

Forum:[Hack Forums](#)

Thread: [PivotSuite - A Network Pivoting Toolkit](#)

owenhackz - July 13, 2019, 9:56 am

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.

PivotSuite as a Server:

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

PivotSuite as a Client:

If the compromised host is behind a Firewall / NAT and isn't directly accessible from our pentest machine, Then we can run pivotsuite as a server on pentest 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 pentest machine, which was only accessible from compromised machine.

Key Features:

Supported Forward & Reverse TCP Tunneling

Supported Forward & Reverse socks5 Proxy Server

UDP over TCP and TCP over TCP Protocol Supported

Corporate Proxy Authentication (NTLM) Supported

Inbuilt Network Enumeration Functionality, Eg. 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.

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

Installation

You can download the latest version of pivotsuite by cloning the Git repository or PyPI Package.

Code:

git clone [GitHub - RedTeamOperations/PivotSuite: Network Pivoting Toolkit](#)

PivotSuite works out of the box with Python version 2.7.x and 3.6.x on any platform.

PivotSuite Standalone Executable Download from Github Release Section

[Releases RedTeamOperations/PivotSuite GitHub](#)

No installation require, No python interpreter require

Download PivotSuite