Pivoting

In a corporate environment, most of the machines are behind a firewall, which makes it impossible to attack them directly. However, if there is a vulnerable machine exposed to the internet which is also connected to the internal network. It might be possible to pivot through the compromised machine and attack the machines on the internal network. The objective of this section is to teach the various pivoting techniques that can be used to attack machines behind a network.

What will you learn?

- Pivoting through a machine by using ssh tunnels
- Using the Meterpreter autoroute script to route traffic through a compromised machine
- Using the Metasploit socks proxy module to proxy traffic through a machine
- Pivoting through a machine by using reGorg

References:

1. Pentesting with Metasploit (https://www.pentesteracademy.com/course?id=10)

Labs:

Basics:

- Pivoting I
  - Objective: Compromise the target B machine which is located behind target A machine. Use Meterpreter autoroute script for pivoting
- Pivoting IV
  - Objective: Compromise the target B machine which is located behind target A machine. Use Meterpreter autoroute script, Metasploit socks4a module and proxychains for pivoting
- Pivoting VI
  - Objective: Compromise the target B machine which is located behind target A machine. Use SSH tunnel and proxychains for pivoting
- Pivoting VII
  - Objective: Compromise the target B machine which is located behind target A machine. Use SSH tunnel and proxychains for pivoting
- Pivoting VIII
  - Objective: Compromise the target B machine which is located behind target A machine. Use reGorg and proxychains for pivoting

More labs for this topic are available under the Network Pivoting and Metasploit section on AttackDefense.