

# **TABLE OF CONTENTS**

1   INTRODUCTION	3
2   REQUIREMENTS	3
3   INSTALLATION	3
4   CONFIGURATION	4
5   EXECUTING COMMANDS	4
6   SUPPORTED COMMANDS	5
Host Reputation	5
Parameters	5
Execution	5
Host Report	6
Parameters	6
Execution	6
Host URLs	7
Parameters	7
Execution	7



URL Reputation	8
Parameters	88
Execution	8
URL Scan	9
Parameters	9
Execution	9
URL Scan Bulk	10
Parameters	10
Execution	10
URL Scan Sync	11
Parameters	11
Execution	11
URL Scan Report	12
Parameters	12
Execution	12
Download Screenshot	13
Parameters	13
Execution	13
Download HTML	13
Parameters	13
Execution	13
Download Text	14
Parameters	12
Execution	14
API Quota	14
Parameters	14
Execution	14



# 1 | INTRODUCTION

SlashNext Phishing Incident Response commands allow users to manually perform certain data enrichment action using SlashNext On-demand Threat Intelligence cloud APIs.

The SlashNext Phishing Incident Response commands enable users to analyzes the provided IoCs (URL, IPv4 or FQDN) with the SlashNext SEER™ threat detection cloud to get definitive, binary verdicts (malicious or benign) along with forensic data including screenshots, HTML, and more.

SlashNext threat detection uses browsers in a purpose-built cloud to dynamically inspect page contents and site behavior in real-time. This method enables SlashNext to follow URL re-directs and multi-stage attacks to more thoroughly analyze the final page(s) and makes a much more accurate, binary determination with near-zero false positives. It also detects all six major categories of phishing and social engineering sites. These include credential stealing, rogue software / malware sites, scareware, phishing exploits (sites hosting weaponized documents, etc.), and social engineering scams (fake deals, giveaways, etc.).

Use cases include abuse inbox management where SOC teams can automate URL analysis for phishing emails to save hundreds of hours versus more manual methods. Playbooks that mine and analyze network logs can also leverage SlashNext URL analysis on demand. SlashNext not only provides accurate, binary verdicts (rather than threat scores), it provides IOC metadata and screen shots of detected phishing pages. These enable easier classification and reporting. Screen shots can be used as an aid in on-going employee phishing awareness training and testing.

The SlashNext Phishing Incident Response commands use an API key to authenticate with the SlashNext cloud. If you don't have a valid API key, contact the SlashNext team: support@slashnext.com

# 2 | REQUIREMENTS

#### Note

Please note that SlashNext Phishing IR commands are tested on Ubuntu 18.04 LTS in full screen terminal on display with resolution of 1080p.

SlashNext Phishing Incident Response Console requires Python 3.6 with setuptools installed on your system and have access to internet.

If you don't have Python3.6 installed please use following commands

sudo apt install python3
sudo apt install python3-pip
sudo python3 -m pip install setuptools

# 3 | INSTALLATION

Please follow the steps given below to install the SlashNext Phishing IR commands on your system.

# 



- Unzip the package provided by SlashNext.
- Open a Terminal and go to the 'src' directory.
- Run the following command which installs all the required modules along with SlashNext Phishing IR commands..

sudo python3 -m pip install.

• In order to uninstall the SlashNext Phishing IR commands package, run the following command.

sudo python3 -m pip uninstall slashnext-phishing-ir-commands

# 4 | CONFIGURATION

SlashNext Phishing IR commands does not require any specific configuration after successful installation but it is strongly recommended to create a workspace directory so that all the evidence downloaded by SlashNext Phishing IR commands is saved at a place where it can be reviewed easily later on. To do just that, Please follow the steps given below.

• Open a terminal and make a new directory which you want to save as a new workspace for SlashNext Phishing IR commands. This directory shall be used to save all the evidence of the data enrichment performed.

```
@snx:~$ mkdir snx_ir_workspace
@snx:~$ cd snx_ir_workspace/
@snx:~/snx_ir_workspace$
```

In this directory, you can use any SlashNext Phishing IR command and your evidence data will be saved in the workspace.

### **5** | EXECUTING COMMANDS

Open a terminal and input slashnext and press tab to see the list of all the available related commands as shown below.

```
@snx:~/snx_ir_workspace$ slashnext-
slashnext-api-quota slashnext-download-text slashnext-bost-urls slashnext-url-scan-bulk
slashnext-download-html slashnext-host-report slashnext-scan-report slashnext-url-scan-sync
slashnext-download-screenshot slashnext-host-reputation slashnext-url-scan

@snx:~/snx_ir_workspace$ slashnext-
```

• Complete the command you want to execute and then provide the required parameters. Please consult the **Supported Commands** section to see the list of required parameters for each command or you can use -**H** or --help with each command to see its list of accepted parameters. As an example the help for slashnext-host-reputation is shown below.

# Important Note

Please note that for each SlashNext Phishing IR command, API Key (-a, --api\_key) is required to be input by user along with the other required parameters of that specific command.

Also note that for each SlashNext Phishing IR command, Base URL (-b, --base\_url) is treated as an optional input with a default value of https://oti.slashnext.cloud/api, user only need to provide this in case of explicit instruction by SlashNext.



### Important Note

Please note that while providing the input value of parameters like **url** and **host**, enclose the value with quotes (") so that any special characters within the parameter value remain unaffected by OS.

# **6** | SUPPORTED COMMANDS

SlashNext Phishing Incident Response commands and the corresponding outputs are listed below.

- 1. slashnext-host-reputation Queries the SlashNext cloud database and retrieves the reputation of a host.
- 2. slashnext-host-report Queries the SlashNext cloud database and retrieves a detailed report.
- 3. slashnext-host-urls Queries the SlashNext cloud database and retrieves a list of all URLs.
- 4. slashnext-url-reputation Queries the SlashNext cloud database and retrieves the reputation of a URL.
- 5. slashnext-url-scan Perform a real-time URL scan with SlashNext cloud-based SEER threat detection engine.
- 6. slashnext-url-scan-bulk Perform a real-time URL scan with SlashNext cloud-based SEER threat detection engine.
- 7. slashnext-url-scan-sync Performs bulk of real-time URL scans with SlashNext cloud-based SEER Engine.
- 8. slashnext-scan-report Retrieve URL scan results against a previous scan request.
- 9. slashnext-download screenshot Downloads a screenshot of a web page against a previous URL scan request.
- 10. slashnext-ownload-html Downloads a web page HTML against a previous URL scan request.
- 11. slashnext-download-text Downloads the text of a web page against a previous URL scan request.
- 12. slashnext-api-quota Find information about your API quota, like current usage, quota left etc.

# **6.1** | HOST REPUTATION

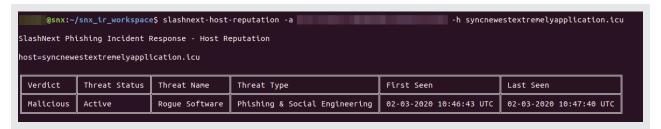
#### slashnext-host-reputation

Queries the SlashNext cloud database and retrieves the reputation of a host.

# **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	required	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address.	string	domain / IP

### Execution





# 6.2 | HOST REPORT

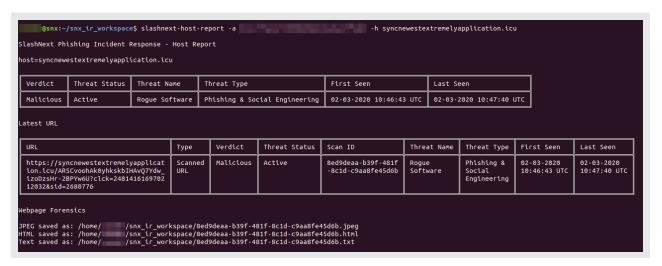
### slashnext-host-report

Queries the SlashNext cloud database and retrieves a detailed report for a host and associated URL.

#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	required	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address.	string	domain / IP

#### Execution





# 6.3 | HOST URLS

#### slashnext-host-urls

Queries the SlashNext cloud database and retrieves a list of all URLs associated with the specified host.

#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	required	The host to look up in the SlashNext Threat Intelligence database, for which to return a list of associated URLs. Can be either a domain name or an IPv4 address.	string	domain / IP
limit	required	The maximum number of URL records to fetch. Default is "10".	numeric	

# Execution





# 6.5 | URL SCAN

#### slashnext-url-scan

Performs a real-time URL scan with SlashNext cloud-based SEER™ Engine. If the specified URL already exists in the cloud database, scan results will be returned immediately. If not, this action will submit a URL scan request and return with the message "check back later" and include a unique Scan ID. You can check the results of this scan using the "slashnext-scan-report" action any time after 60 seconds using the returned Scan ID.

#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	required	The URL that needs to be scanned.	string	URL
extended_info	optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.	string	

#### Execution

The input and output of the command/action are highlighted below.

In case result is not available in the cloud database.

```
-u alrbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage/ -e true

SlashNext Phishing Incident Response - URL Scan

url=airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage/

Your Url Scan request is submitted to the cloud and may take up-to 60 seconds to complete.

Please check back later using "slashnext-scan-report" action with Scan ID = 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5 or running the same "slashnext-url-scan" action one more time
```

In case result is available in the cloud database.





# 6.4 | URL REPUTATION

# slashnext-url-reputation

Queries the SlashNext cloud database and retrieves the reputation of a URL.

### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	required	The host to look up in the SlashNext Threat Intelligence database.	string	URL

### **Execution**





# 6.6 | URL SCAN BULK

#### slashnext-url-scan-bulk

Performs bulk URL scan with the SlashNext cloud-based SEER $^{\text{TM}}$  Engine. The scan results are returned immediately if a URL already exists in the cache. For unknown URLs, a scan request will be sent, and the command will poll periodically to check the scan status and return results immediately when they become available.

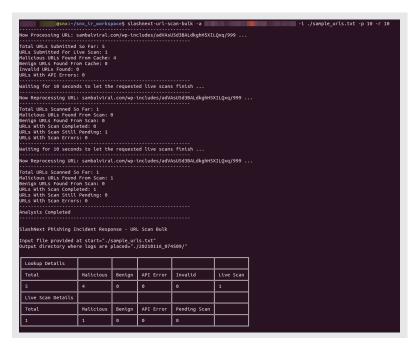
#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
input	required	Input file path containing line separated valid URLs.	string	Valid file as per OS
output	optional	Output directory path where scan logs will be stored.	string	Valid directory as per OS
poll_interval	optional	Time interval after which pending scan status is checked, value is in seconds. If no poll_interval value is specified, the default value is 60 seconds.	integer	
retries	optional	Total number of times, the scan status is checked for pending scans. If no retries value is specified, the default value is 10.	integer	

### Execution

### Important Note

Please note that during the bulk scan process, user can abort the scan process at any time by pressing CTRL+C, partial logs can still be viewed.





# 6.7 | URL SCAN SYNC

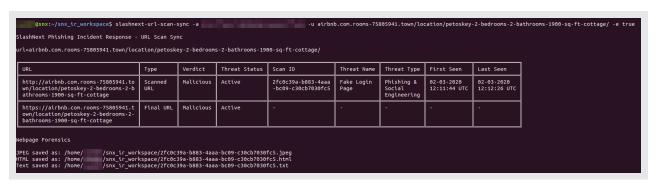
### slashnext-ur-scan-sync

Performs a real-time URL scan with SlashNext cloud-based SEER™ Engine in a blocking mode. If the specified URL already exists in the cloud database, scan result will be returned immediately. If not, this action will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish.

### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	required	The URL that needs to be scanned.	string	URL
extended_info	optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.	string	
timeout	optional	A timeout value in seconds. If the system is unable to complete a scan within the specified timeout, a timeout error will be returned. You can run the command again with a different timeout. If no timeout value is specified, a default timeout value is 60 seconds.	numeric	

# Execution





# 6.8 | URL SCAN REPORT

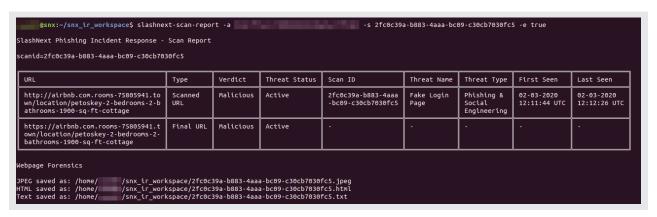
### slashnext-scan-report

Retrieves the results of a URL scan against a previous scan request. If the scan is finished, results will be returned immediately; otherwise the message "check back later" will be returned.

#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	required	Scan ID of the scan for which to get the report. Can be retrieved from the "slashnext-url-scan" action or "slashnext-url-scan-sync" action.	string	SNX scan ID
extended_info	optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.	string	

# Execution





# 6.9 | DOWNLOAD SCREENSHOT

### slashnext-download-screenshot

Downloads a screenshot of a web page against a previous URL scan request.

#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	required	Scan ID. Can be retrieved from the "slashnext-url-scan" action or the "slashnext-url-scan-sync" action.	string	SNX scan ID
resolution	optional	Resolution of the web page screenshot. Can be "high" or "medium". Default is "high".	string	

#### Execution

The input and output of the command/action are highlighted below.

```
@snx:~/snx_ir_workspace$ slashnext-download-screenshot -a -s 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5 -r medium
SlashNext Phishing Incident Response - Download Screenshot
scanid=2fc0c39a-b883-4aaa-bc09-c30cb7030fc5

JPEG saved as: /home/ /snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.jpeg
```

# 6.10 | DOWNLOAD HTML

### slashnext-download-html

Downloads a web page HTML against a previous URL scan request.

### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	required	Scan ID. Can be retrieved from the "slashnext-url-scan" action or the "slashnext-url-scan-sync" action.	string	SNX scan ID

### Execution

```
:@snx:~/snx_ir_workspace$ slashnext-download-html -a -s 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5
SlashNext Phishing Incident Response - Download HTML
scanid=2fc0c39a-b883-4aaa-bc09-c30cb7030fc5
HTML saved as: /home/ /snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.html
```



# 6.11 | DOWNLOAD TEXT

# slashnext-download-text

Downloads the text of a web page against a previous URL scan request.

#### **Parameters**

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	required	Scan ID. Can be retrieved from the "slashnext-url-scan" action or the "slashnext-url-scan-sync" action.	string	SNX scan ID

#### **Execution**

The input and output of the command/action are highlighted below.

```
@snx:~/snx_ir_workspace$ slashnext-download-text -a -s 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5

SlashNext Phishing Incident Response - Download Text

scanid=2fc0c39a-b883-4aaa-bc09-c30cb7030fc5

Text saved as: /home/ /snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.txt
```

# 6.12 | API QUOTA

#### slashnext-api-quota

Find information about your API quota, like current usage, quota left etc.

### **Parameters**

No parameters are required for this action.

### Execution

```
@snx:-/snx_ir_workspace$ slashnext-api-quota -a

SlashNext Phishing Incident Response - API Quota

Licenced Quota Remaining Quota Expiration Date

Unlimited Unlimited 2020-12-01

Note: Your annual API quota will be reset to zero, once either the limit is reached or upon quota expiration date indicated above.
```