USER

GUIDE

**DEAKIN DETONATOR TOOLKIT**

CONTENTS

**Introduction**

About the Toolkit........................................................................................................................................2

Executing the Toolkit..................................................................................................................................2

**Installation**

Old...............................................................................................................................................................3

New.............................................................................................................................................................4

**Tools**

About the Tools...........................................................................................................................................5

Nmap...........................................................................................................................................................6

SMB Enumeration........................................................................................................................................7

SNMP-Check................................................................................................................................................8

Shodan API...................................................................................................................................................9

Dirb............................................................................................................................................................10

JohnTheRipper...........................................................................................................................................11

Hashcat......................................................................................................................................................12

Hydra.........................................................................................................................................................13

Urlsnarf......................................................................................................................................................14

SearchSploit...............................................................................................................................................15

SMG-Ghost Scanner..................................................................................................................................16

ARP Spoofing.............................................................................................................................................17

Enum4linux...............................................................................................................................................18

**Attack Vectors**

About the Attack Vectors..........................................................................................................................19

CVE 2021-41773........................................................................................................................................20

ZeroLogon.................................................................................................................................................21

CVE 2021-44228........................................................................................................................................22

Find offset.................................................................................................................................................23

**Walkthroughs**

About the Walkthroughs...........................................................................................................................24

**References**

About the References................................................................................................................................25



Hardhat Enterprises

Introduction

**About the Toolkit:**

In its simplest definition, Deakin Detonator Toolkit is a penetration testing toolkit.

Made by University students, DDT is our capstone project, completed over successive trimesters.

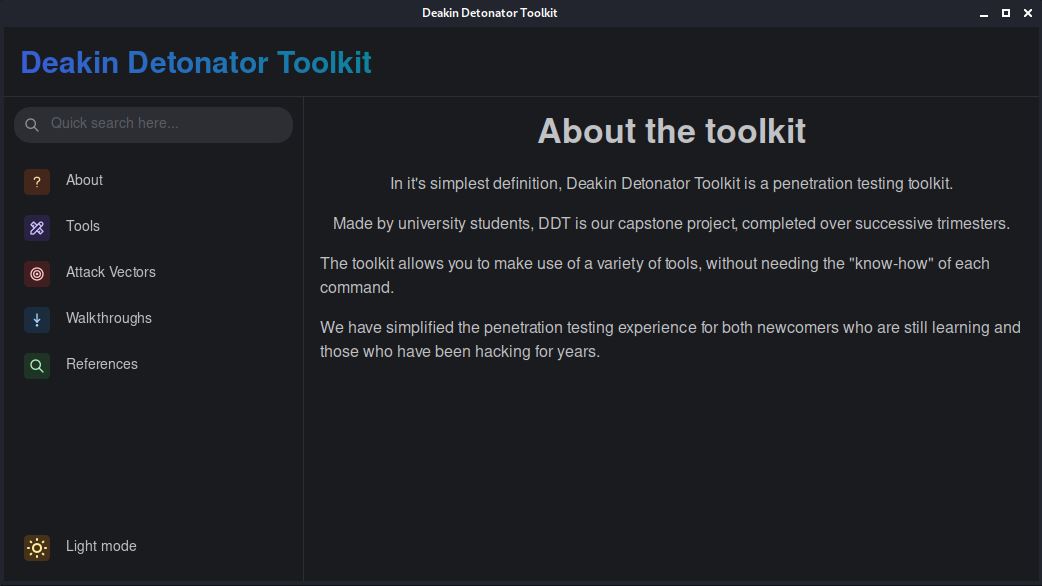
The toolkit allows you to make use of a variety of tools, without needing the “know how” of each command.

We have simplified the penetration testing experience for both newcomers who are still learning and those who have been hacking for years.

**Executing the Toolkit:**

Upon executing the toolkit, the user will be met with a Graphical User Interface (GUI) that has been built with use of Mantine, ReactJS and TypeScript, and shipped as a desktop client via Tauri.

The **About** page will be displayed on default.



The toolkit includes 5 sections **About** / **Tools** / **Attack Vectors** / **Walkthroughs / References** and features an option to switch between **Light and Dark mode**.

🔧**Setup -** The following steps are to be performed on a Kali OS:

1. Update Package list.

$ sudo apt update

2. Upgrade all packages.

$ sudo apt upgrade --fix-missing -y

3. Install Tauri pre-requisites.

$ sudo apt install libwebkit2gtk-4.0-dev \

build-essential \

curl \

wget \

libssl-dev \

libgtk-3-dev \

libayatana-appindicator3-dev \

librsvg2-dev

4. Install rust.

$ curl --proto ‘=https’ --tlsv1.2 https://sh.rustup.rs -sSf | sh

5. Install volta (to manage node installations).

$ curl https://get.volta.sh | bash

6. Close your current terminal and open a new one.

7. Install node.

$ volta install node

8. Install yarn.

$ volta install yarn

9. Clone the repo.

$ git clone https://github.com/Hardhat-Enterprises/Deakin-Detonator-Toolkit

10. Change current directory to the toolkit.

$ cd Deakin-Detonator-Toolkit

11. Install all project dependencies.

$ yarn install

Installation (Old)

12. Install the exploits to the current location.

$ ./install\_exploits.sh

13. Run the application in dev mode, this will hot-reload upon changes made to the code.

$ yarn run tauri dev

Installation (New)

🔧**Setup -** The following steps are to be performed on a Kali OS:

1. Clone the repo.

$ git clone https://github.com/Hardhat-Enterprises/Deakin-Detonator-Toolkit

2. Change current directory to the toolkit.

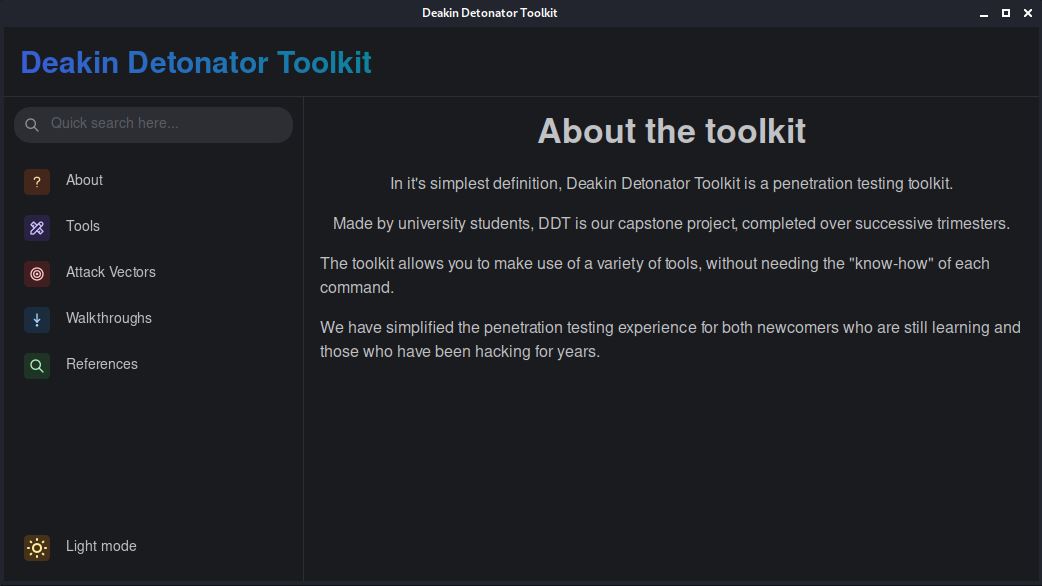
$ cd Deakin-Detonator-Toolkit

3. Run the install script.

$ ./install\_dependencies.sh

4. Run the application (dev mode).

$ yarn run tauri dev



Tools

**About the Tools:**

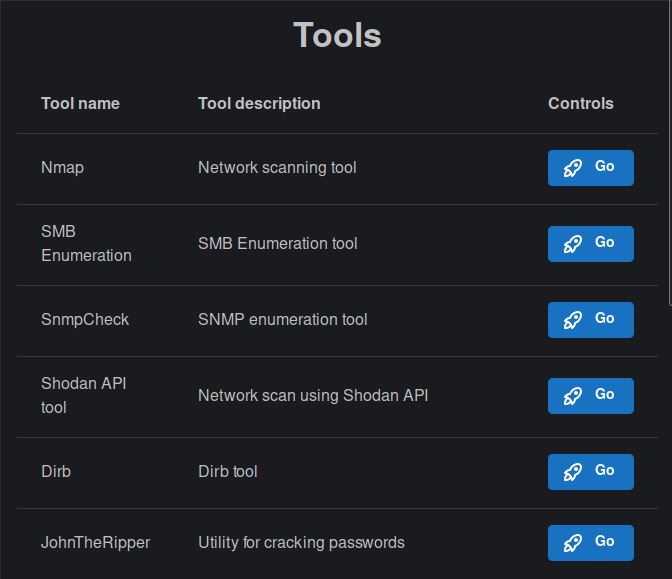
To begin, navigate to the **Tools** tab on the left-hand side of the application.

The DDT features a number of useful tools that can assist with penetration testing or system monitoring. These include:

* Nmap
* SMB Enumeration
* SNMP-Check
* Shodan API
* Dirb
* JohnTheRipper
* Hashcat
* Hydra
* Urlsnarf
* SearchSploit
* SMG-Ghost Scanner
* ARP Spoofing



To launch a tool, simply click the icon to begin execution.

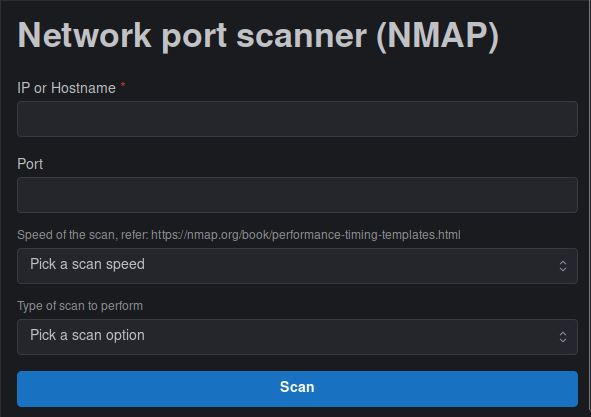


Tools

**Nmap:**

Nmap is a network scanning tool that allows a user to discover everything connected to a network and receive a wide variety of information about what is connected. The tool utilises several scanning techniques that include but are not limited to UDP, TCP connect(), TCP SYN (half-open) and FTP. Nmap offers several advanced features including an Operating System (OS) detection and Firewall status check and provides a number of scan types.

**How to use Nmap:**



**Step 1**: Enter an IP or Hostname.

Eg: 127.0.0.1

**Step 2**: Enter a Port number.

Eg: 5173

**Step 3**: Pick a scan speed - *Note; Higher speeds require a faster host network.*

T0 - Paranoid / T1 - Sneaky / T2 - Polite / T3 - Normal / T4 - Aggressive / T5 - Insane

Eg: T2

**Step 4**: Select the type of scan to perform.

Eg: Operating System

**Step 5**: Click Scan to commence the Nmap operation.

**Step 6**: View the Output block below to view the results of the Scan.

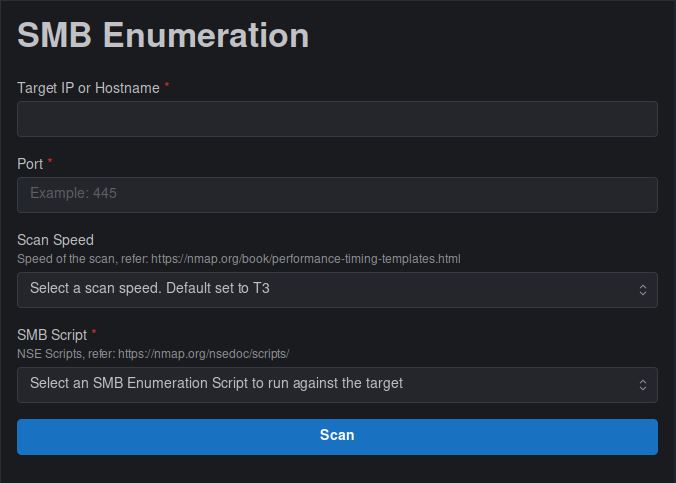


Tools

**SMB Enumeration:**

SMB (Server Message Block) represents a network protocol widely used for providing shared access across files, printers, and serial ports within a network. This tool acts to enumerate an SMB server in order for potential vulnerabilities or misconfigurations to be identified.

**How to use SMB Enumeration:**



**Step 1:** Enter an IP or Hostname.

Eg: 127.0.0.1

**Step 2:** Enter a Port number.

Eg: 445

**Step 3**: Pick a scan speed - *Note; Higher speeds require a faster host network.*

T0 - Paranoid / T1 - Sneaky / T2 - Polite / T3 - Normal / T4 - Aggressive / T5 - Insane

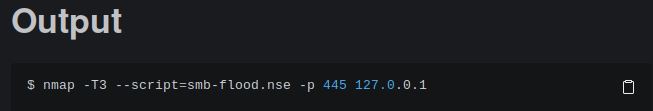
Eg: T3

**Step 4:** Select an SMB Enumeration Script to run against the target.

Eg: smb-flood.nse

**Step 5**: Click Scan to commence the SMB Enumeration operation.

**Step 6**: View the Output block below to view the results of the Scan.



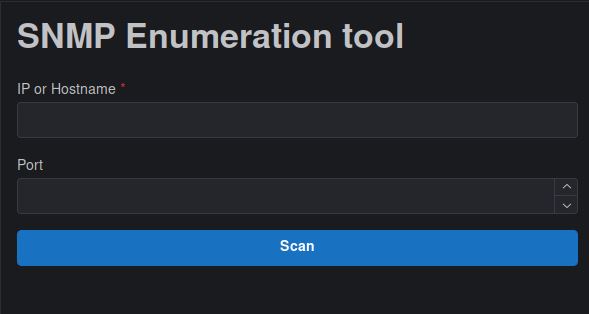
Tools

**SNMP-Check:**

SNMP check is an enumeration tool that allows the user to enumerate the SNMP devices to allow for an output that is in a much more user-friendly standard.

SNMP is an Internet Standard protocol that is used for monitoring and managing network devices that are connected over an IP.

**How to use SNMP-Check:**



**Step 1**: Enter an IP or Hostname.

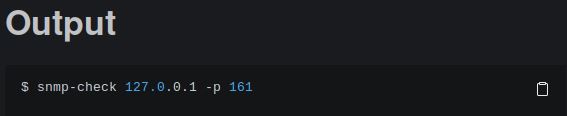
Eg: 127.0.0.1

**Step 2**: Enter a Port number - *Note; Default Port number is 161.*

Eg: 161

**Step 3**: Click Scan to commence the SNMP Enumeration operation.

**Step 4**: View the Output block below to view the results of the SNMP-Check.



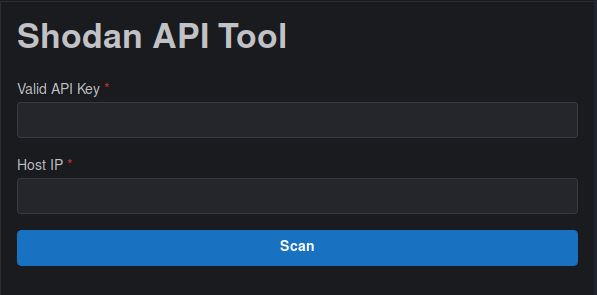
Tools

**Shodan API:**

The Shodan API is a powerful tool that allows external network scans to be performed with use of a valid API key. This key is obtained through account creation within Shodan; see the below link to create an account:

<https://developer.shodan.io/api/requirements>

**How to use Shodan API:**



**Step 1**: Enter a Valid API Key - *Note; See above for account creation to receive API Key.*

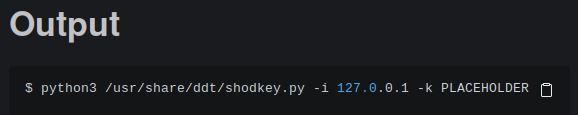
Eg: PLACEHOLDER

**Step 2**: Enter a Host IP.

Eg: 127.0.0.1

**Step 3**: Click Scan to commence Shodan API operation.

**Step 4**: View the Output block below to view the results of the tools execution.

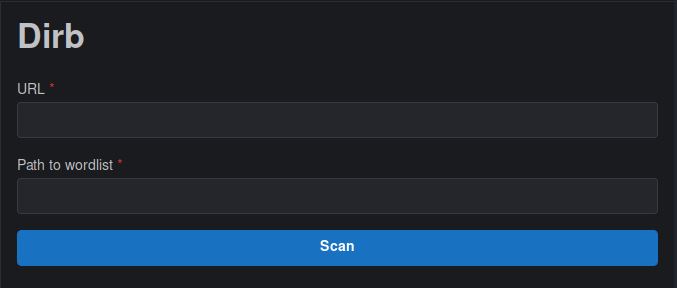


Tools

**Dirb:**

Dirb is a Web Content Scanner that acts to seek out any existing or hidden Web Objects. This is a dictionary-based attack that takes place upon a web server and will analyse the results within this process.

**How to use Dirb:**



**Step 1:** Enter a valid URL.

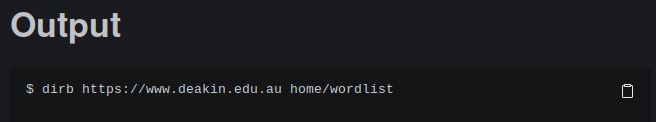
Eg: https://www.deakin.edu.au

**Step 2:** Enter a file directory pathway to access a wordlist.

Eg: home/wordlist/wordlist.txt

**Step 3:** Click Scan to commence Dirb’s operation.

**Step 4:** View the Output block below to view the results of the tools execution.

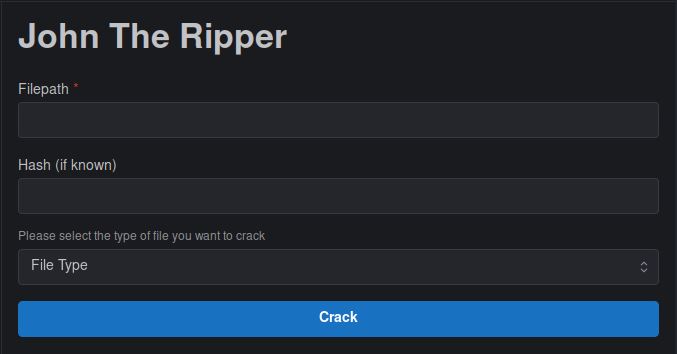


Tools

**JohnTheRipper**

JohnTheRipper is a password recovery and password security auditing tool that supports hundreds of hash and cipher types. A few examples of these include network traffic captures, encrypted private keys, filesystems, archives, document files, database servers, etc. The currently implemented version supports cracks for .zip and .rar filetypes.

**How to use JohnTheRipper:**



**Step 1:** Enter a file directory pathway to access the .zip or .rar file.

Eg: home/example/example.zip

**Step 2:** Enter a Hash if known.

Eg: PLACEHOLDER

**Step 3:** Select a file type.

Eg: zip

**Step 4:** Click Crack to commence JohnTheRipper’s operation.

**Step 5:** View the Output block below to view the results of the tools execution.

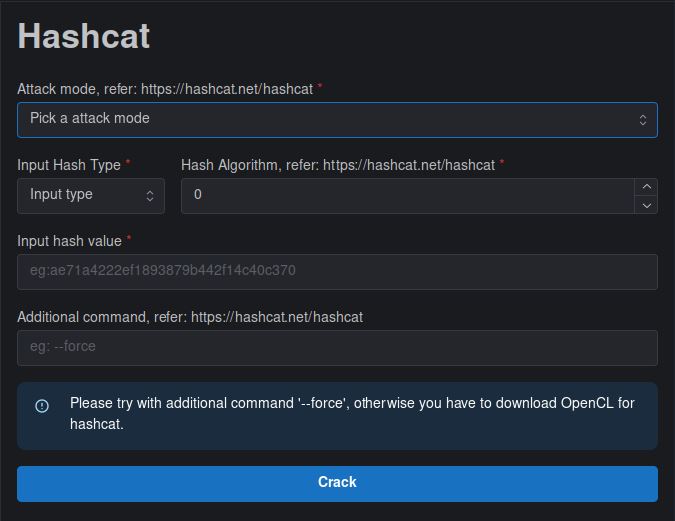
Tools

**Hashcat:**

Hashcat is an advanced password recovery tool that provides brute-force attacks that are conducted with the hash values of passwords that are either guessed or applied by the tool. The tool in the DDT currently supports 3 attack modes including Straight, Brute-force and Hybrid Wordlist + Mask. A list of the Hashing Algorithm codes can be found at:

<https://hashcat.net/hashcat/>

**How to use Hashcat:**



**Step 1:** Pick an Attack mode.

Eg: Straight

**Step 2:** Input Hash Type and Hash Algorithm code.

Eg: Hash Value, 2

**Step 3:** Input the hash value.

Eg: ae71a4222ef1893879b442f14c40c370

**Step 4:** Input password file.

Eg: /root/pwd.txt

**Step 5:** Add Additional command as found through the website.

Eg: --force

**Step 6:** Click Crack to commence Hashcat’s operation.

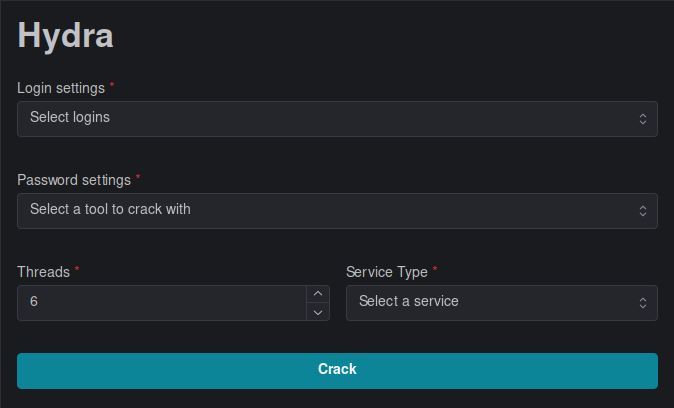
**Step 7:** View the Output block below to view the results of the tools execution.

Tools

**Hydra:**

Hydra is a login cracking tool that supports several protocols within its attacks. The tool can be applied for cracking singular passwords, files, and character sets. These brute-force attacks can be applied to SMTP, SSH, NFS, and several others.

**How to use Hydra:**



**Step 1:** Select the Login settings.

Eg: Single Login

**Step 2:** Specify the Username for the Login.

Eg: kali

**Step 3:** Select the Password settings.

Eg: Single Password

**Step 4:** Input the Password for the Login.

Eg: root

**Step 5:** Select the number of Threads and Service Type.

Eg: 6, SSH

**Step 6:** Enter an IP address and Port number.

Eg: 192.168.1.1:22

**Step 7:** Click Crack to commence Hydra’s operation.

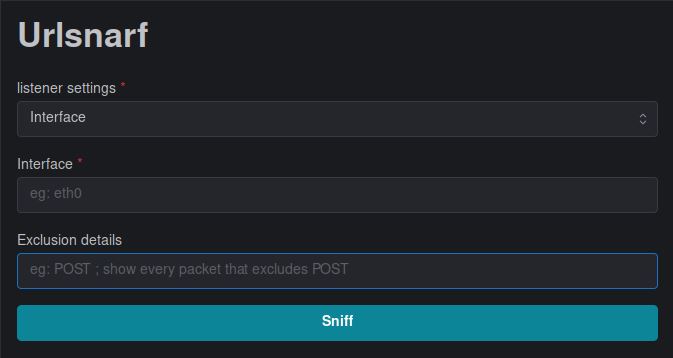
**Step 8:** View the Output block below to view the results of the tools execution.

Tools

**Urlsnarf:**

Urlsnarf is a network traffic sniffing tool that works to output all URL’s that are requested from HTTP traffic in the from of CLF (Common Log Format) that is very commonly used within web servers. The tool in the DDT provides two listener settings being through an interface or packet capture file.

**How to use Urlsnarf:**



**Step 1:** Select the Listener settings.

Eg: Interface

**Step 2:** Input the Interface.

Eg: eth0

**Step 3:** Enter any Exclusion details within the sniff:

Eg: POST *(every packet besides POST will be shown)*

**Step 4:** Click Sniff to commence Urlsnarf’s operation.

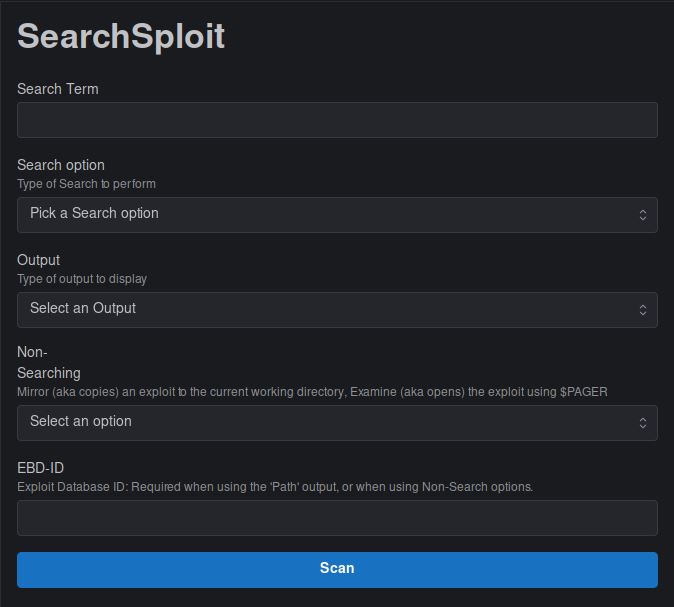
**Step 5:** View the Output block below to view the results of the tools execution.

Tools

**SearchSploit:**

SearchSploit is a command-line tool used for searching through Exploit-DB that allows an offline copy of the exploited database to be withheld. This tool is useful for conducting security assessments on segregated networks and provides several search options within its operation.

**How to use SearchSploit:**



**Step 1:** Enter a Search Term followed by selecting a Search Option.

Eg: data, Exact

**Step 2:** Select an Output type.

Eg: json

**Step 3:** Select a Non-Searching option.

Eg: Mirror

**Step 4:** Enter an Exploit Database ID.

Eg: PLACEHOLDER *(required when using the ‘Path’ output or Non-Search options)*

**Step 5:** Click Scan to commence SearchSploit’s operation.

**Step 6:** View the Output block below to view the results of the tools execution.

Tools

**SMG-Ghost Scanner:**

SMG-Ghost Scanner is a tool used to scan a target to see if they are vulnerable to the attack vector CVE2020-0796. This vulnerability fell within Microsoft’s SMB 3.1.1 protocol stack implementation where due to the failure of handling particular requests and response messages, an attacker could perform remote code execution to act as the systems user.

**How to use SMG-Ghost Scanner:**

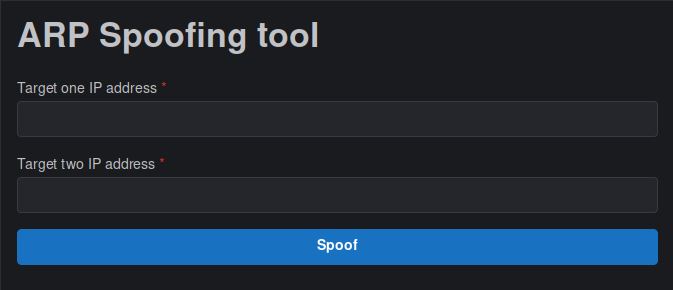
\*WORK IN PROGRESS\*

Tools

**ARP Spoofing:**

ARP Spoofing is a Man in the Middle attack where an interception can be made on the communication between devices on a network. The tool will send out forged ARP responses to the IP addresses of at least two devices, where the devices will connect to the attackers MAC address due to confusion on the router and workstation. These devices will further communicate with the attacker whilst being unknowing that an attack has even taken place.

**How to use ARP Spoofing:**



**Step 1:** Enter the IP address of the 1st target.

Eg: 192.168.1.1

**Step 2:** Enter the IP address of the 2nd target.

Eg: 127.0.0.1

**Step 3:** Click Spoof to commence ARP Spoofing’s operation.

**Step 4:** View the Output block below to view the results of the tools execution.

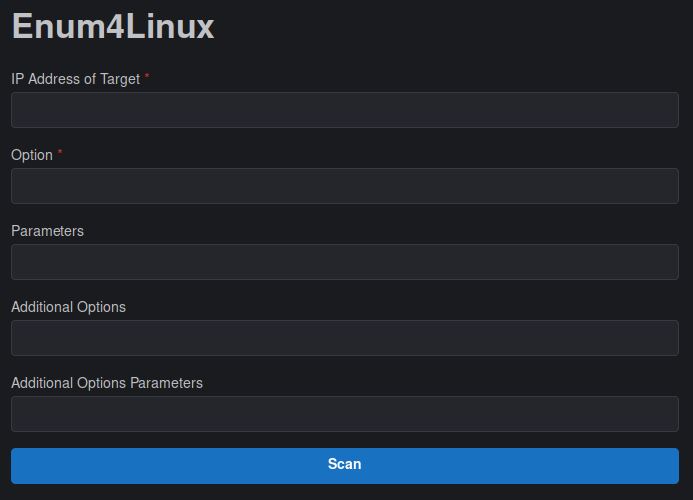
Tools

**Enum4linux:**

Enum4linux is a tool used for the enumeration of information from Windows and Samba operating systems. It is particularly useful for identifying the remote OS of a system and providing a list of the users and group memberships found within the system. Options for the tool can be found at:

<https://www.kali.org/tools/enum4linux/>

**How to use Enum4linux:**



**Step 1**: Enter a Target IP address.

Eg: 192.168.1.1

**Step 2**: Enter an Option for the Enumeration.

Eg: U (*get userlist)*

**Step 3**: Enter any Parameters.

Eg: example.txt

**Step 4**: Enter any Additional Options/Parameters.

**Step 5**: Click Scan to commence Enum4Linux’s operation.

**Step 6**: View the Output block below to view the results of the tools execution.

Attack Vectors

**About the Attack Vectors:**

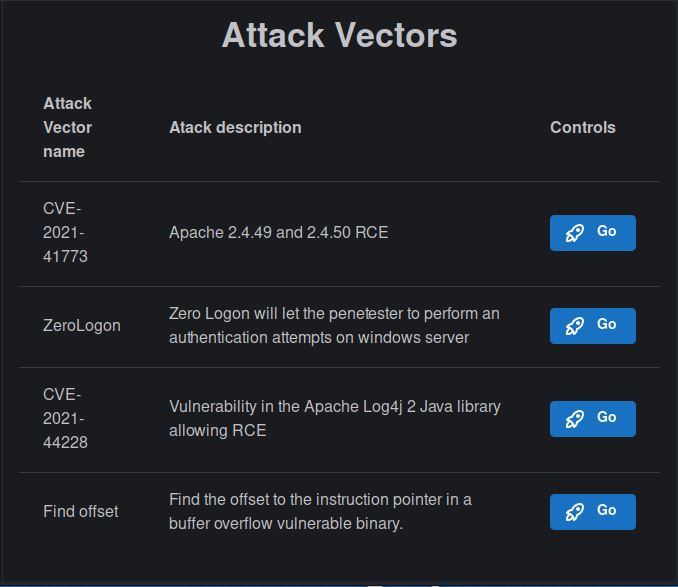
To start, navigate to the **Attack Vectors** tab on the left-hand side of the application.

The DDT features Attack Vectors that represent particular paths, methods or scenarios that are able to be exploited with intention of breaking into an IT system and further compromising the security of the system. These include:

* CVE 2021-41773 (Apache 2.4.49 and 2.4.50 RCE)
* ZeroLogon
* CVE 2021-44228 (Apache Log4j2 Java library allowing RCE)
* Find Offset



To launch an attack vector, simply click the icon to begin execution.

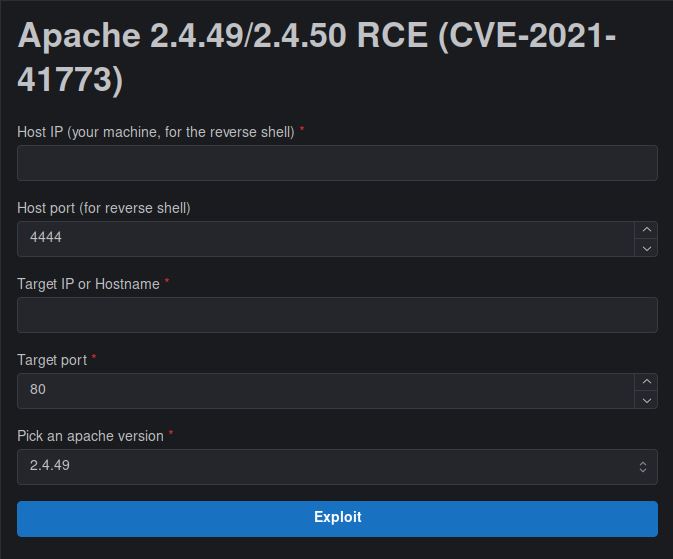
****

Attack Vectors

**CVE 2021-41773 (Apache 2.4.49 and 2.4.50 RCE):**

This attack vector targets the Apache HTTP Server (versions 2.4.49 and 2.4.50) where a path traversal attack can be used for mapping URLs to files that are located outside the directories and configured by alias-like directives. These requests will succeed if files that are located outside of the directories do not have protection by the default configurations, where this can ultimately lead to remote code execution.

**How to use CVE 2021-41773:**



**Step 1:** Enter a Host IP address.

Eg: 192.168.1.1 *(your machine for the reverse shell)*

**Step 2:** Enter a Host port.

Eg: 4444 *(for reverse shell)*

**Step 3:** Enter a Target IP address or Hostname and Target port.

Eg: 127.0.0.1, 80

**Step 4:** Choose a version of Apache to exploit.

Eg: 2.4.49

**Step 5:** Click Exploit to commence the RCE’s operation.

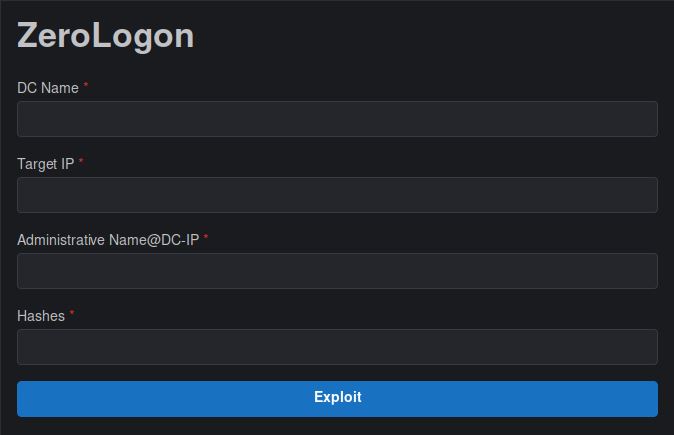
**Step 6:** View the Output block below to view the results of the attack vectors execution.

Attack Vectors

**ZeroLogon:**

The ZeroLogon CVE allows an attacker that has unauthenticated access to a domain controller within their network access to create a Netlogon session that can be exploited to grant domain administrative privileges. The vulnerability here lays within an implementation flaw for AES-CFB8 where a cryptographic transformation takes place with use of a session key.

**How to use ZeroLogon:**



**Step 1:** Enter a Doman Controller name.

Eg: PLACEHOLDER

**Step 2:** Enter a Target IP address.

Eg: 192.168.1.1

**Step 3:** Enter an Administrative name @ Domain Controller IP.

Eg: PLACEHOLDER

**Step 4:** Enter any relevant Hashes.

Eg: PLACEHOLDER

**Step 5:** Click Exploit to commence ZeroLogon’s operation.

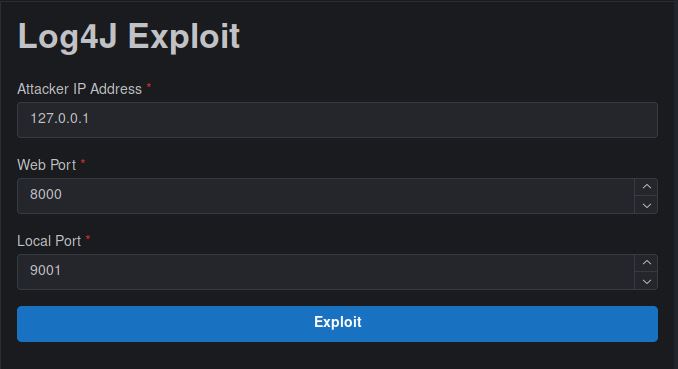
**Step 6:** View the Output block below to view the results of the attack vectors execution.

Attack Vectors

**CVE 2021-44228 (Apache Log4J2 RCE):**

This attack vector exploits vulnerabilities within Apache’s Log4j2 where an attacker that is in control of log message/log message parameters is able to execute remote arbitrary code that is to be loaded in from LDAP servers upon message lookup substitution being active.

**How to use CVE 2021-44228:**



**Step 1:** Enter an Attacker IP address.

Eg: 127.0.0.1

**Step 2:** Enter a Web Port.

Eg: 8000

**Step 3:** Enter a Local Port.

Eg: 9001

**Step 4:** Click Exploit to commence the RCE’s operation.

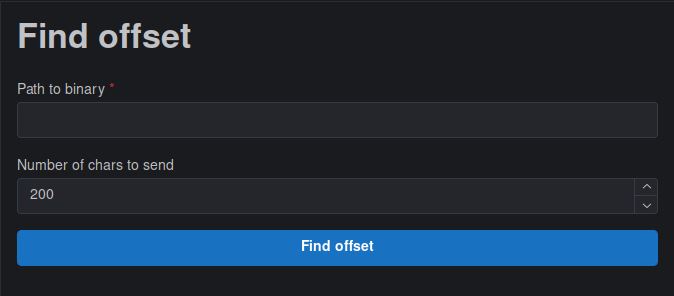
**Step 5:** View the Output block below to view the results of the attack vectors execution.

Attack Vectors

**Find offset:**

This attack vector acts to find the offset to the instruction pointer in a buffer overflow vulnerable binary.

**How to use Find offset:**



**Step 1:** Input a file directory pathway to the binary.

Eg: home/binary

**Step 2:** Enter the number of chars to send.

Eg: 200

**Step 3:** Click Find Offset to commence the tools operation.

**Step 4:** View the Output block below to view the results of the attack vectors execution.

Walkthroughs

**About the Walkthroughs:**

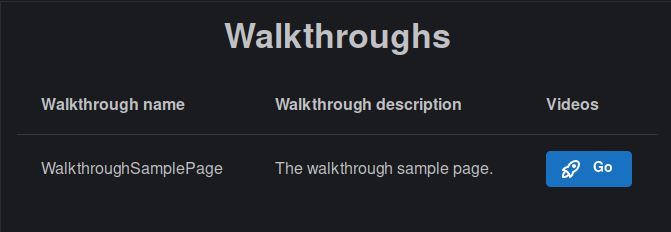
To start, navigate to the **Walkthroughs** tab on the left-hand side of the application.

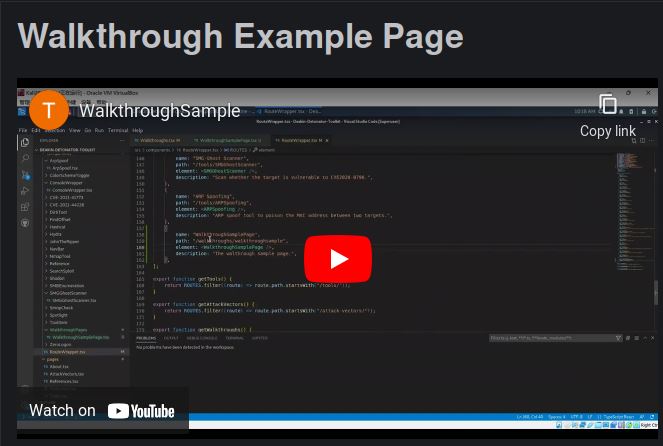
The DDT features walkthroughs that demonstrate further on how to use the application and particular tools or attack vectors. These include:

* WalkthroughSamplePage



To launch a walkthrough, simply click the icon to begin execution.





References

**About the References:**

To start, navigate to the **References** tab on the left-hand side of the application.

The DDT includes references that correlate to the useful resources used to create the GUI which each contain a description and a link. These include two main categories:

* GUI Development
* Tools



To open a reference link, simply click the icon to begin execution.

