# Pivoting in Penetration Testing: A Comprehensive Guide

0verlo0ked · Follow
Published in InfoSec Write-ups
4 min read · Nov 18, 2024

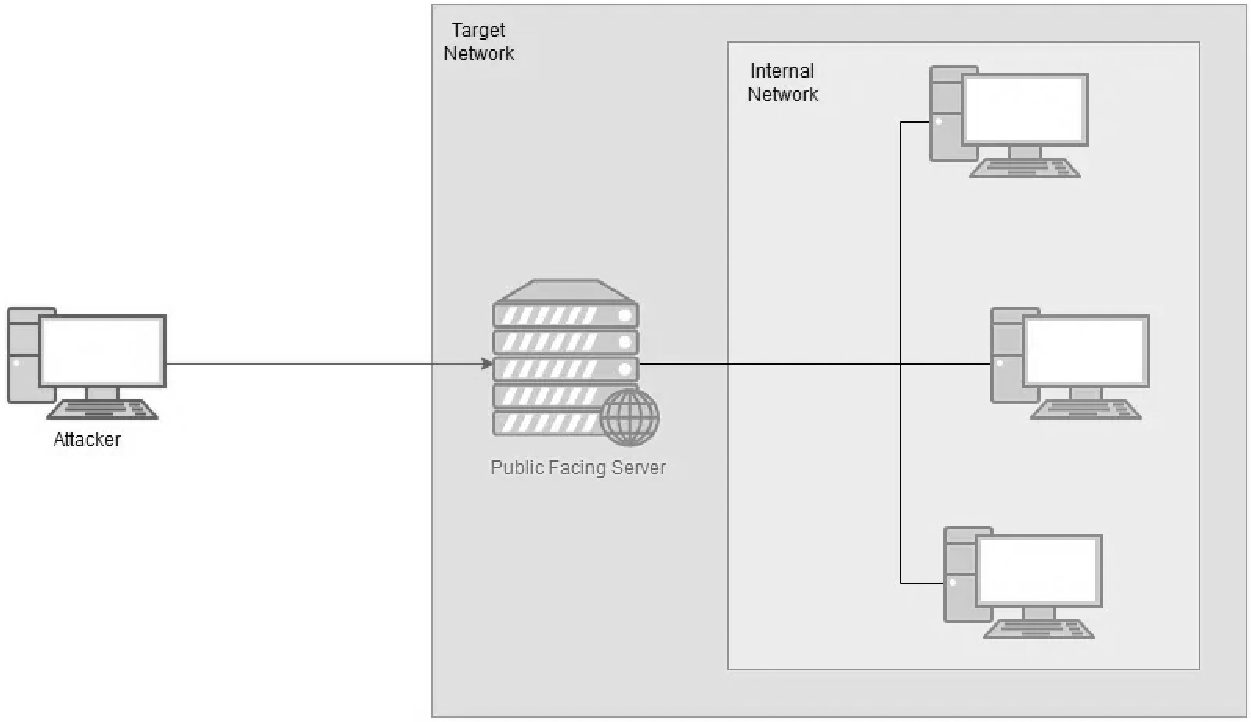
***Pivoting** is a vital technique in penetration testing that allows an attacker to exploit a compromised system to access deeper layers of a target network. It's the art of leveraging initial access to one machine to explore, exploit, and gain control over other machines in the same network. This guide delves into the essentials of pivoting, providing practical techniques and tools to enhance your understanding.*

## Why Pivoting is Essential ?

Most networks are segmented, with sensitive systems hidden behind layers of security. Initial access, such as exploiting a public-facing server, rarely grants direct access to critical systems. Pivoting bridges this gap, enabling lateral movement within the network to target these hidden assets.

**Example Scenario:** Imagine a network with four machines:

- One **public-facing server** exposed to the internet.
- Three **internal machines** inaccessible from outside.



By compromising the public-facing server, you can use it as a gateway to pivot into the internal network and attack the remaining targets.

## Core Techniques in Pivoting

Pivoting revolves around two main methodologies:

1. **Tunneling/Proxying**
2. **Port Forwarding**

## 1. Tunneling/Proxying

**Definition:**
Tunneling or proxying involves creating a route for all desired traffic through the compromised host. This can include protocols like HTTP, SSH, or even custom proxies to route traffic into the target network.

**Key Tools:**

- **Proxychains:** A Linux tool that redirects local traffic through a proxy.

- **FoxyProxy:** A browser extension to manage proxy configurations.
- **SSH Tunneling:** A versatile method using SSH to redirect traffic.
- **Socat**: A multipurpose relay tool for forwarding traffic.
- **Chisel:** A fast, cross-platform tool for creating HTTP tunnels.
- **sshuttle:** A simple VPN-like solution for tunneling (Unix-based).

**When to Use:**
Tunneling is ideal for:

- Redirecting multiple traffic types.
- Scanning internal subnets with tools like Nmap.
- Accessing multiple services across multiple machines.

## 2. Port Forwarding

**Definition:**
Port forwarding involves linking a port on your local machine to a specific port on the target machine via the compromised host. It's faster and more reliable than tunneling but is limited to specific ports.

**Key Tools:**

- **SSH Forwarding:** Redirect traffic using `ssh -L` for local forwarding or `ssh -R` for reverse forwarding.
- **Plink**: A lightweight command-line tool for SSH forwarding (Windows).
- **Socat**: A versatile choice for forwarding TCP/UDP ports.

**When to Use:**
Port forwarding is optimal for:

- Accessing a single service, such as an RDP or database.

- Testing vulnerabilities on specific ports.

## Enumeration: The First Step to Pivoting

Before pivoting, you must understand the network layout. The more information you gather, the better your chances of successful lateral movement.

## Enumeration Techniques

1. **Checking Existing Information on the Compromised Machine:**

- Use `arp -a` to inspect the ARP cache for nearby hosts.
- Look for DNS configurations (`/etc/resolv.conf` on Linux, `ipconfig /all` on Windows).
- Check static mappings in `/etc/hosts` or `C:\Windows\System32\drivers\etc\hosts`.

**2. Using Pre-Installed Tools:**

- Run `ping`, `traceroute`, or `netstat` to identify reachable systems.
- Some Linux systems might already have **Nmap** installed.

**3. Deploying Statically Compiled Tools:**

- Upload static binaries of tools like **Nmap**, **Netcat**, or **LinPEAS** if pre-installed options are unavailable. Statically compiled tools run without dependencies, making them versatile.

**4. Creating Simple Scripts:**

- Bash one-liner for ping sweep:

```
for i in {1..255}; do (ping -c 1 192.168.1.$i | grep "bytes from" &); done
```

- Check for open ports in Bash:

```
for i in {1..65535}; do (echo > /dev/tcp/192.168.1.1/$i) >/dev/null 2>&1 && ech
```

5. **Proxying Scans:**

- Use **proxychains** to redirect traffic from local tools to the internal network:

```
proxychains nmap -sT -Pn -p 80,443 192.168.1.1
```

## Practical Tools and Techniques

### 1. Proxychains Setup

Proxychains can route traffic from tools like Nmap or Metasploit through a compromised host. To use Proxychains:

1. Edit `/etc/proxychains.conf` to include the proxy:

```
socks4 127.0.0.1 9050
```

2. Run the desired command through Proxychains:

```
proxychains nmap -sT -p 22,80 192.168.1.1
```

### 2. SSH Tunneling

SSH can be used for both port forwarding and tunneling:

- **Local Forwarding:**

```
ssh -L 8080:192.168.1.2:80 user@target
```

- This command forwards traffic from your local port 8080 to port 80 on 192.168.1.2 .
- **Dynamic Forwarding (SOCKS Proxy):**

```
ssh -D 9050 user@target
```

- This creates a SOCKS proxy on port 9050.

### 3. Socat

Socat is excellent for forwarding or relaying traffic:

- Simple TCP forwarder:

```
socat TCP4-LISTEN:8080,fork TCP4:192.168.1.2:80
```

- Reverse shell setup:

```
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp-listen:4444
```

### 4. Chisel

Chisel allows for creating fast HTTP-based tunnels:

1. Start the server on your machine:

```
./chisel server -p 8000 --reverse
```

2. Connect from the target machine:

```
./chisel client 192.168.1.1:8000 R:8080:192.168.1.2:80
```

* * *

### Best Practices for Pivoting

1. **Prefer Native Tools:** Use pre-installed utilities to avoid detection.
2. **Stay Stealthy:** Avoid noisy scans; focus on targeted enumeration.
3. **Segment Analysis:** Understand each network layer before proceeding.
4. **Document Everything:** Maintain a network map to track your progress.

* * *

### Additional Resources

Provide links to documentation, tutorials, and open-source tools. For example:

- Chisel GitHub Repository
- Proxychains Documentation
- SSH Tunneling Guide

- Metasploit Pivoting Techniques

## Conclusion

Pivoting is a powerful skill that bridges the gap between initial access and complete network compromise. By mastering the tools and techniques outlined here, you'll be better prepared to navigate complex networks during penetration testing engagements.

*Remember: enumeration is your best friend, and the right combination of tools and creativity can make all the difference.*

Pentesting Writeup Ctf Ctf Writeup Pivoting

Follow

## Published in InfoSec Write-ups

49K Followers · Last published 1 hour ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

## Written by 0verlo0ked

59 Followers · 10 Following

Fueled by Caffeine . Join me as I share rare insights and unconventional tricks to level up in the world of hacking.