

Phishing IR Commands v1.0.0

SlashNext Phishing IR Commands Guide

Version 1.0.0 (February 03, 2019)

This document outlines the process to install the SlashNext Phishing Incident Response (Linux-style) commands built by SlashNext. It also provides details on how to efficiently use the integrated commands to request reputation and real-time scan of specific IoCs using the underlying On-demand Threat Intelligence APIs.

- [Introduction](#)
 - [Requirements](#)
 - [Installation](#)
 - [Configuration](#)
 - [Executing Commands](#)
 - [Supported Commands](#)
 - [Host Reputation](#)
 - [Parameters](#)
 - [Execution](#)
 - [Host Report](#)
 - [Parameters](#)
 - [Execution](#)
 - [Host URLs](#)
 - [Parameters](#)
 - [Execution](#)
 - [URL Scan](#)
 - [Parameters](#)
 - [Execution](#)
 - [URL Scan Sync](#)
 - [Parameters](#)
 - [Execution](#)
 - [URL Scan Report](#)
 - [Parameters](#)
 - [Execution](#)
 - [Download Screenshot](#)
 - [Parameters](#)
 - [Execution](#)
 - [Download HTML](#)
 - [Parameters](#)
 - [Execution](#)
 - [Download Text](#)
 - [Parameters](#)
 - [Execution](#)
 - [API Quota](#)
 - [Parameters](#)
 - [Execution](#)
-

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 analyze 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

Requirements

Note

Please note that SlashNext Phishing IR commands have been 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
```

Installation

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

Note

Please note that SlashNext shall provide you with package which contains following directory structure.

```
docs
|  SlashNext Phishing IR Commands Guide.pdf
|  SlashNext Phishing IR SDK Guide.pdf
src
|  setup.py
|  README.md
|  LICENSE.txt
|  SlashNextPhishingIR
|  ...
|  ...
|  SlashNextPhishingIRCommands
|  ...
|  ...
examples
```

- 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
```

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 placed where it can be reviewed easily later on. To do just that, Please following 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.

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-host-urls      slashnext-url-scan-sy
slashnext-download-html  slashnext-host-report    slashnext-scan-report
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.

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

This action queries the SlashNext cloud database and retrieves the reputation of a host.

Usage: slashnext-host-reputation -a [api_key] -b [base_url] -h [host]
-a --api_key           Please provide a valid API Key or contact support@slashnext.com
-b --base_url          Please provide a valid Base URL or contact support@slashnext.com
-h --host              The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 add
-V --version           Version of SlashNext phishing IR commands.
-H --help              Prints this help/usage.

Developed by SlashNext, Inc. (support@slashnext.com)
```

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://o ti.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.

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-scan** - Perform a real-time URL scan with SlashNext cloud-based SEER threat detection engine.
5. **slashnext-url-scan-sync** - Perform a real-time URL scan with SlashNext cloud-based SEER threat detection engine in a blocking mode.
6. **slashnext-scan-report** - Retrieve URL scan results against a previous scan request.
7. **slashnext-download screenshot** - Downloads a screenshot of a web page against a previous URL scan request.
8. **slashnext-ownload-html** - Downloads a web page HTML against a previous URL scan request.
9. **slashnext-download-text** - Downloads the text of a web page against a previous URL scan request.
10. **slashnext-api-quota** - Find information about your API quota, like current usage, quota left etc.

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

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

```
@snx:~/snx_ir_workspace$ slashnext-host-reputation -a [REDACTED] -h syncnewestextremelyapplication.icu
```

SlashNext Phishing Incident Response - Host Reputation

host=syncnewestextremelyapplication.icu

Verdict	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
Malicious	Active	Rogue Software	Phishing & Social Engineering	02-03-2020 10:46:43 UTC	02-03-2020 10:47:40 UTC

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

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

```
@snx:~/snx_ir_workspace$ slashnext-host-report -a [REDACTED] -h syncnewestextremelyapplication.icu
```

SlashNext Phishing Incident Response - Host Report

host=syncnewestextremelyapplication.icu

Verdict	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
Malicious	Active	Rogue Software	Phishing & Social Engineering	02-03-2020 10:46:43 UTC	02-03-2020 10:47:40 UTC

Latest URL

URL	Type	Verdict	Threat Status	Scan ID	Threat Name	Threat Type	First Seen	Last Seen
https://syncnewestextremelyapplication.icu/ARSCvoohAk0yhkskBIHavQ7Ydw_izoDzSHr-2BPYw6U?clck=248141616970212032&sid=2680776	Scanned URL	Malicious	Active	8ed9deaa-b39f-481f-8c1d-c9aa8fe45d6b	Rogue Software	Phishing & Social Engineering	02-03-2020 10:46:43 UTC	02-03-2020 10:47:40 UTC

Webpage Forensics

JPEG saved as: /home/[REDACTED]/snx_ir_workspace/8ed9deaa-b39f-481f-8c1d-c9aa8fe45d6b.jpeg
HTML saved as: /home/[REDACTED]/snx_ir_workspace/8ed9deaa-b39f-481f-8c1d-c9aa8fe45d6b.html
Text saved as: /home/[REDACTED]/snx_ir_workspace/8ed9deaa-b39f-481f-8c1d-c9aa8fe45d6b.txt

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	optional	The maximum number of URL records to fetch. Default is "10".	numeric	

Execution

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

```
@snx:~/snx_ir_workspace$ slashnext-host-urls -a [redacted] -h mostashari.com -l 3
```

SlashNext Phishing Incident Response - Host URLs

host=mostashari.com

URL	Type	Verdict	Threat Status	Scan ID	Threat Name	Threat Type	First Seen	Last Seen
https://mostashari.com/chat/secure.bankofamerica.comlogin-sign-onV2Screen.go2018/	Scanned URL	Malicious	Active	N/A	Fake Login Page	Phishing & Social Engineering	02-03-2020 11:36:45 UTC	02-03-2020 11:38:04 UTC
https://mostashari.com/chat/secure.bankofamerica.comlogin-sign-onV2Screen.go2018/successfull.php	Scanned URL	Malicious	Active	N/A	Fake Login Page	Phishing & Social Engineering	02-03-2020 11:36:45 UTC	02-03-2020 11:38:02 UTC
https://mostashari.com/chat/secure.bankofamerica.comlogin-sign-onV2Screen.go2018/sign-onV2Screen.php	Scanned URL	Malicious	Active	N/A	Fake Login Page	Phishing & Social Engineering	02-03-2020 11:36:45 UTC	02-03-2020 11:38:04 UTC

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.

```
@snx:~/snx_ir_workspace$ slashnext-url-scan -a [redacted] -u a1rbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage/ -e true
```

SlashNext Phishing Incident Response - URL Scan

url=a1rbnb.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.

```
@snx:~/snx_ir_workspace$ slashnext-url-scan -a [redacted] -u airbnb.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/



| URL                                                                                                | Type        | Verdict   | Threat Status | Scan ID                              | Threat Name     | Threat Type                   | First Seen              | Last Seen               |
|----------------------------------------------------------------------------------------------------|-------------|-----------|---------------|--------------------------------------|-----------------|-------------------------------|-------------------------|-------------------------|
| http://airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage  | Scanned URL | Malicious | Active        | 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5 | Fake Login Page | Phishing & Social Engineering | 02-03-2020 12:11:44 UTC | 02-03-2020 12:12:26 UTC |
| https://airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage | Final URL   | Malicious | Active        | -                                    | -               | -                             | -                       | -                       |



Webpage Forensics

JPEG saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.jpeg
HTML saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.html
Text saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.txt
```

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

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

```
@snx:~/snx_ir_workspace$ slashnext-url-scan-sync -a [redacted] -u airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage/ -e true

SlashNext Phishing Incident Response - URL Scan Sync

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



| URL                                                                                                | Type        | Verdict   | Threat Status | Scan ID                              | Threat Name     | Threat Type                   | First Seen              | Last Seen               |
|----------------------------------------------------------------------------------------------------|-------------|-----------|---------------|--------------------------------------|-----------------|-------------------------------|-------------------------|-------------------------|
| http://airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage  | Scanned URL | Malicious | Active        | 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5 | Fake Login Page | Phishing & Social Engineering | 02-03-2020 12:11:44 UTC | 02-03-2020 12:12:26 UTC |
| https://airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage | Final URL   | Malicious | Active        | -                                    | -               | -                             | -                       | -                       |



Webpage Forensics

JPEG saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.jpeg
HTML saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.html
Text saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.txt
```

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

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

```
@snx:~/snx_ir_workspace$ slashnext-scan-report -a [redacted] -s 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5 -e true
SlashNext Phishing Incident Response - Scan Report
scanid=2fc0c39a-b883-4aaa-bc09-c30cb7030fc5
```

URL	Type	Verdict	Threat Status	Scan ID	Threat Name	Threat Type	First Seen	Last Seen
http://airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage	Scanned URL	Malicious	Active	2fc0c39a-b883-4aaa-bc09-c30cb7030fc5	Fake Login Page	Phishing & Social Engineering	02-03-2020 12:11:44 UTC	02-03-2020 12:12:26 UTC
https://airbnb.com.rooms-75805941.town/location/petoskey-2-bedrooms-2-bathrooms-1900-sq-ft-cottage	Final URL	Malicious	Active	-	-	-	-	-

```

Webpage Forensics
JPEG saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.jpeg
HTML saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.html
Text saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.txt

```

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 [redacted] -s 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5 -r medium
SlashNext Phishing Incident Response - Download Screenshot
scanid=2fc0c39a-b883-4aaa-bc09-c30cb7030fc5
JPEG saved as: /home/[redacted]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.jpeg
```

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

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

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

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 [REDACTED] -s 2fc0c39a-b883-4aaa-bc09-c30cb7030fc5
SlashNext Phishing Incident Response - Download Text
scanid=2fc0c39a-b883-4aaa-bc09-c30cb7030fc5
Text saved as: /home/[REDACTED]/snx_ir_workspace/2fc0c39a-b883-4aaa-bc09-c30cb7030fc5.txt
```

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

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

```
@snx:~/snx_ir_workspace$ slashnext-api-quota -a [REDACTED]
SlashNext Phishing Incident Response - API Quota
```

Licensed 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.