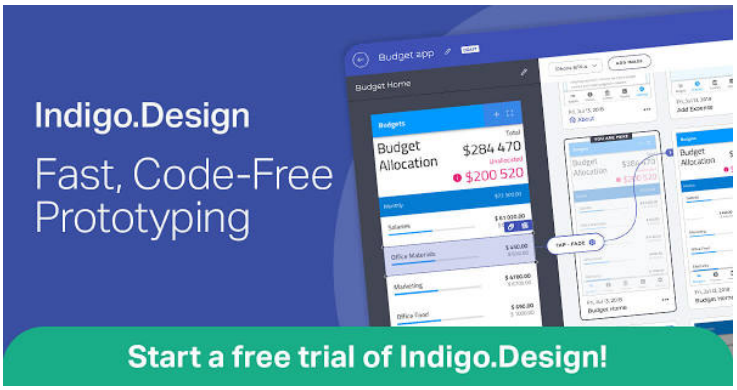


Infragistics

Code-Free Protc

Fast, code-free prototypir
Indigo.Design. Start your

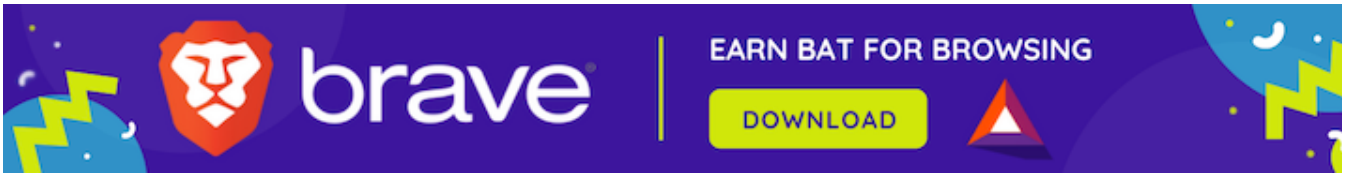
Leprechaun - Tool Used To Map Out The Network Data Flow To Help Penetration Testers Identify Potentially Valuable Targets

14 DAYS AGO 6:30 PM
ZION3R

The purpose of this tool is to help penetration testers identify potentially valuable targets on the internal network environment. By aggregating netstat routes from multiple hosts, you can easily figure out what's going on within.

Getting Started

These instructions will get you a copy of the project up and running on your local machine for development and testing purposes. See deployment for notes on how to deploy the project on a live system.



Prerequisites

You'll need a few Ruby gems to get started - if you don't have them already, that is.

```
r00t@r00t-KitPloit: ~
gem install 'securerandom'
gem install 'terminal-table'
gem install 'getopt'
```

Lastly, make sure you have Graphviz installed. You can install that with the following command:

```
apt install graphviz -y
```

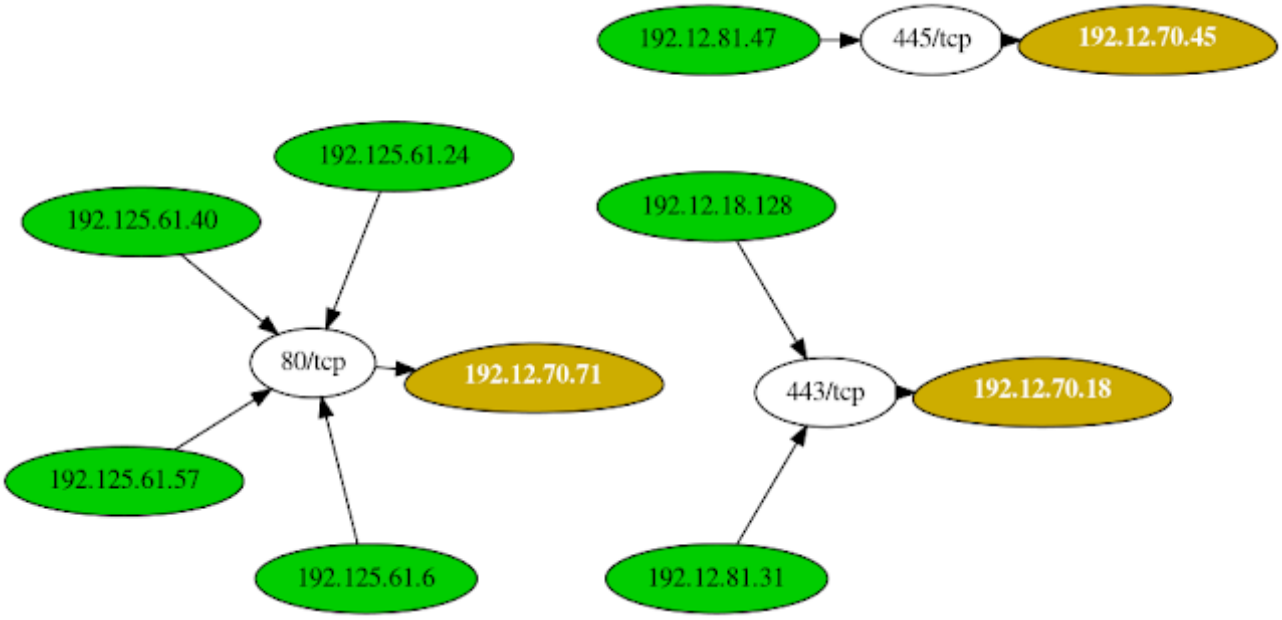
Tool help menu

If you run the script without any arguments, you'll see the following help menu:

```
r00t@r00t-KitPloit: ~
[root:vonahisec-kali:~/scripts/leprechaun]# ./leprechaun.rb

 ------------------------------------------------------------
 Leprechaun v1.0 - Alton Johnson (@altonjx)
 ------------------------------------------------------------

  Usage: ./leprechaun.rb -f /path/to/netstat_results.txt -p <port>

  -f  File containing the output of netstat results
  -p  Port you're interested in. e.g., 80. Specify "all", "common", or separate ports with co
  -e  The type of destination IP addresses you want to see connections to (e.g. external/inte

  Example: ./leprechaun.rb -f netstat_output.txt -p 80
  Example: ./leprechaun.rb -f netstat_output.txt -p all
  Example: ./leprechaun.rb -f netstat_output.txt -p common
  Example: ./leprechaun.rb -f netstat_output.txt -p 80,443 -t external
```

Example outputs

```
r00t@r00t-KitPloit: ~
+--------------+-----------------------------+-----------------------------------+
| Server       | Number of connected clients | Highest traffic destination port  |
+--------------+-----------------------------+-----------------------------------+
| 192.12.70.71 | 4                           | 80/tcp (4 clients)                |
| 192.12.70.18 | 2                           | 443/tcp (2 clients)               |
| 192.12.70.45 | 1                           | 445/tcp (1 clients)               |
+--------------+-----------------------------+-----------------------------------+
```



Additional References

Blog post: https://blog.vonahi.io/post-exploitation-with-leprechaun/

LinkedIn Article: https://www.linkedin.com/pulse/finding-gaps-your-network-segmentation-using-johnson-oscp-osce/

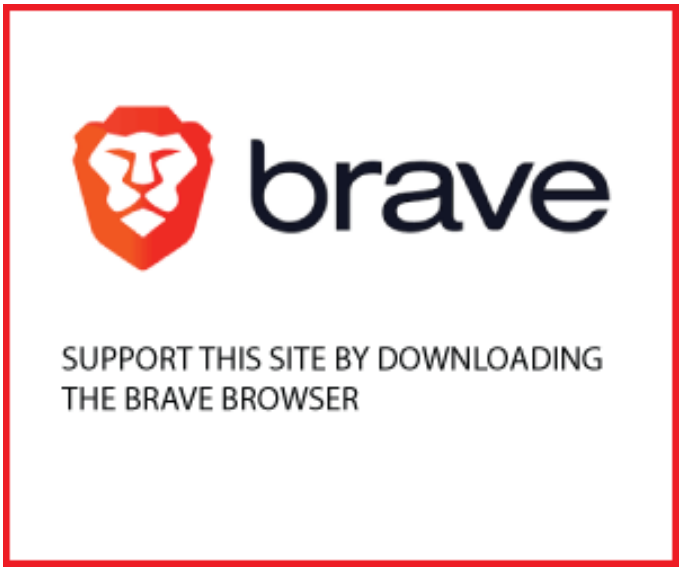
Authors

> **Alton Johnson** - *Creator* - Twitter - LinkedIn - GitHub

Acknowledgments & Credits

> Josh Stone - Influenced by Routehunter

Download Leprechaun



TAGS

LEPRECHAUN X NETSTAT X POST EXPLOITATION X PRIVILEGE ESCALATION

Facebook

A Simple API Testing Platform - Record & Replay API Tests

Ad loadmill.io

Ehtools - Framework Of Serious Wi-Fi Penetration Tools

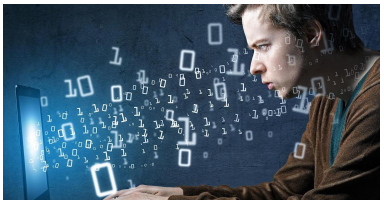
kitploit.com

Honeywell Forge Cybersecurity - The Future Is Protected

Ad honeywell.com

Trape v2.0 - Tracker On Internet: OS Analysis An

kitploit.com



GitHub security | GitHub leaks - Detect secrets leaked in code

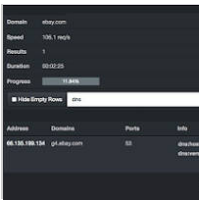
Ad gitguardian.com

NWHT - Network Wireless Hacking Tools

kitploit.com

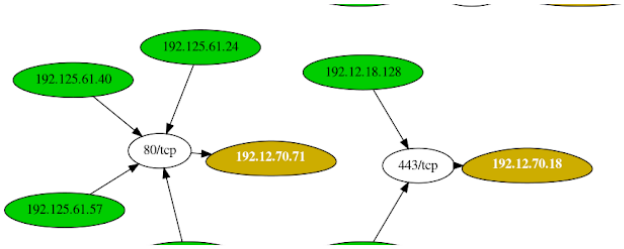
HAL - The Hardware Analyzer

kitploit.com

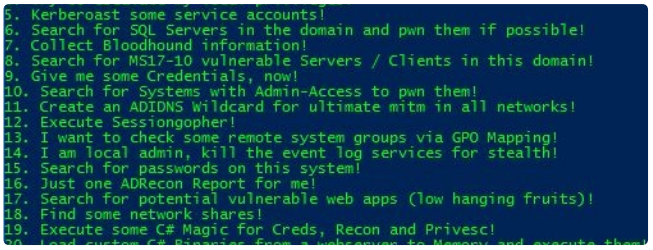


Xray - A Too Recon, Map OSINT Gath From Public

kitploit.com



Leprechaun - Tool Used To Map Out The Network Data Flow To Help Penetration Testers Identify Potentially Valuable Targets



WinPwn - Automation For Internal Windows Penetrationtest / AD-Security

GCPBucketBrute - A Script To Enumerate Google Storage Buckets, Determine What Access You Have To Them, And Determine If They Can Be Privilege Escalated

PREVIOUS

RdpThief - Extracting Clear Text Passwords From Mstsc.Exe Using API Hooking

NEXT

Glances - An Eye On Your System. A Top/Htop Alternative For GNU/Linux, BSD, Mac OS And Windows Operating Systems

POST COMMENT FACEBOOK DISQUS

0 Comments

Sort by **Oldest**

Add a comment...

Facebook Comments Plugin

FOLLOW US!

Your Email

Subscribe to our Newsletter

Zurich® Cyber Insurance Policy

Dedicated Cyber Coverages

Learn About the Zurich® Cyber Insurance Policy to Help Protect Yourself From Cyber Risks.

zurichna.com

OPEN

POPULAR

ANDRAX v4 DragonFly - Penetration Testing on Android

ANDRAX is a Penetration Testing platform developed specifically for Android smartphones, ANDRAX has the ability to run natively o...

CAPE - Malware Configuration And Payload Extraction

CAPE is a malware sandbox. It is derived from Cuckoo and is designed to automate the process of malware analysis with the goal of extrac...

Subdomain3 - A New Generation Of Tool For Discovering Subdomains

Subdomain3 is a new generation of tool , It helps penetration testers to discover more information in a shorter time than other tools.T...

Burp Suite Secret Finder - Burp Suite Extension To Discover Apikeys/Tokens From HTTP Response

Burp Suite extension to discover a apikey/tokens from HTTP response. Install download SecretFinder wget https://raw.githubusercon...

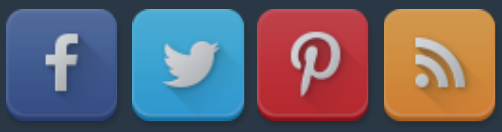
CCAT - Cloud Container Attack Tool For Testing Security Of Container Environments

Cloud Container Attack Tool (CCAT) is a tool for testing security of container environments. Quick reference Where to get help : ...

BLOG ARCHIVE

Blog Archive

SOCIAL



Your Email

Subscribe to our Newsletter

BY FEEDBURNER

RECOMMENDED

1. SSD cloud server on DigitalOcean
2. Exploit Collector
3. BlackPloit
4. Hacking Reviews

5. Hacking Land

CONTACT FORM

Name

Email *

Message *

Send

COPYRIGHT © 2019 KITPLOIT - PENTEST & HACKING TOOLS