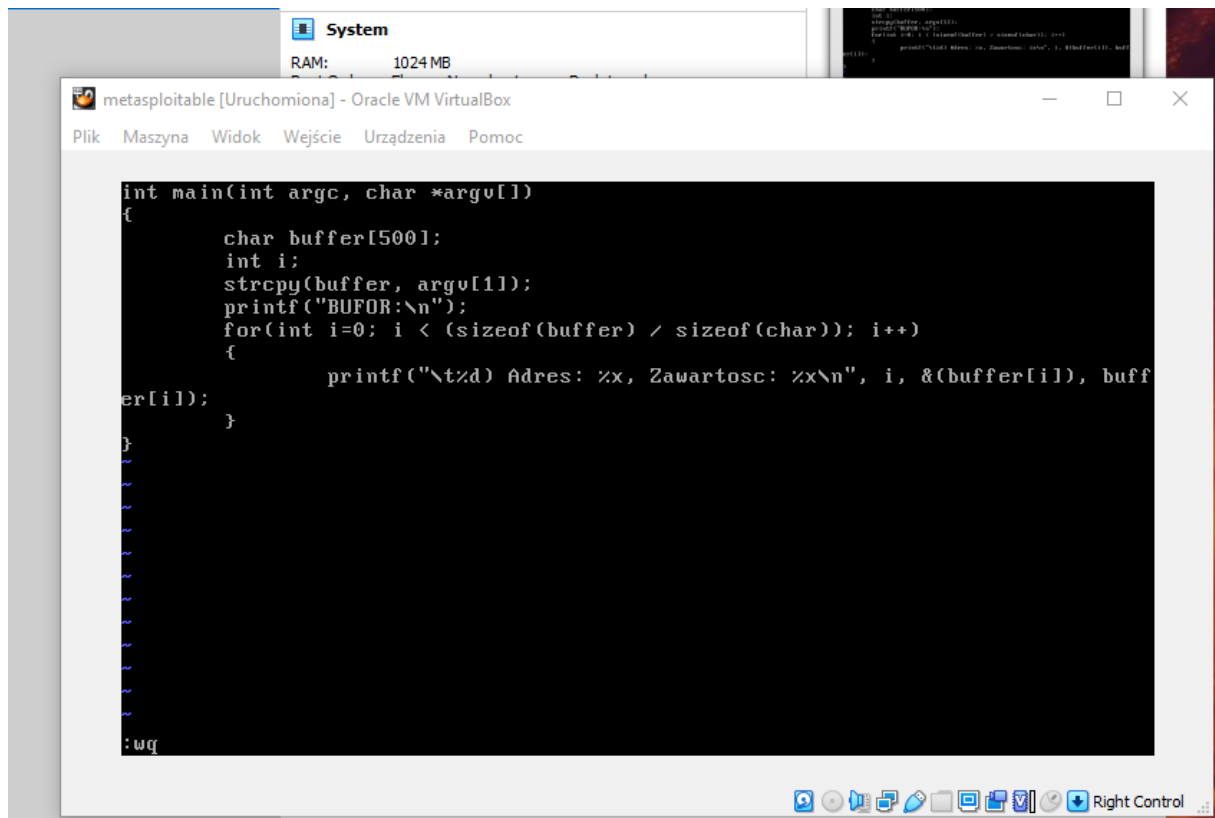
Opis

Brak

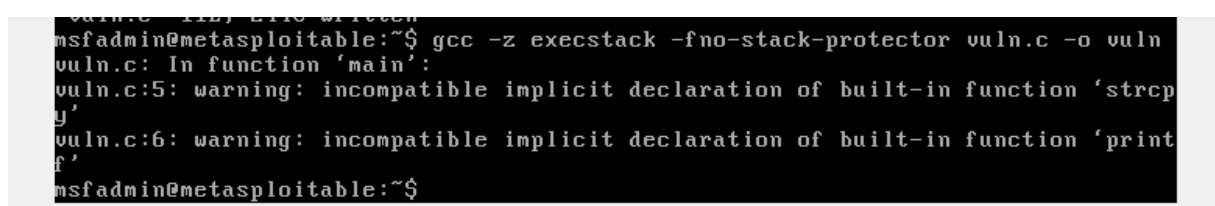
Podgląd



Przygotowanie programu do ataku (vuln.c)



Kompilacja pozwalająca na wykonanie ataku



Przetestowanie

```
msfadmin@metasploitable:~$ ./vuln aaa
BUFOR:
0) Adres: bfb4f01e, Zawartosc: 61
1) Adres: bfb4f01f, Zawartosc: 61
2) Adres: bfb4f020, Zawartosc: 61
3) Adres: bfb4f021, Zawartosc: 61
4) Adres: bfb4f022, Zawartosc: 0
5) Adres: bfb4f023, Zawartosc: 0
6) Adres: bfb4f024, Zawartosc: 1
7) Adres: bfb4f025, Zawartosc: 0
8) Adres: bfb4f026, Zawartosc: 0
```

Przesłanie pliku shellcode.bin na maszynę

```
msfadmin@metasploitable:~$ ls -la
total 52
drwxr-xr-x 5 msfadmin msfadmin 4096 2022-01-10 13:53 .
drwxr-xr-x 6 root      root      4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root      root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
-rw----- 1 root      root      4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
-rw-r--r-- 1 msfadmin msfadmin  46 2022-01-10 12:59 shellcode.bin
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
-rwxr-xr-x 1 msfadmin msfadmin 6653 2022-01-10 12:58 vuln
-rw-r--r-- 1 msfadmin msfadmin  244 2022-01-10 13:51 vuln.c
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$
```

Wywołanie

„setarch `uname -m` -R” – wyłącza tymczasowo „Address space layout randomization”

```
msfadmin@metasploitable:~$ setarch `uname -m` -R ./vuln aaaaaa
BUFOR:
0) Adres: bffffcbe, Zawartosc: 61
1) Adres: bffffcbf, Zawartosc: 61
2) Adres: bffffcc0, Zawartosc: 61
3) Adres: bffffcc1, Zawartosc: 61
4) Adres: bffffcc2, Zawartosc: 61
5) Adres: bffffcc3, Zawartosc: 61
6) Adres: bffffcc4, Zawartosc: 0
7) Adres: bffffcc5, Zawartosc: 0
8) Adres: bffffcc6, Zawartosc: 0
```

Wybranie adresu „bffff78”

```
segmentation fault
msfadmin@metasploitable:~$ setarch `uname -m` -R ./vuln `perl -e 'print "\x90\x100;'"`cat shellcode.bin`perl -e 'print "\x78\xfb\xff\xbf\x50";'
```

Poszukiwany adres

```
msfadmin@metasploitable:~$ setarch `uname -m` -R ./adr  
bffffd00
```

Wyliczona odległość początku bufora od adresu powrotu

Decimal value:

$3221224704 - 3221223694 = 1010$

<input type="text" value="bffffd00"/>	-	<input type="text" value="bffff90e"/>	= ?
<input type="button" value="Calculate"/>		<input type="button" value="Clear"/>	

Pomimo wielu prób i różnych sposobów podejść nie udało się przeprowadzić ataku (uruchomić shellcode)

```
528) Adres: bffffb1c, Zawartosc: 50  
529) Adres: bffffb1d, Zawartosc: 4  
530) Adres: bffffb1e, Zawartosc: ffffffff  
531) Adres: bffffb1f, Zawartosc: ffffffff  
532) Adres: bffffb20, Zawartosc: 2  
533) Adres: bffffb21, Zawartosc: 0  
534) Adres: bffffb22, Zawartosc: 0  
535) Adres: bffffb23, Zawartosc: 0  
536) Adres: bffffb24, Zawartosc: ffffffff  
537) Adres: bffffb25, Zawartosc: ffffffff  
538) Adres: bffffb26, Zawartosc: ffffffff  
539) Adres: bffffb27, Zawartosc: ffffffff  
Segmentation fault  
msfadmin@metasploitable:~$
```