PivotSuite : Hack The Hidden Network – A Network Pivoting Toolkit

DISCLAIMER: This Information / Toolkit is for educational purposes only. Author is not responsible for its use

Manish Gupta

PivotSuite: Hack The Hidden Network

- Agenda

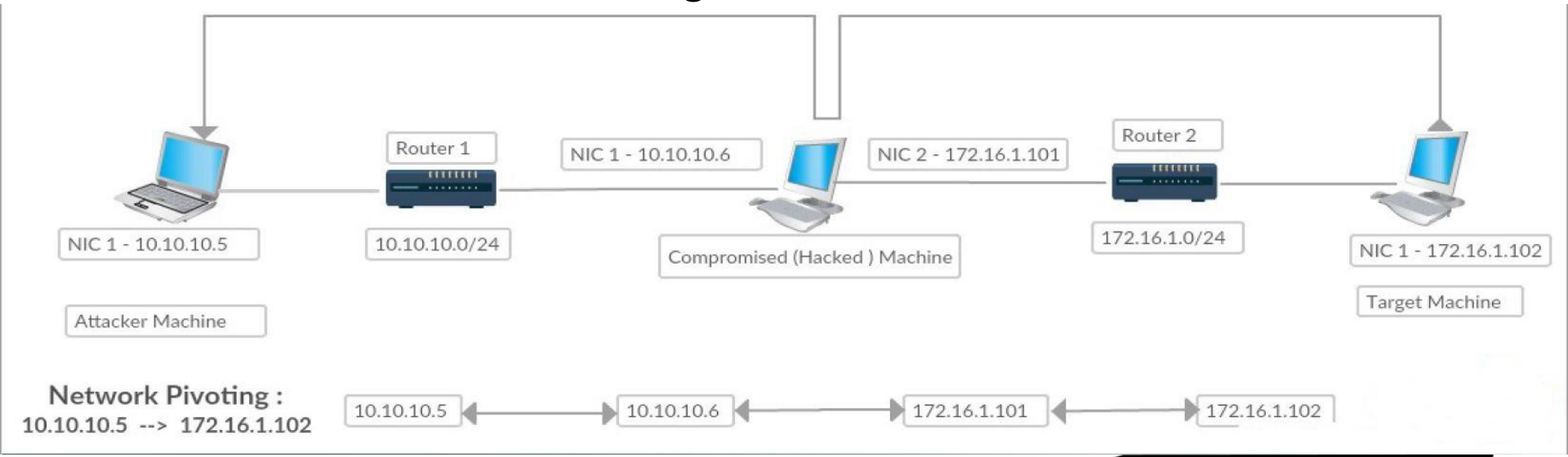
  - What is Network Pivoting ?
  - How to Perform Network Pivoting ?
  - Problem Statement : Real Time Network Pivoting Scenarios
  - Solutions : Network Pivoting using PivotSuite
  - Key Features and Advantages of PivotSuite

1. What is Network Pivoting ?

- Pivoting is a technique that route the traffic from a hacked computer toward other networks that are not accessible by a hacker machine
- Pivoting is a technique that use a compromised system to move around inside a network.

PivotSuite: Hack The Hidden Network

1. What is Network Pivoting ?



2. How to Perform Network Pivoting ?

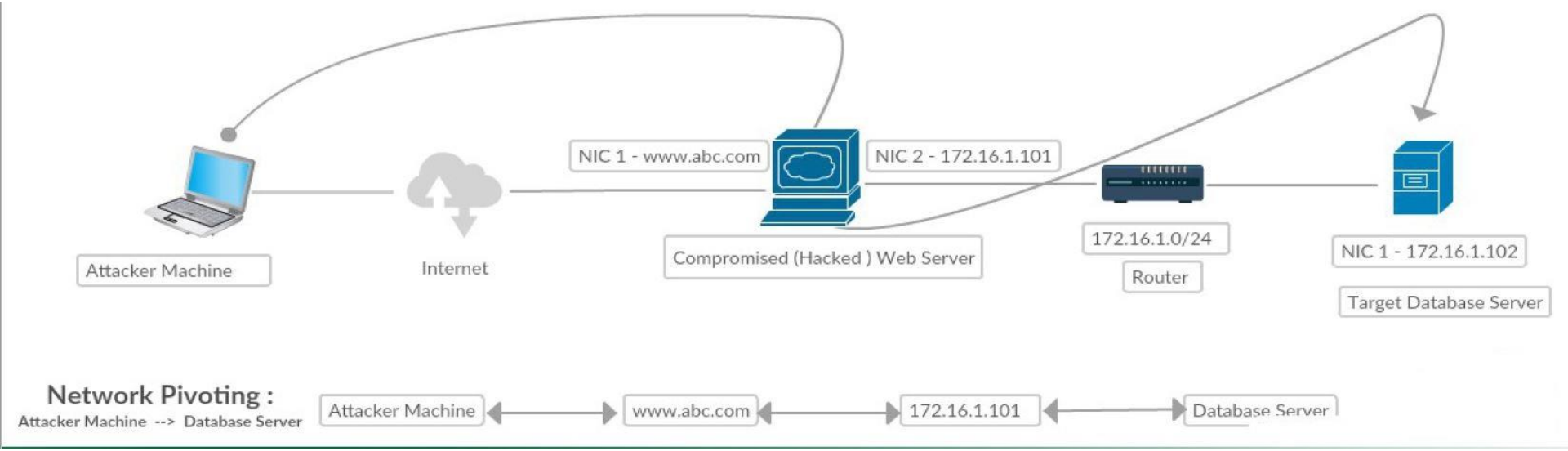
- Tunnelling
- Port Forwarding
- TCP Relay
- Proxy Server
- Dynamic Port Forwarding (Socks Proxy)

3. Real Time Network Pivoting Scenarios

- **Forward Connection -** If the compromised host is directly accessible (Forward Connection) from Our pen-test (Hacker Machine). E.g. Webserver

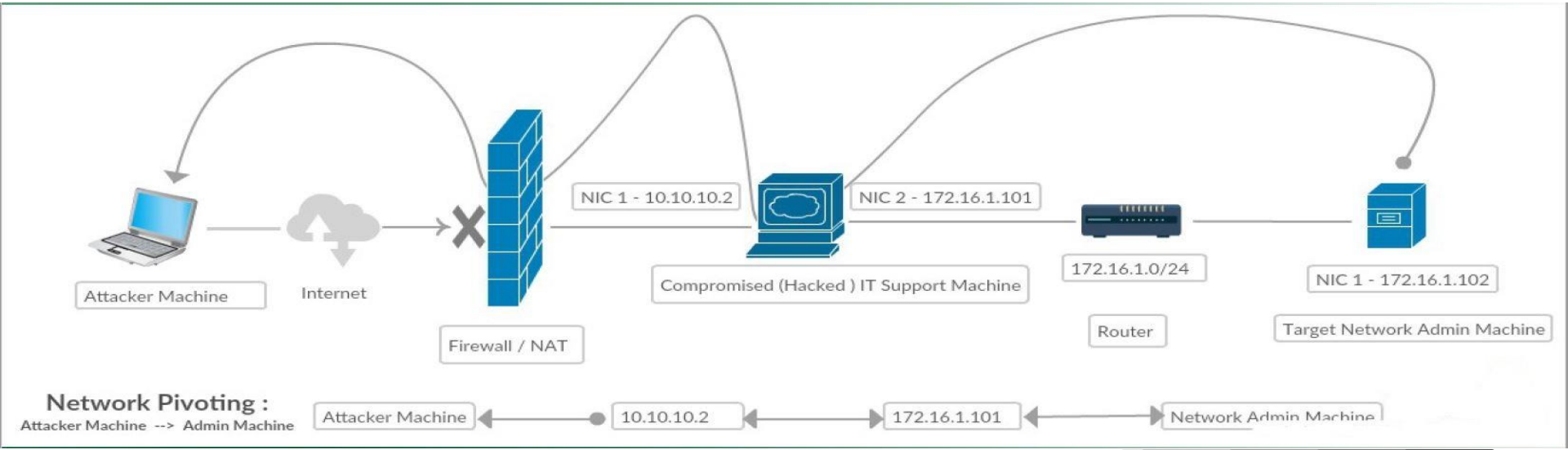
- **Reverse Connection -** If the compromised host is behind a Firewall / NAT and isn't directly accessible from our pen-test machine. E.g. Enterprise Internal System

3.1 Forward Connection -



PivotSuite: Hack The Hidden Network

3.2 Reverse Connection -



4. Network Pivoting using PivotSuite

Introduction About PivotSuite:

PivotSuite is a portable, platform independent and powerful network pivoting toolkit, Which helps Red Teamers / Penetration Testers to use a compromised system to move around inside a network. It is a Standalone Utility, Which can use as a Server or as a Client.

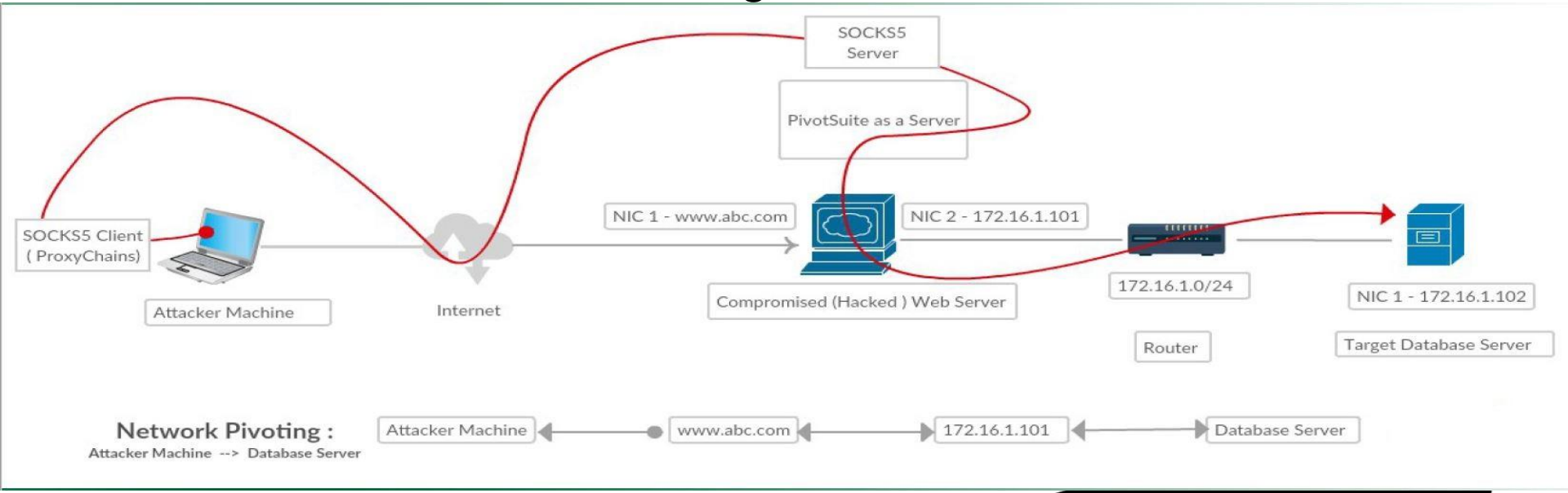
4.1 Forward Connection using PivotSuite

PivotSuite as a Server :

If the compromised host is directly accessible (Forward Connection) from Our pen-test machine, Then we can run **PivotSuite as a server on compromised machine** and access the different subnet hosts from our pen-test machine, Which was only accessible from compromised machine.

PivotSuite: Hack The Hidden Network

4.1 Forward Connection using PivotSuite

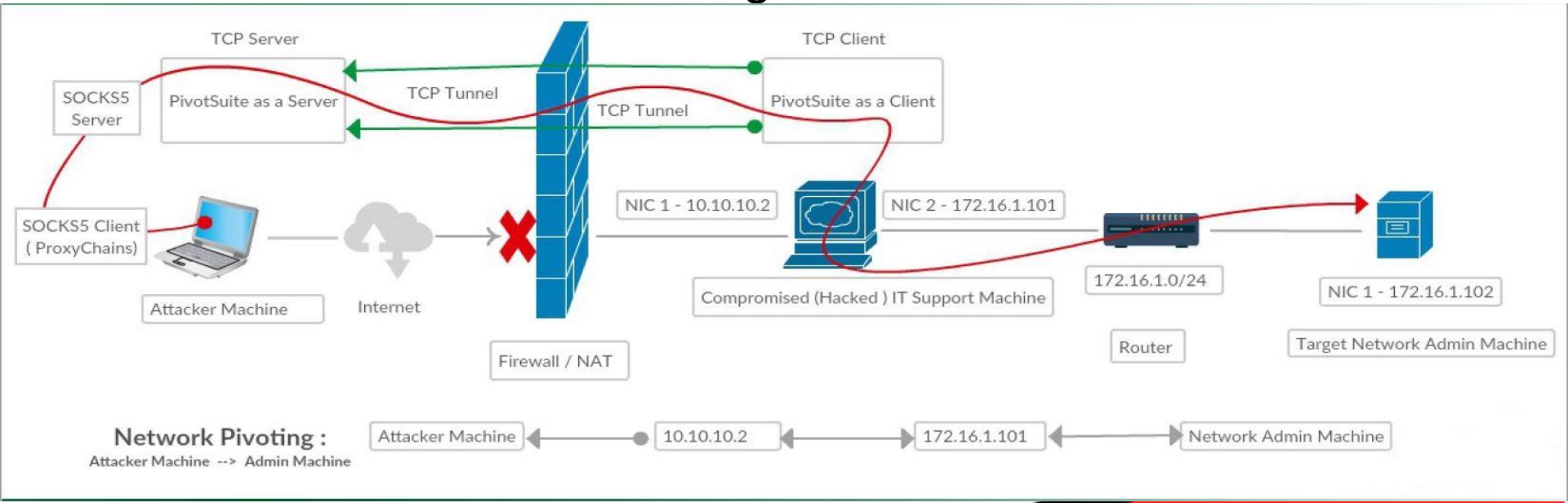


4.2 Reverse Connection using PivotSuite

PivotSuite as Client & Server :

If the compromised host is behind a Firewall / NAT and isn't directly accessible from our pen-test machine, Then we can run **PivotSuite as a server on pen-test machine** and **PivotSuite as a client on compromised machine** for creating a reverse tunnel (Reverse Connection). Using this we can reach different subnet hosts from our pen-test machine, which was only accessible from compromised machine.

4.2 Reverse Connection using PivotSuite



5.1 Key Features

- Supported Forward & Reverse TCP Tunnelling
- Supported Forward & Reverse socks5 Proxy Server
- UDP over TCP and TCP over TCP Protocol Supported
- Corporate Proxy Authentication (NTLM) Supported
- Inbuilt Network Enumeration Functionality, E.g.. Host Discovery, Port Scanning, OS Command Execution
- PivotSuite allows to get access to different Compromised host and their network, simultaneously (Act as C&C Server)
- Single Pivoting, Double Pivoting and Multi-level pivoting can perform with help of PivotSuite.
- PivotSuite also works as SSH Dynamic Port Forwarding but in the Reverse Direction.

5.2 Advantage Over Other tools:

- Doesn't required admin/root access on Compromised host
- PivotSuite also works when Compromised host is behind a Firewall / NAT, When Only Reverse Connection is allowed.
- No dependency other than python standard libraries.
- No Installation Required
- UDP Port is accessible over TCP

AHMEDABAD BSIDES

Thank You

Feedback & Suggestion

Email:

admin@myhacker.online

Manish Gupta