Reverse Shell
+
Shell Spawning

DURATION : 0’30

© Nicolas VIEUX Version : 2024.01

Reverse Shell

© Nicolas VIEUX

What is a Reverse Shell ?

- A reverse shell or a remote shell takes advantage of the target system's vulnerabilities to initiate a shell session and then access the victim's computer.
- The goal is to connect to a remote computer and redirect the input and output connections of the target system's shell so the attacker can access it remotely.
- Reverse shells allow attackers to open ports to the target machines, forcing communication and enabling a complete takeover of the target machine. Therefore it is a severe security threat. This method is also commonly used in penetration tests.

How Does a Reverse Shell Work ? 1/2

- In a standard remote shell attack, attackers connect a machine they control to the target's remote network host, requesting a shell session.
- This tactic is known as a bind shell. Attackers can use a reverse shell if a remote host is not publicly accessible (i.e., due to firewall protection or a non-public IP). The target machine initiates the outgoing connection in a reverse shell attack and establishes the shell session with the listening network host.
- For hosts protected by a network address translation (NAT), a reverse shell may be necessary for performing maintenance remotely.
- Although there are legitimate uses for reverse shells, cybercriminals also use them to penetrate protected hosts and perform operating system commands.

How Does a Reverse Shell Work ? 2/2

- Reverse shells allow attackers to bypass network security mechanisms like firewalls.
- Attackers can achieve reverse shell capabilities via phishing emails or malicious websites.
- If the victim installs the malware on a local workstation, it initiates an outgoing connection to the attacker's command server. An outgoing connection often succeeds because firewalls generally filter incoming traffic.
- An attacker may exploit command injection vulnerabilities on a server to compromise the system. In the injected code, a reverse shell script provides a command shell enabling additional malicious actions.

Where can I find a Reverse Shell ?

- Either you develop it yourself or you take it from the internet:
  - Online - Reverse Shell Generator : https://www.revshells.com/
  - Reverse Shell – Cheat Sheet : https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/
  - Create a Reverse Shell : https://www.golinuxcloud.com/create-reverse-shell-cheat-sheet/
  - PHP - Reverse Shell : https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Shell Spawning

Spawn a shell in a TTY shell

- Once you get a shell on the linux victim machine this shell could be without TTY (terminal connection) and most likely to go on with the penetration test you will need to spawn TTY shell.
- In fact, a shell without the TTY functions does not allow you to perform important things such as the simple “su” command that is used to change user or the “nano” file creation and modification tool. There are other important functions in a penetration test which don’t work on a shell without TTY.
- So to spawn a shell in a TTY shell there are some useful commands. These must be run from within the not TTY shell.

How can I spawn full TTY shell

- Command line to spawn a full TTY shell :
  - python3 -c 'import pty; pty.spawn("/bin/bash")'
  - python -c 'import pty; pty.spawn("/bin/sh")'
  - echo os.system('/bin/bash')
  - /bin/sh -i
  - script -qc /bin/bash /dev/null
  - perl -e 'exec "/bin/sh";'
  - Etc.
- For more information :
  - https://github.com/curtishoughton/Penetration-Testing-Cheat-Sheet/blob/master/Techniques/spawning-tty.md