Ridge Security RidgeBot™

User Manual

Version 4.2.4

Contact Information:

Ridge Security Technology Inc.
1601 McCarthy Blvd.
Milpitas, CA 95035
United States

www.ridgesecurity.ai

Table of Contents

Chapter 1 Introducing RidgeBot

What is RidgeBot?

RidgeBot is an intelligent security validation Robot. RidgeBot is modeled with a collective knowledge of threats, vulnerabilities, and exploits, and equipped with state-of-the-art hacking techniques. RidgeBot acts like a real attacker, relentlessly locates, exploits, and documents its findings. RidgeBot automates penetration testing and attack simulation, making it affordable to run at scale. The solution works within a defined scope and instantly replicates to address highly complex structures.

RidgeBot provides continuous security validation services. It assists security testers in overcoming knowledge, experience and time limitations and always performs at a superior level. The shift from manual-based, labor-intensive testing to machine-assisted automation alleviates the current severe shortage in security professionals. It allows human security experts to forgo daily labor-intensive work and devote more effort to the research of new threats and new technologies.

What is new in Each RidgeBot Version

New Features in Version 4.2.3

- This release is a bug fix release, no new features.

New Features in Version 4.2.2

- Support a system-level proxy for RidgeBot communication with License Server/Jira Cloud/GitLab
- Support Nexpose's "Asset Vulnerability List Export" report
- User can configure the retention period for RidgeBot logs
- PT Task using the new "Host Penetration" scenario will not launch web crawler during attack surface discovery and penetration testing.
- Restart RidgeBot services(NGINX and API) automatically when detecting RidgeBot's IP address is changed
- "check-license" Output/Error Message Enrichment

- Remove License Type Restriction When Installing a New License
- Support long API authentication token for Jira Cloud integration
- New Plugins
- Bugfixes

New Features in Version 4.2.1

- "show system" command to show RidgeBot software version in the management console
- Disk Cleanup – to clear disk space
- Supports additional DevOps platforms for Issue Tracking
- Differential reports for periodic tasks
- Optimized priority of Jira cases created by RidgeBot
- New warning message and additional error codes
- New Plugins
- Bugfixes

New Features in Version 4.2

- Online Updates for Software and Plugin library
- Support Microsoft Authenticator for 2FA
- Option to set the hostname of the RidgeBot server in the management console
- Increase the Maximum number of targets per task from one Class C subnet to Four Class C subnets (1024 targets)
- Bugfixes

New Features in Version 4.1.1

- Jira integration – On prem only
- New license types for MSSP – MSV and ProX (with 2nd test window)
- License server port change to 443 – applies to RidgeBot version 4.1.1 or later
- Scenario: Intranet Ransomware Attack Simulation and Intranet Penetration Scenario
- Include new plugins in the new version of the Plugin library, V4.10.6
- Bug fixes

New Features in Version 4.1.0

- Web automation login sequence recorder
- RidgeBot Login with Two Factor Authentication
- Add language field in the Report management list
- Include new plugins in the new version of the Plugin library, V4.6.4
- Bug fixes

New Features in Version 4.0.2

- Import targets from Asset Table
- Include a new version of the Plugin library, 3.42.7
- Bug fixes

New Features in Version 4.0.1

- Attack Surface Identification Scenario only requires a valid license to start – does not deduct IP host license
- Report Localization for Italian
- New debug features in the RidgeBot management console – check-license and backup log
- Include a new version of the Plugin library, 3.42.3
- Bug fixes

New Features in Version 4.0:

- New Adversary Cybersecurity Emulation (ACE) Scenarios – 3 new ACE scenarios
- A new Penetration Test scenario for 3rd Party Scanning Result Validation
- Additional task list UI actions to "clone" a task or create a "draft" task
- New task scheduler support for scheduled tasks and periodic tasks
- New historical reports for periodic Penetration Test tasks
- Automatic attack confirmation after 24 hours for high-impact plugins
- More syslog messages for Penetration Test vulnerability/risk findings and new ACE tasks
- Asset Management enhancements

New Features in Version 3.9:

- RidgeBot User Interface Enhancement
- Enhancements task workflow, policy and configuration

- Simplified Licensing based on scenario selection
- Report Preview
- Include new plugin library 3.22
- API Enhancements
- Bug fixes

New Features in Version 3.8:

- OWASP Top 10:2021 Report available for Web Penetration scenario
- Rename Asset Profiling scenario to Attack Surface Identification scenario including new "Attack Surface Report" template
- Add Google Cloud Platform support in the cloud deployment (Beta)
- Include new plugin library 2.12
- Bug fixes

New Features in Version 3.7:

- A new feature adding Stealth Level in Task configuration to support flow control
- Bug fixes

New Features in Version 3.6:

- OWASP Top 10:2017 Report available for Web Penetration scenario
- Scan Type default for Web Penetration and Internal Host scenarios
- Task Configuration: Scan Network Port Range now uses "All Ports" as default
- GUI Simplification to set the "# of Bots" configuration
- New Plugins and Bug fixes

New Features in Version 3.5:

- Report Localization for Korean and Spanish
- Report Co-Branding
- Management API
- New Plugins and Bug fixes

New Features in Version 3.4:

- Post Exploitation and Lateral Movement
- New Crawler Engine Selection in Crawler configuration (Intelligent, Static, or Dynamic)
- Report Management including password encryption
- Route Priority
- New Plugins and Bug fixes

New Features in Version 3.3:

- High-performance web crawler and enhanced webpage logins
- CEF format syslog messages to support for SIEM or SOC integration
- Support Brute-force attack for VNC Remote Desktop application
- New Plugins and Bug fixes

New Features in Version 3.2:

- Ransomware Attack Simulation Scenario
- Attack Topology – Auto Drawing
- Enhance Report to include Kill Chain
- Support Reports in CSV format and Customized Content

RidgeBot Features

Every RidgeBot task automates the entire attack process. When it connects to an organization's IT environment, RidgeBot automatically discovers all the different types of assets on the network and then uses the collective knowledge database of vulnerabilities to mine the target system. Once RidgeBot discovers vulnerabilities, it uses built-in hacking techniques and exploit libraries to launch a real attack against the vulnerability. If successful, the vulnerability is validated and RidgeBot documents the entire kill chain transaction.

RidgeBot provides rich analytics for risk assessment and prioritization, generating a comprehensive report that includes remediation advice. RidgeBot has a powerful "brain" that contains artificial intelligence algorithms and an expert knowledge base that guides RidgeBot in attack pathfinding/selection, launching iterative attacks based on learning along the path to achieve much wider test coverage and deeper inspection. Due to its friendly usability and unlimited scalability, RidgeBot is adopted by both large organizations as well as smaller web application development teams.

- **Asset auto-discovery**: RidgeBot can automatically identify broad types of assets, including networks, hosts, applications, plug-ins, images, IoT devices, and mobile devices.
- **Vulnerability mining**: RidgeBot leverages Ridge Security's Threat Intelligence platform that includes 2-billion security intelligence data points, 100 million attack libraries, and 150K exploit libraries.
- **Vulnerability exploits**: RidgeBot supports various attack modes that meet customers' varying needs, automatically verifies the efficacy of the vulnerability findings, and ensures that test output is accurate, reliable, and usable.
- **Risk prioritization**: RidgeBot visualizes the kill chain and quantifies risks based on multiple factors, giving organizations a clear idea of what to focus on first.

This document provides the details to navigate and configure RidgeBot operations. For information and instructions on installing RidgeBot Software onto an appliance, VM or Cloud platform, please refer to the RidgeBot Deployment QuickStart Guide available from Software Downloads.

Chapter 2 Getting Started

This chapter explains how to get started with the RidgeBot solution.

The chapter has the following sections:

Deploying RidgeBot

Installation

RidgeBot is delivered as a software package for new installation or software upgrade. It can be installed in a bare metal server as an appliance, in a virtual machine or on a cloud platform. These installation options must meet the RidgeBot minimum hardware and support requirements provided in the RidgeBot Deployment QuickStart Guide.

RidgeBot Installation Package

The installation software is available in the following packages:

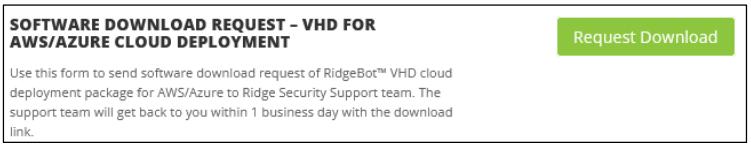
- RidgeBot ISO installation for Appliance and VM
- RidgeBot VHD file for AWS, and Google Cloud Platform
- There are RidgeBot public offers in both AWS Marketplace and Azure Marketplace.

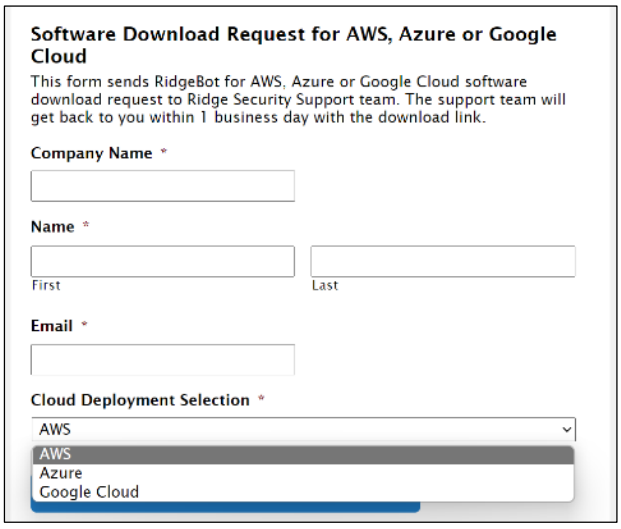
Link to Request RidgeBot Installation and Upgrade Packages

- https://partners.ridgesecurity.ai/partner-home/software-downloads/

- Choose **ISO Installation** to request the RidgeBot ISO installation package, software upgrade package and Plugin Library upgrade package

-
- Choose **VHD** for AWS, Azure or Google Cloud Platform Cloud Deployment. For a Google Cloud user, the requester will receive a separate email with the VHD file access credentials that is only valid for 3 days. *****

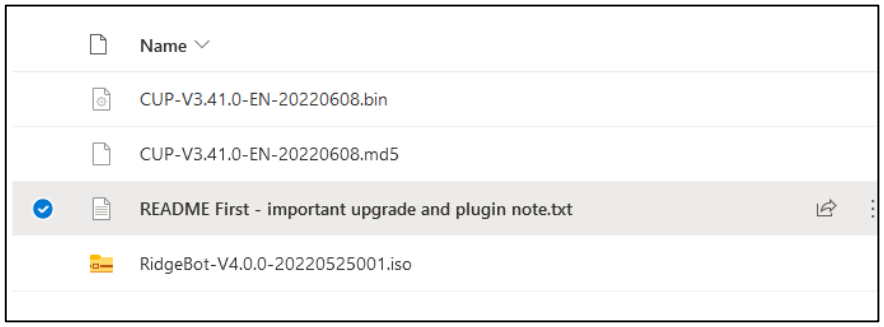




***Note**: Google Cloud is available for early access to test only.

Software Installation

- The software installation instruction is included in the **RidgeBot Deployment Quickstart Guide**.
- The instruction to install the **Software upgrade package** or the **Plugin library upgrade** package is included in the "**README First**" file. This "**README First**" file will include special procedure for each version of the upgrade package. This file is available in the same directory as the upgrade package.



- Software version 4.2 or later will require a new license file. The 4.1.1 or earlier version of the license file will be removed from the RidgeBot after it is upgraded to software version 4.2.

Deployment Mode

RidgeBot offers three types of deployment modes to fit various network topologies and network managing regulations.

- **On-Premises Mode**: Due to security compliance or regulations, remote access via a cloud platform or VPN tunnel is not allowed, or specific business-critical systems are restricted from being accessed from an external network. For this scenario, RidgeBot provides an On-Premises deployment option. The RidgeBot system can be installed on a specialized hardware appliance or as a software image to run on virtual machines in On-Premises servers.

The RidgeBot hardware appliance or software image is preloaded with the RidgeThreat Intelligence database and RidgeBrain algorithms. With a purchased license, the hardware appliance or virtual image is activated. The RidgeBot system is deployed in the location specified with an approved configuration. It connects to the IT network with the appropriate authorization. One or multiple hardware appliances

or virtual machines form the RidgeBot platform, which accomplishes various security validation tasks based on your needs.

- **VPN Mode**: RidgeBot can be deployed off-premises and uses a Virtual Private Network (VPN) capability to initiate security validation service on your networks and systems. The RidgeBot SaaS cloud platform also supports the combined use of the SaaS and VPN Modes when the service is available

For detailed information on VPN configuration, see the VPN section in Chapter 9 System Settings.

Web Browser Recommendation and Update

RidgeBot recommends using Chrome 61 or Firefox 48 and newer versions. On the web browser, type in the URL https://RidgeBot_IPaddress. If your browser version does not meet the minimum system requirement, the system prompts you to upgrade your browser as shown below. You can upgrade it either from the browser's official website or download the upgrade package provided by the system.

License Authentication

A license is required to activate and use RidgeBot. RidgeBot requires connectivity to the license server. In an Appliance deployment using an "offline" license, this license is pre-activated. After the license installation, the appliance can be operated offline. For a VM or Cloud deployment, RidgeBot will only has the online license, and it needs to communicate with the License server regularly. For initial access, follow these steps to install the license.

1. Use the recommended web browser to access the RidgeBot system. The RidgeBot URL is the IP Address of the RidgeBot interface.

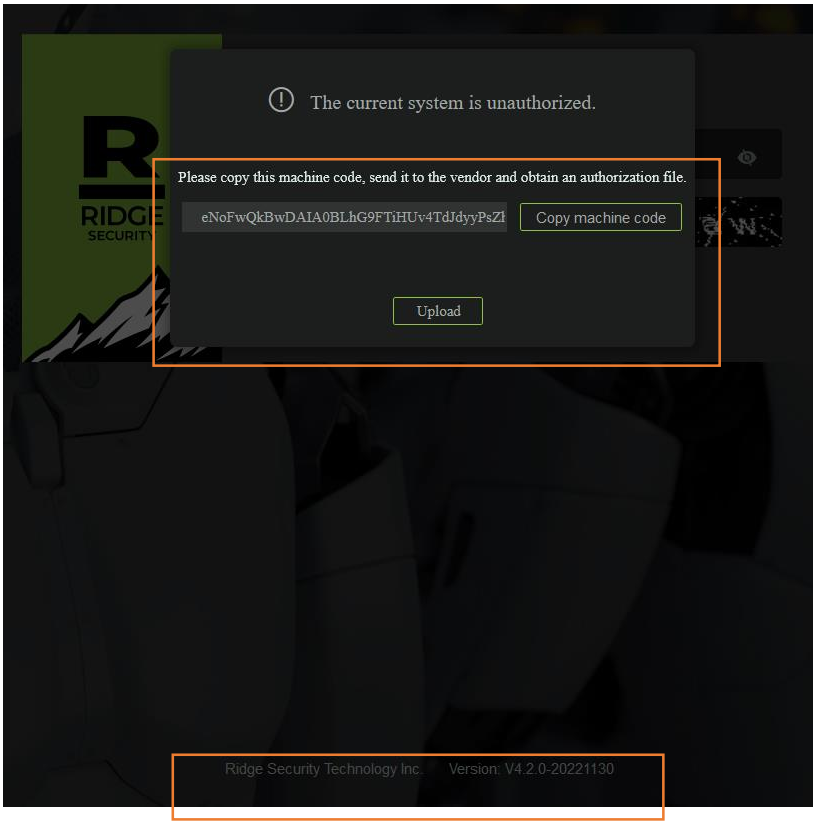


Figure 1: Authentication Page

2. Copy and submit the generated machine code from the dialog box into the Ridge Security Online License request to get an authorization license file.
3. Upload the authorization license file. Once the license file is uploaded successfully, the browser will return to the log in page. Otherwise, RidgeBot will return to the authentication page.

> **Note**: If RidgeBot is installed in a virtual machine and a user runs another copy of the same virtual machine (same machine code and license file), the License server deactivates the license. If a user needs to move the license, see the License Migration section for details.

Accessing RidgeBot

Starting in RidgeBot version 4.2.0, a valid license is required to access the RidgeBot GUI. When using an online license, RidgeBot will need to validate the license with the license server before user can access the GUI.

On the login page, type in the username, password and the verification code to access the RidgeBot system.

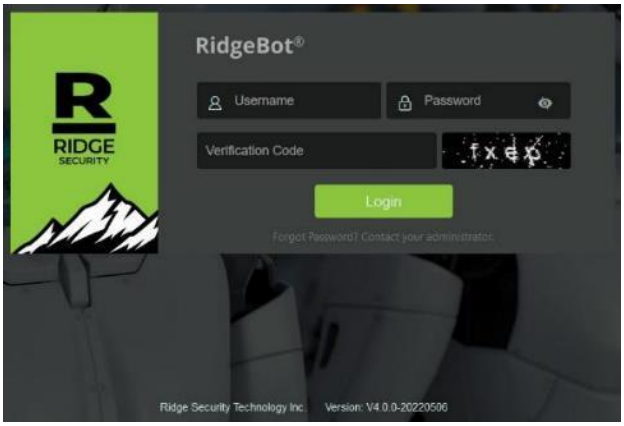


Figure 2: RidgeBot Login Page

The default username and password are admin/admin. Upon initial login, RidgeBot enforces a password change with a pop-up dialog box.

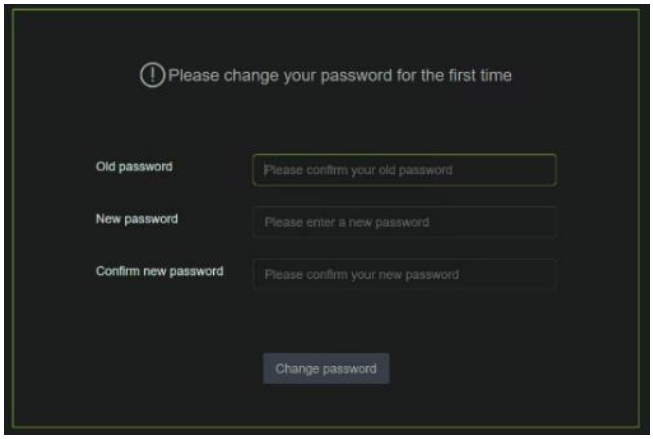


Figure 3: Password Change Page

Change the password from the GUI

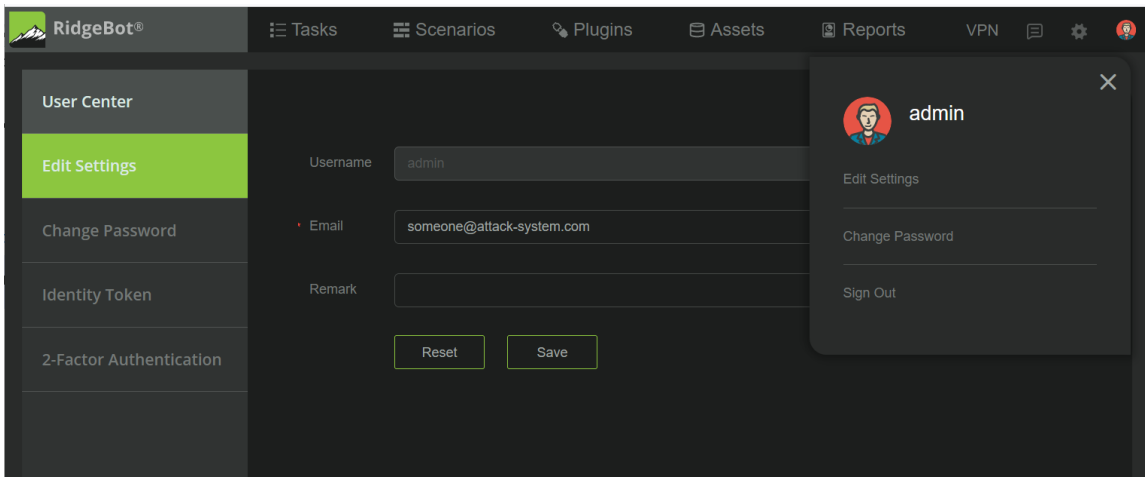
1. In the upper right corner, mouse over the "login user icon", and then click "Change Password" on the pop-up menu.
2. Complete the options on the page.
3. Click **Save**.

The default system timeout is 30 minutes. You will be logged out automatically when it times out. You can change the timeout value and the password policy on the Security configuration page. For detailed information about changing these parameters, see the section in Chapter 9 Security Settings.

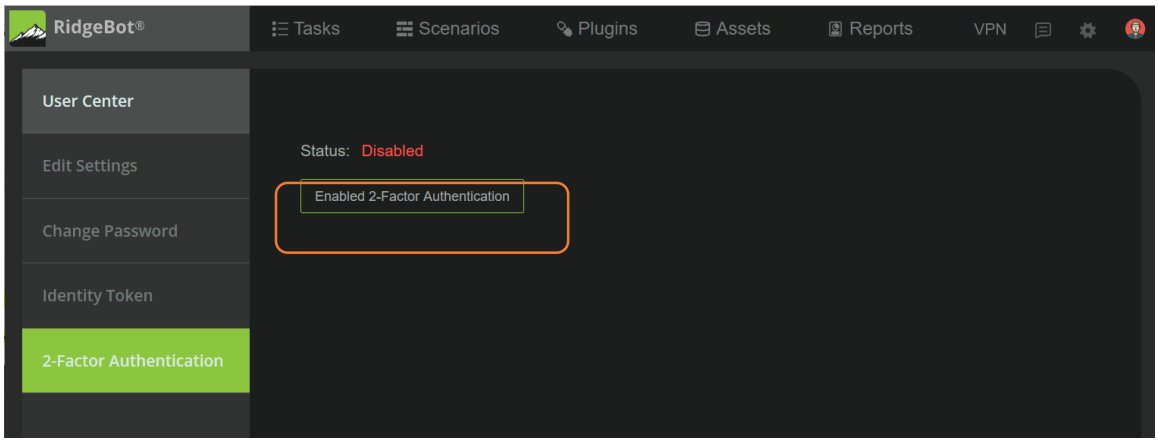
Note: The RidgeBot management IP should be the first default route in the network routing table.

Setup Two-Factors Authentication in RidgeBot Login

1. In the upper right corner, mouse over the "login user icon", and then click on "Edit Settings" on the pop-up menu.
2. In the User Center (left frame), click on the 2-Factor Authentication selection

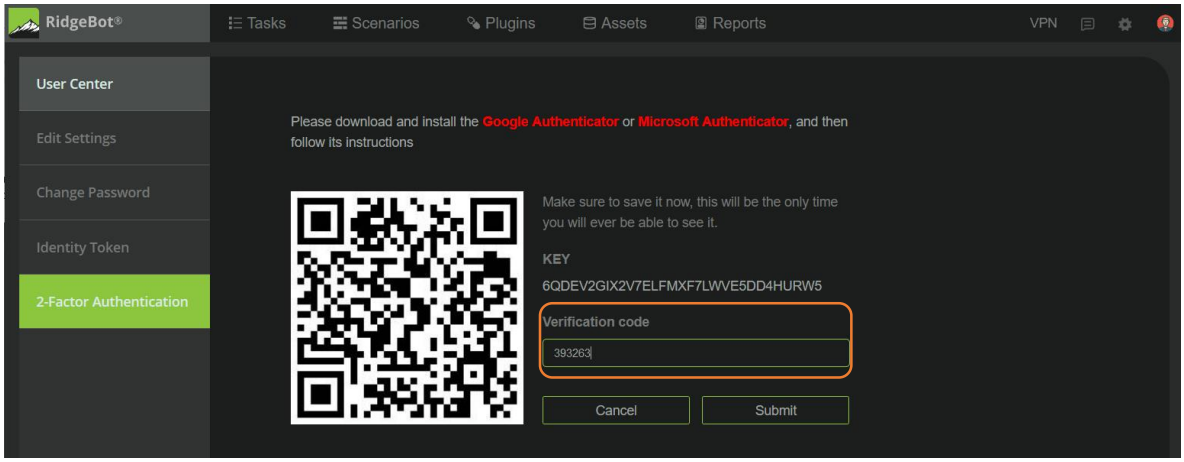


3. 2-Factor Authentication is Disable by default, click on the "Enable 2-Factor Authentication" box to enable the feature

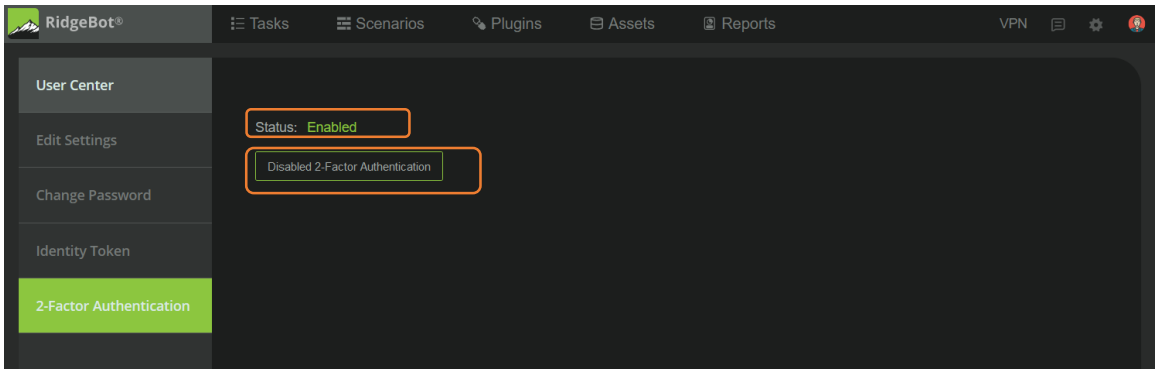


Note: RidgeBot supports Google or Microsoft Authenticator for the 2 Factor authentication code. It is recommended user to install the preferred authenticator in the mobile device before starting the binding process.

4. The next few steps are common to using a Microsoft or Google Authenticator. To illustrate the process using the Google Authenticator in the mobile device, scan the QR code shown in the screen and enter the code from your google authenticator into the "Google verification code" field and click "submit" by the code expired.



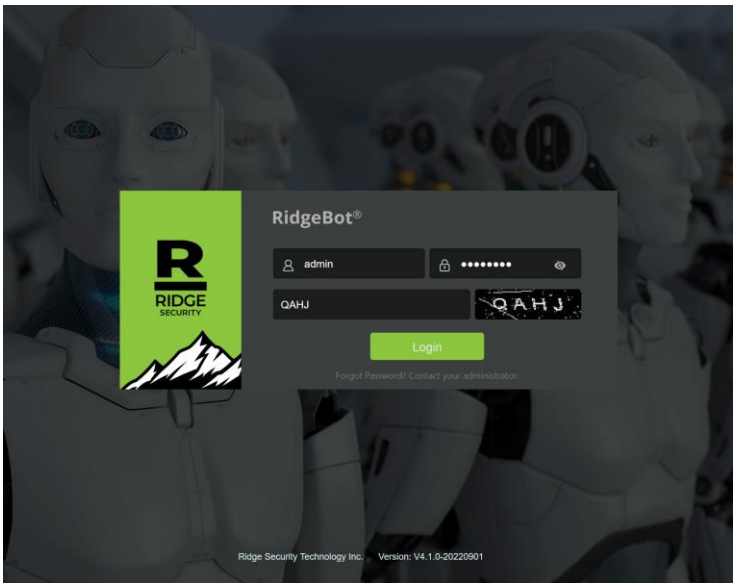
5. Once the code is accepted, the status is now "Enabled"



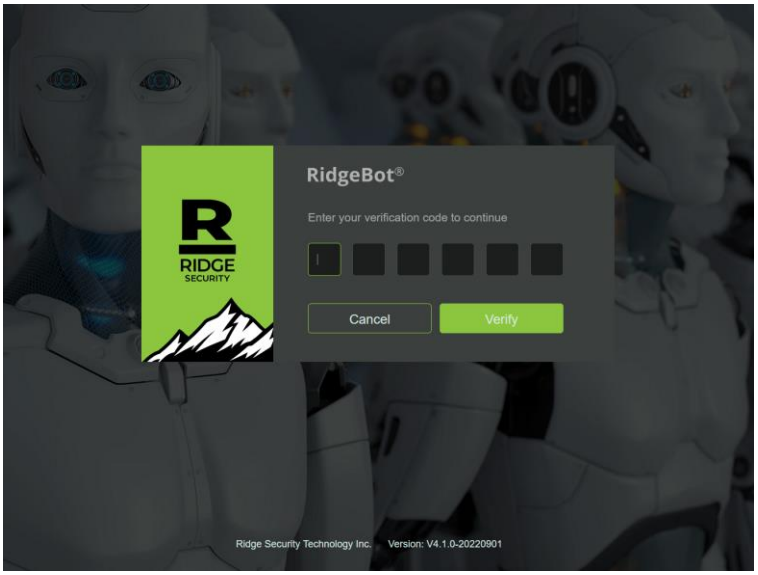
6. To disable, click on the "Disable 2-Factor Authentication"

To Login with 2-Factor Authentication:

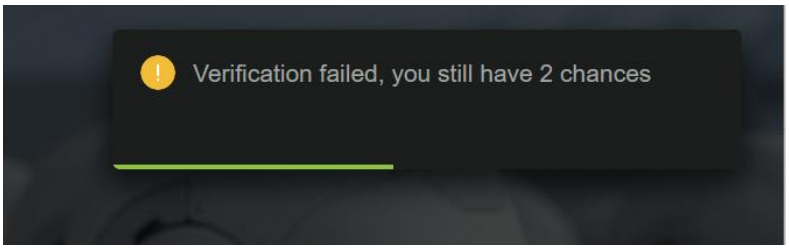
1. Enter the username, password and the captcha verification code



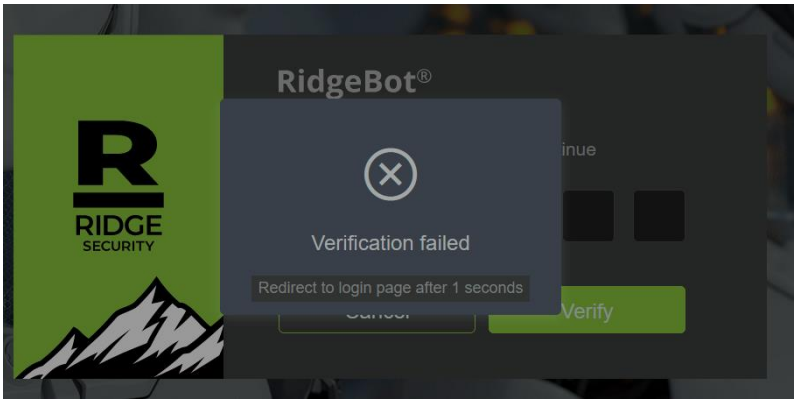
2. Enter the verification code from the google authenticator (from the same account) and click on "Verify"



If the code is incorrect, an error message will display momentarily on the upper left corner.



If the incorrect code is entered three times, the login will be aborted.



Layout of the RidgeBot GUI

After a successful login, the Home Page is displayed.

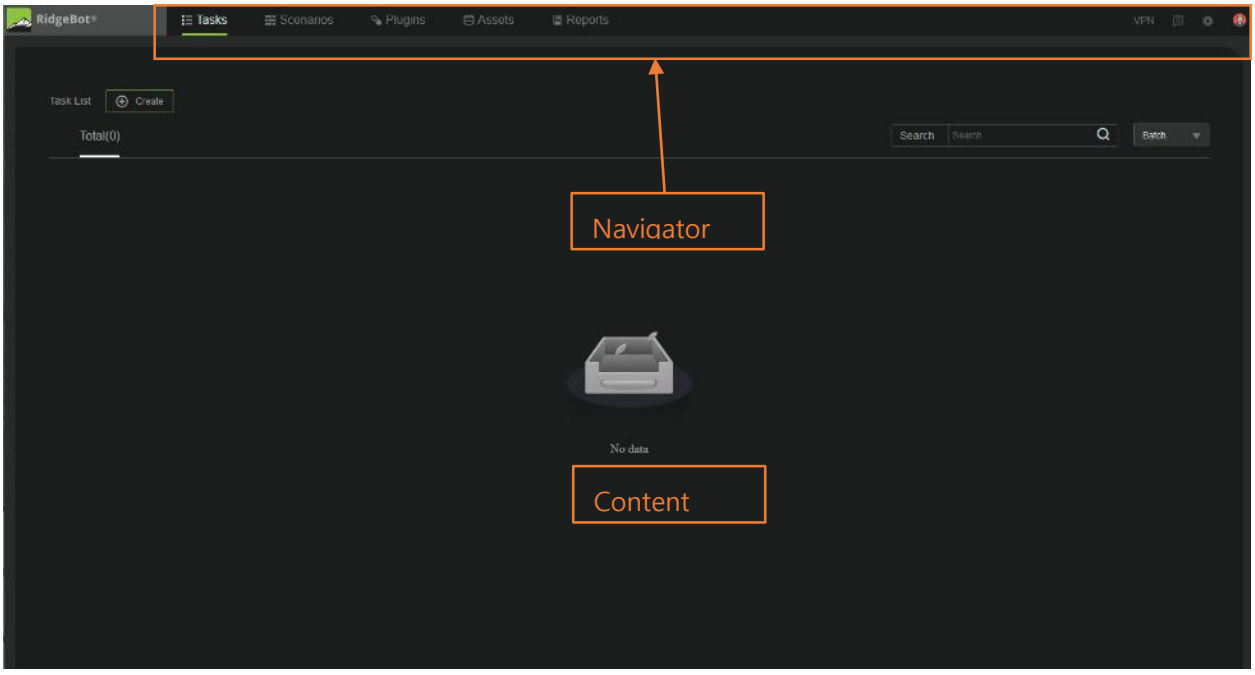


Figure 4: RidgeBot GUI Layout

The **Navigation Bar** is located at the top of the page. It indicates the page you are currently viewing and allows you to navigate to different pages. The following table describes the links on the Navigation Bar.

Link	Description
Tasks	Click to go to the Tasks page where you can get all the specified tasks and create your own tasks. For detailed information about tasks, see Chapter 3 Tasks.
Scenarios	Click to go to the Scenario center where you can view the System scenarios or create and modify Custom Scenarios. For detailed information about scenarios, see Chapter 4 Scenarios.
Plugins	Click to go to the Plugins page where you can create customized plugins and then create your own Web POC. For detailed information about customized plugins, see Chapter 5 Customized Plugins.
Assets	Pull down the menu to select RidgeBot Assets information such as Hosts, Services, Sites, Domains, Credentials and Sessions.
Reports	Click to go to the Reports page where you can check task report information and status. Other actions allow you to download or delete an individual report or a batch of reports. For detailed information about reports, see Chapter 6 Reports and Report Management.
VPN	When you mouse over the button, VPN connection information is displayed. It also provides quick access to the VPN configuration page. For detailed information about VPN configuration, see the VPN section in Chapter 9 System Settings.

Messages	Click to go to the Message Center to see a display of all task messages and RidgeBot messages. You can review the messages and take actions. For detailed information about messages, see Chapter 8 Message Center.
System Settings	When you click the icon, the System Settings menu appears. Click the desired menu item to go to the desired page. For detailed information about all types of System Settings, see Chapter 9 System Settings
	When you click the icon, the user account menu appears. You can edit the account settings or change the account password.

Table 1: Description of the Navigation Bar

The **Content Area** displays detailed information of the feature selected in the Navigation Bar.

- **Tasks**: The task list shows running and completed Tasks.
- **Scenarios**: The Scenario Center shows System and Custom Scenarios.
- **Plugins**: The Plugin List shows user-created plugins.
- **Assets**: The Assets content area shows the information selected from the pulldown menu.
- **Reports**: The Reports content area shows the Report List with the report information and possible selected actions

Chapter 3 Tasks

A task specifies the execution details for RidgeBot to perform a Penetration or Attack Simulation test, including attack targets, attack mode, detection method, dictionaries to be used, proxy, credentials, and plugins.

This chapter has the following sections:

Before creating a task, please read the description of the following task components to gain a better understanding of a task in the RidgeBot system.

- **Scenarios**: A scenario is a pre-defined configuration based on a Penetration or Attack Test use case. It selects the appropriate license type, scan parameters and plugins.
- **Credential**: Credentials are the information used to log on to certain URLs. You can add cookies for multiple domains in the task to simplify the configuration for different attack targets.
- **Plugins**: The RidgeBot system embeds a wealth of vulnerability scanning plugins applicable to different assets and vulnerabilities. Once the plugins are selected and enabled, the system automatically scans and detects vulnerabilities and its subsequent attacks to identify the risks.
- **?**: Explanations are provided for options on the configuration page, and you can get the information by mousing over the question mark icon following option names.

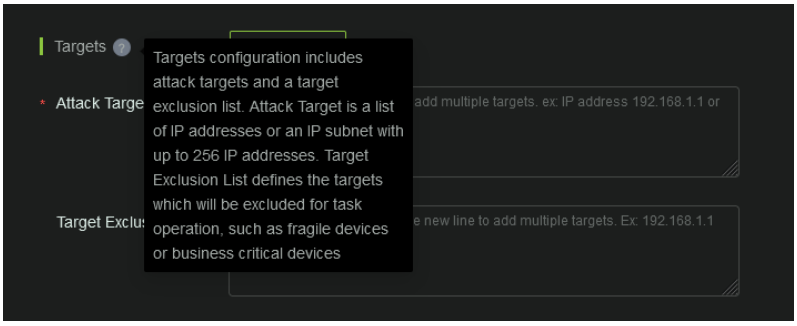


Figure 5: Getting Help

Creating a Task

The task list is blank upon initial access to the RidgeBot system. To create a task, follow these steps:

1. On the **Navigation Bar**, click **Task** to visit the task page.

> **Note**: if this is a first Task, click on the New Task icon.

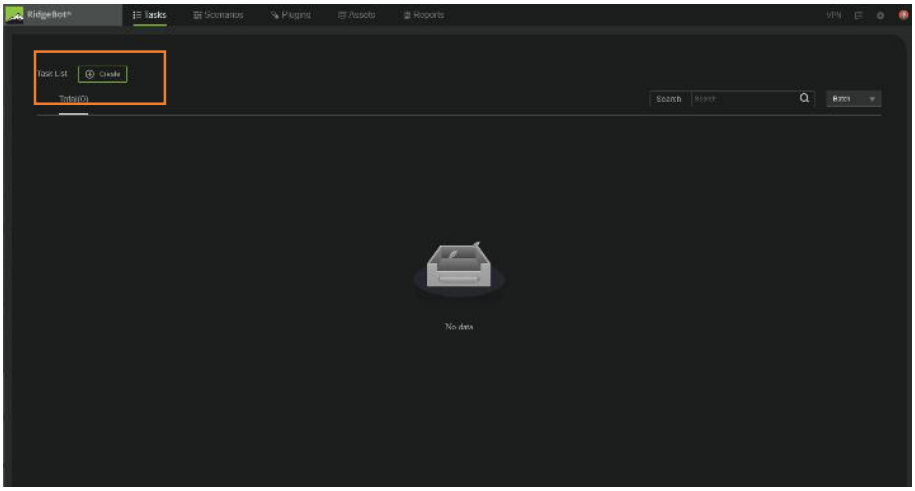
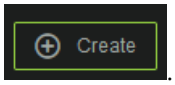
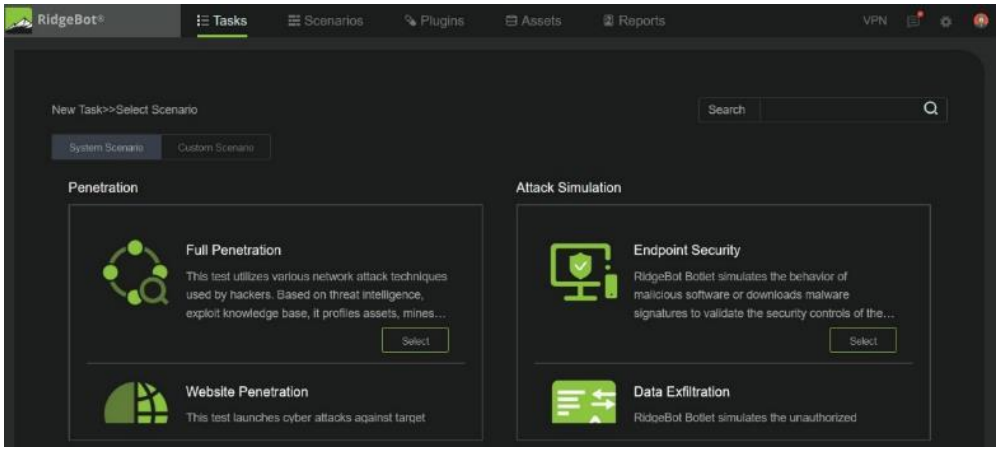


Figure 6: Tasks Menu with no Tasks Configured

2. Click the **+Create** button 

.

3. The **New Task > Select Scenario** page appears. Choose one of the System Scenario icons or a scenario from the Custom Scenario list. You must create a custom scenario to be able to modify the task default configuration parameters and to select plugins.



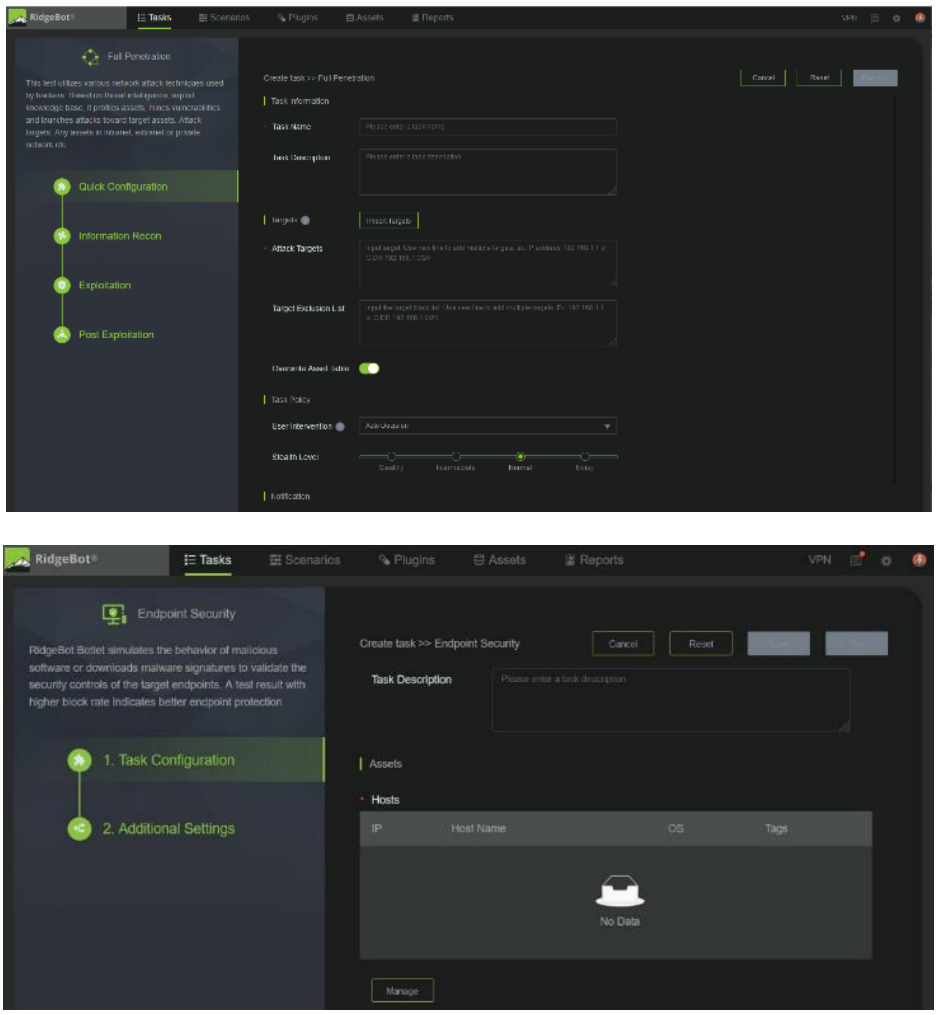


Figure 7: Task Menu –Task Scenario Selection and Task Configuration

Note: This section only describes task related options. For an explanation of scenario options, see Chapter 4 Scenarios.

4. Enter the Task Name.
5. For a Penetration task, enter the Attack Targets. It can be either an IP address or a website URL. For an Attack Simulation task, you select the host targets from a list of Assets.
6. After finishing the above steps, click the **Run Now** button to run the task.

At any step, click the **Reset** button to restore all parameters to the scenario's default settings.

At any step, click the **Cancel** button to return to the **New Task > Select Scenario** page to re-choose a scenario for the task.

After clicking the **Run Now** button, the page display changes back to the Task List and the newly created task is displayed in the list. You can view the status of your task and view detailed information of the task by clicking the name of the task. The remainder of this chapter discusses information about task details and task operations.

Configuring a Penetration Task

On the Task configuration page, the vertical sidebar shows the scenario description of the task and the configuration steps to follow.

To configure a task, you must follow the configuration steps shown in the vertical sidebar menu. In each step, there are required and optional fields to enter information. You can modify the default parameters if available.

Task Configuration – Quick Configuration

The Quick configuration is organized into five sections: Task information, Targets, Task Schedule, Task Policy and Notification.

On the **Quick Configuration** page, you specify values for basic task options.

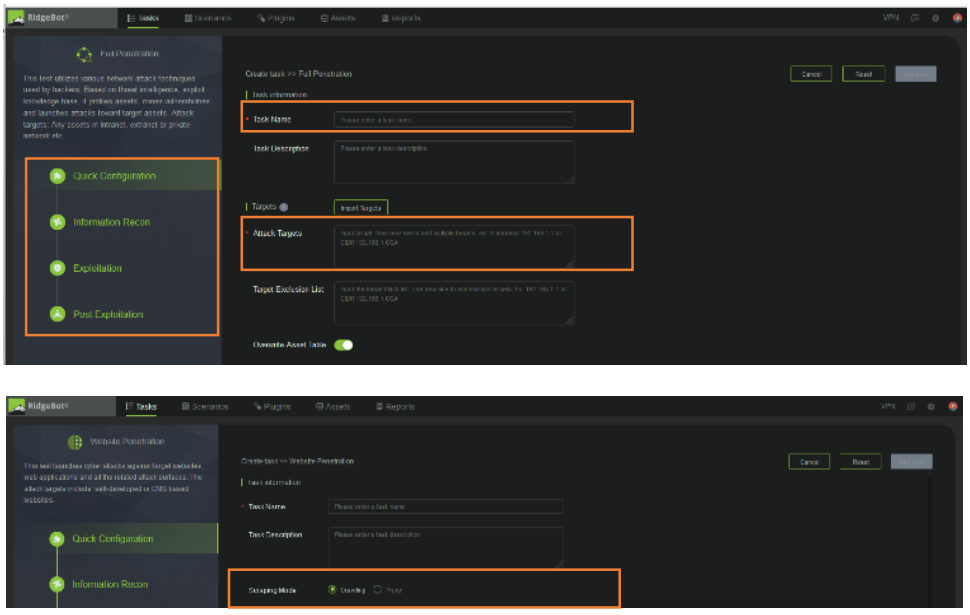
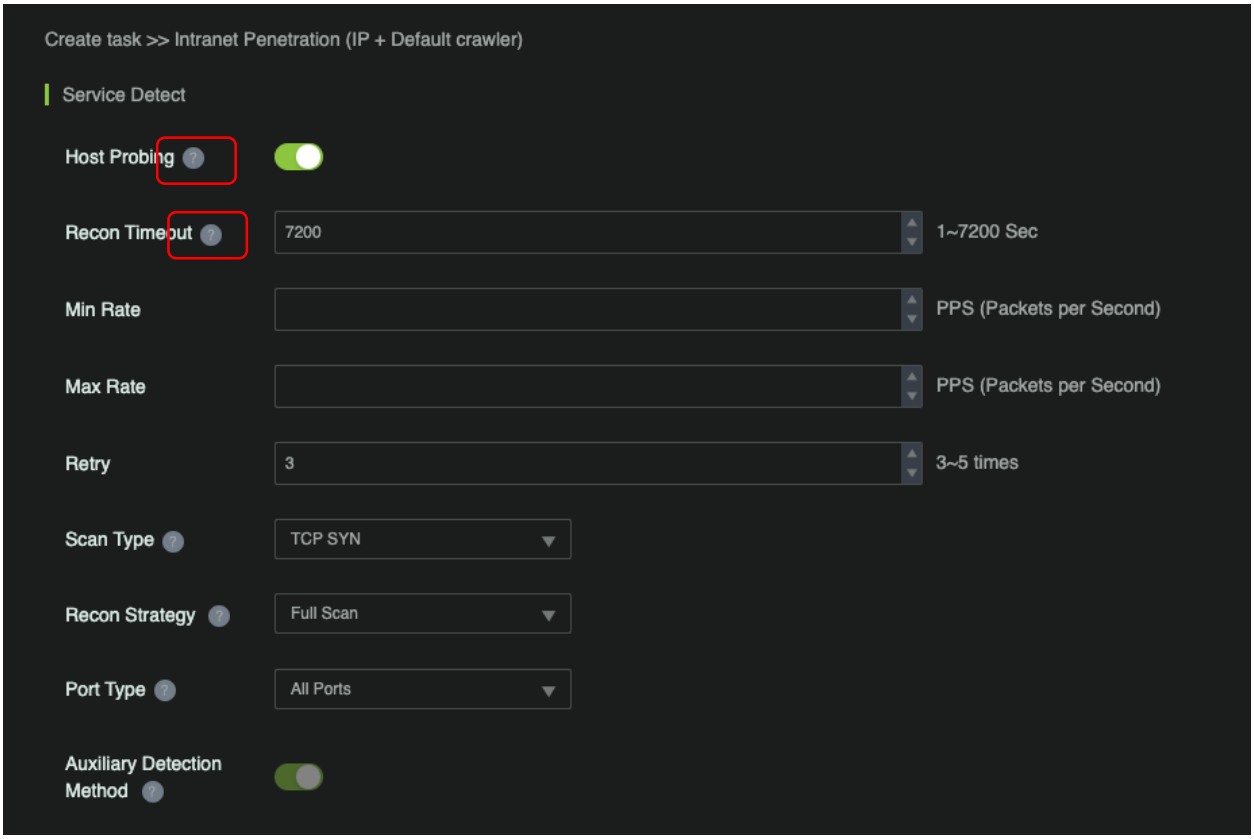
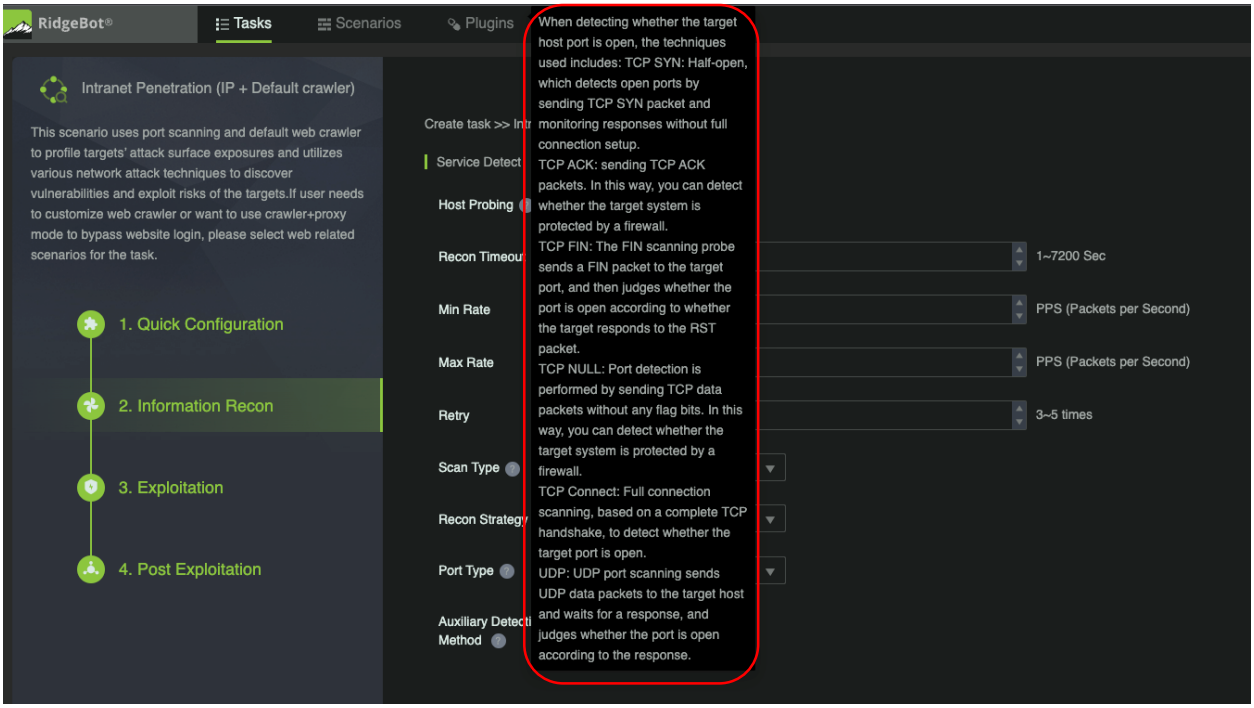


Figure 8: Task Quick Configuration (Top – Host), (Bottom – Web Application)

RidgeBot GUI has a build in help one some of the selections to help the customers to configure the task. These are round buttons with ? mark in it.



Hove the mouse over these buttons a help hint will appear.



1) Task Information

i) **Task Name**: The name of the task is mandatory. Note that the task name is used as the title of the task report.

ii) **Task Description**: An optional field for the description of the task.

iii) **Scraping Mode** (available for Website or 3rd Party framework penetration): This option selects how the crawler searches through the URLs either by crawling or by proxy. **Crawling** is the default mode.

Proxy mode can be used in certain password protected webpages and SPA. In this proxy mode, the RidgeBot crawler will record the URL as selected by the user and then use the URLs to look for vulnerabilities. There are two options:

(1) **Proxy**: This mode is used for manual URL operation. There is no crawler interaction. RidgeBot will record the URL when user clicks on the webpage in the target website. The recorded manual URL is used as the attack surface.

(2) **Proxy and crawler**: This mode uses the recorded manual URLs from the proxy mode and uses a crawler to look for additional attack surfaces from these URLs. The crawler mode automatically selects a static or dynamic mode.

1. **Static**: This mode is for login bypass. After user login, a static crawler uses the cookie obtained by the login continuous crawler. A Proxy+Static crawler can be used for the sites such as PHP, ASP, ASP.net, and WordPress.

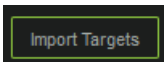
2. **Dynamic**: This mode is similar to the proxy static mode. After user login, a dynamic crawler uses the cookie obtained by the login continuous crawler. A Proxy+Dynamic is used for sites such as HTML5, RESTAPI base SPA and mobile app.

Note: The web crawler is assigned to only one task at any given time. When a user launches multiple web-based scenario tasks, the first task runs while the remaining tasks are on hold until the first task is completed.

Scrapping mode is only available in the web-based scenario. When a task is configured to use a crawler proxy, it could affect other running tasks. It is recommended to have only one "Proxy and crawler" task running in RidgeBot.

See chapter 7 for more information on how to set up scraping proxy mode.

2) Targets

i) **Import Targets**: Click on this icon 

to select and import the targets file.

ii) **Attack Targets**: The attack targets can be IP address network segments, or domain names, based on the selected scenario. To specify multiple targets, enter them individually on different lines (press Enter after each entry). Or you can list the targets in a .txt file, and then upload the file by clicking the **Upload File** button.

iii) **Target Exclusion List**: Enter targets to be excluded. This option is useful to exclude specific targets when the "Attack Targets" entry is a CIDR.

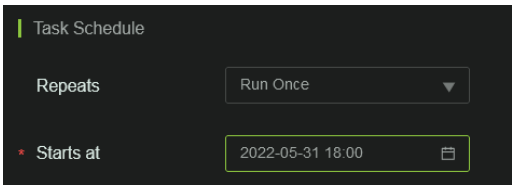
iv) **Overwrite Asset Table**: The default setting is "enabled". When enabled, RidgeBot updates the asset information from this task into the Assets list.

3) Task Schedule

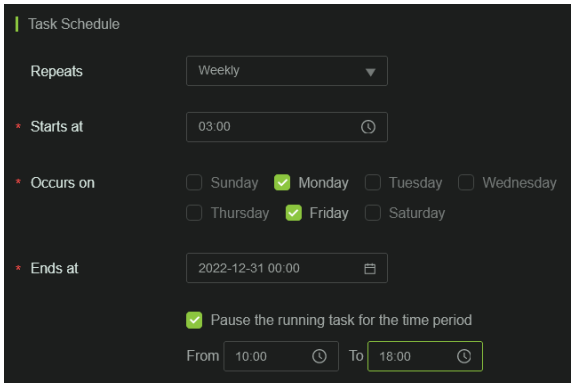
i) **Repeats**: This option allows you to specify a schedule for when the task is run.

(1) **Run now**: Run the task immediately, only once.

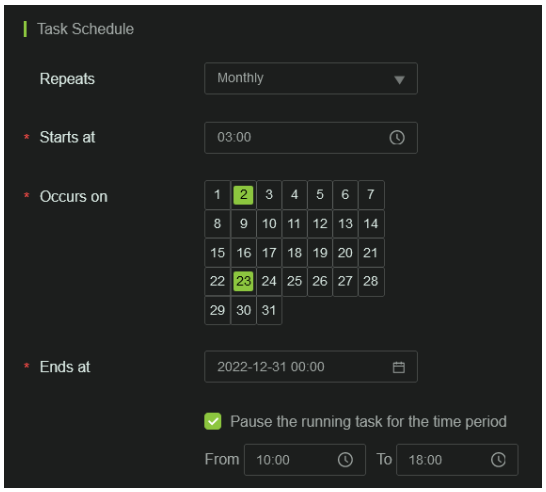
(2) **Run once:** Run the task once at the specified date and time (in 24-hour format).



(3) **Weekly:** Run the task every week on the specified days.



(4) **Monthly:** Run the task every month on the specified dates.



ii) **Pause**: This option allows you to pause a running task during specific time periods to prevent it from interfering with other activities, such as the middle of the working day.

iii) **From** and **to**: For example, if you want to pause the task between 10am (10:00) and 6pm (18:00), you configure this in the From and To fields. Times are configured in 24-hour format.

4) Task Policy

i) **User Intervention**: This option allows you to manage individual plugins to minimize the impact on the target.

(1) **Auto Decision**: RidgeBot automatically executes the selected plugins on the targets.

(2) **User Decision**: RidgeBot waits for user acknowledgement before executing high impact plugins on the selected target. If an email notification is set, RidgeBot sends an email notification every 4 hours. If the user does not respond within 24 hours, RidgeBot ignores the high impact plugins in the list and completes the task.

ii) **Stealth Level**: This mode provides the option to control the packet rate to a target and have different response timeouts from the target. For each selection, the penetration testing

task duration is varied. There are four settings: Stealthy, Intermediate, Normal, Noisy. Each setting has a different level of traffic behavior to minimize being detected by security devices and can improve the interaction with a target in certain test environments. Each setting predefines different delay, retry and timeout timers, offering a tradeoff between speed and results.

(1) **Normal** is the default mode that balances between penetration testing task duration and typical target response times.

(2) **Stealthy/Intermediate** modes are useful to minimize detection by a security device and to handle targets with slow responses. It has a response timeout greater than 60sec and a request delay that varies between 24 to 4 sec. The mode increases the overall test duration.

(3) **Noisy** mode gets a quick scan of a target. The response timeout is less than 15sec. This mode is useful in a controlled test environment.

5) **Notification**: Specify the email addresses to receive task results. This function requires a mail server to be configured. See Chapter 9 System Settings > Email for more details.

Task Configuration – Information Recon

The Information Recon has a Service Detect or Crawler configuration based on the selected scenario. The Host-based scenario contains a Service Detect configuration, while Web application-based scenarios use a Crawler configuration.

This section allows you to customize parameters based on the target.

1) **Service Detect configuration**: You can modify network parameters that can affect the discovery, fingerprinting and services of the targets.

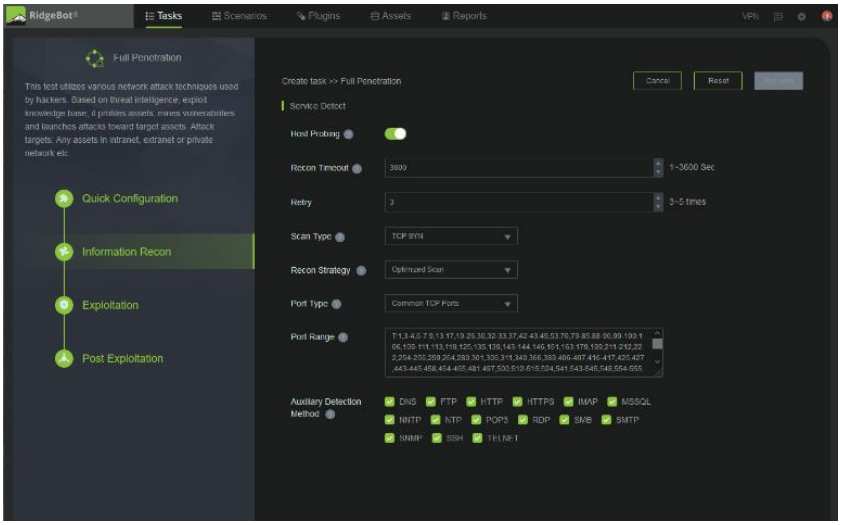


Figure 9: Scan Proxy Configuration

a) **Host Probing**: Enable or disable probing.

b) **Recon Timeout**: Set the maximum wait time for a response from the target during the discovery process.

c) **Retry**: Set the number of retries following a recon timeout.

d) **Scan Type**: TCP Syn (Default), UDP Scan, TCP Ack Scan, or TCP Fin Scan.

e) **Recon Strategy**: This parameter sets the strategy to send various types of packets to the target during the fingerprinting process. The options are Fast, Full or Optimized Scan (default).

   (i) **Fast Scan**: RidgeBot sends only Null packets to a target for IP port fingerprinting.

   (ii) **Optimized Scan**: RidgeBot sends only default protocol packets to a target's well-known IP ports for IP port fingerprinting, for example, sending SSL packets to port 443.

   (iii) **Full Scan**: RidgeBot sends all possible recon packets to a target and uses all the available rules in RidgeBot's database to detect the target's port fingerprints.

f) **Port Type**: Selects the type of ports to use. Options are Common TCP Ports (default), Common UDP Ports, Common Ports, All Ports, Vulnerable Ports, Enterprise Intranet, Database or Custom Ports (user specified port(s)).

g) **Port Range**: This option shows the port defined by the Port Type selection. When Custom Ports type is selected, you must enter a port number or a range of port numbers.

h) **Auxiliary Detection Method**: This option is used to gather OS/System information from the application response data to improve the accuracy of fingerprinting.

Notes: Selecting "Common Port" shows the common service port numbers.

2) **Crawler Configuration**: Under this tab you can customize web crawler parameters such as the maximum running time, the total number of pages to crawl, the total depth to go down in a path, the algorithm for removal of duplicates, suffix filtering, keyword-based URL whitelist entries, and URL Filter entries (blacklist). **Note**: It is recommended to add the website logout URL in the URL Filter to prevent the crawler from logging out of the website during operation. An example of a logout URL is: https://bot.ridgesecurity.ai/logout.

   a) **Crawler Mode**: The default mode is Intelligent. Other options are Static or Dynamic. Intelligent mode allows the crawler to automatically select Static or Dynamic based on the webpage. Static mode is applicable to static web pages. The Dynamic crawler mode is typically used for websites that use dynamic update web pages such as Single Page Application (SPA).

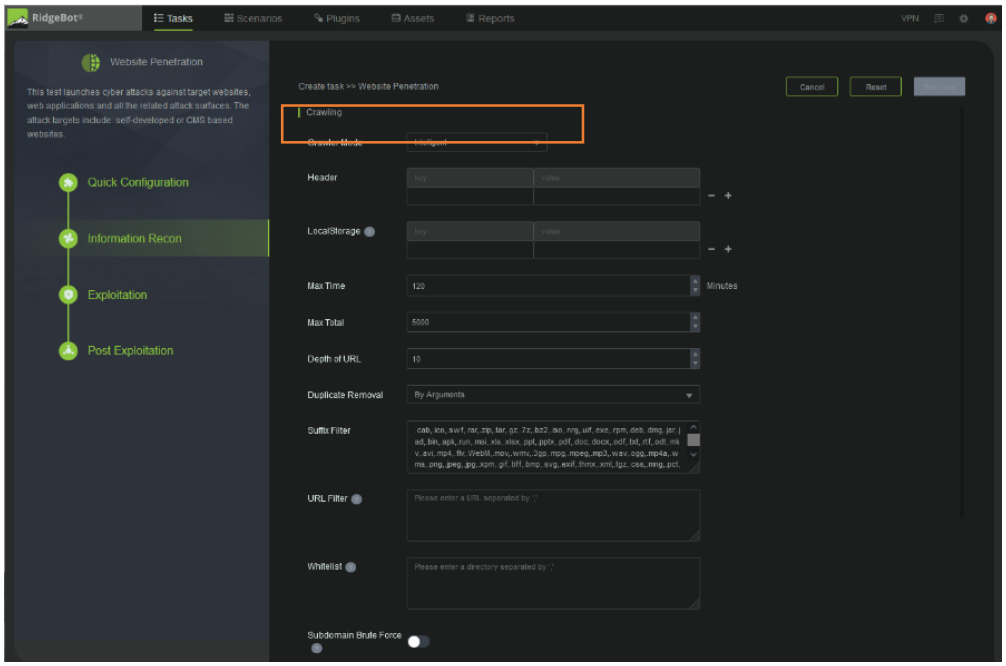


Figure 10: Crawler Configuration

   b) **Header**: Use this field for HTTP header cookie name/value pairs and other HTTP header parameters.

   c) **Local Storage**: Use this field to enter the web browser's local storage name/value.

   d) **Max Time**: This is the maximum time allowed for the crawler to search.

   e) **Max Total**: This parameter sets the maximum number of pages of the web URI for the crawler to examine.

f) **Depth of URL**: This parameter defines the number of levels that the web crawler indexes in the URL path.

g) **Duplicate Removal**: Removal duplicate URLs based on Arguments, Paths or None.

h) **Suffix Filter**: A pre-defined set of suffixes is given, and you can add additional suffixes in this field.

i) **URL Filter**: The URL listed in this field is blacklisted and excluded from the crawler. This list can be set up to prevent the crawler from triggering an URL that can affect the result unexpectedly.

j) **Whitelist**: The directory listed in this field is accessed by the crawler.

k) **Subdomain Brute Force**: This option is disabled by default. Recursive Subdomain Brute Force uses the dictionary to try to gain access to all possible URLs at all levels.

l) **404 Page Policy**: This attribute is optional. Some websites return a successful response code for a non-existing webpage. This attribute sets the policy for the crawler to terminate this specific search. The 404 Page Policy allows an entry for the HTTP message status code, location, and body.

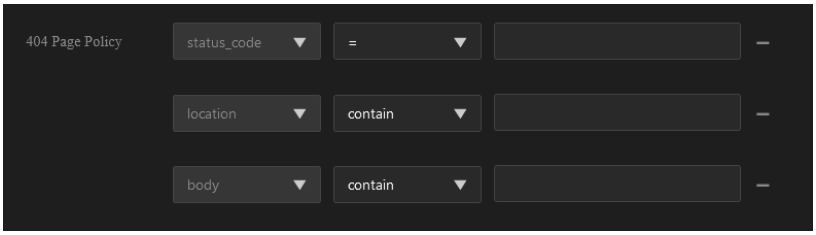


Figure 11: 404 Page Policy

m) **URL Rewrite Policy**: This feature replaces an URL with another one, as defined. Use the + to add additional policy entries. Use – to delete an entry.

n) **Web Form Autofill**: This allows you to enter the key and value of the web form. RidgeBot uses this information to get access to the form.

Task Configuration – Exploitation

Click the **Exploitation** tab on the vertical sidebar menu to display the Exploitation Policy configuration. You can configure a policy to manage the attack and exploitation of the target.

1. **Risk Control**: This parameter allows you to select the plugin based on the impact category to be used in the attack/exploitation of the target.
2. Brute Force:

a) **Password Brute Force**: This option is enabled by default. When enabled, RidgeBot tries the dictionary username and password to gain access to the target.

b) **Brute Force Method**: Password Guessing (the default) uses one account with different passwords from the dictionary. Password Spray uses multiple accounts with one password from the dictionary.

c) **Service Type**: This option selects a specific dictionary to execute a brute force attack. The default is to select all.

3. **Attack Strategy**: Auto-Exploitation is enabled by default. You can disable the auto-exploitation feature, and then RidgeBot does not use plugins that exploit the detected vulnerability.

> **Caution**: Disabling Auto-Exploitation may impact vulnerability detection in the targets since RidgeBot may use the same plugin to find and exploit vulnerabilities in a target.

4. **WebShell Policy**: This policy is only applicable to Web application scenarios. This policy is set up for WebShell to automatically do a cleanup.

Task Configuration – Post Exploitation

RidgeBot uses a "Botlet" to perform Post Exploitation such as privilege escalation and lateral movement on a compromised host via an RCE vulnerability. It scans and profiles the asset to find attack surfaces and then launches attacks on the host. Once it compromises the host, a Botlet looks for other potential targets from which the compromised host can be accessed.

Typically, a Botlet scans the target(s) looking for attack surfaces and vulnerabilities to launch an attack. Once it compromises a target, it tries to elevate its privilege using SUID in Linux or exploit the MS16-032 Windows secondary logon service, and then launches Post Exploitation using weak password brute-force and RCE attacks on the secondary target.

Starting with version 3.4, a Botlet can do Post Exploitation attacks using SSH, SMB, MySQL server, weak password brute-force attacks and RCE attacks for Elasticsearch, Hadoop, ShellShock, Strut2, vsftpd, and Weblogic. Additional Botlet capabilities will be added in subsequent software releases.

> Notes:
>
> 1. A Botlet does not perform high-risk attacks that can cause a target to crash.
>
> 2. A Botlet's weak password dictionary is a subset of the RidgeBot system's weak password dictionary. In the current version, the Botlet dictionary cannot be modified.

3. A Botlet's run plugin can be identified by the extension (Post Exploitation) in the plugin name.

4. A Botlet does auto clean up. A Botlet self-terminates under the following conditions:

a. If the target reboots. A Botlet operates in the target's memory, and it is removed if the target reboots.

b. When the task is deleted, a Botlet removes itself from the target.

c. When a Botlet loses communication with RidgeBot, it removes itself within 7 days.

Post Exploitation configuration defines the lateral movement parameters under which RidgeBot can continue to find and exploit vulnerabilities in other hosts. Note: It is required to provide the lateral movement targets.

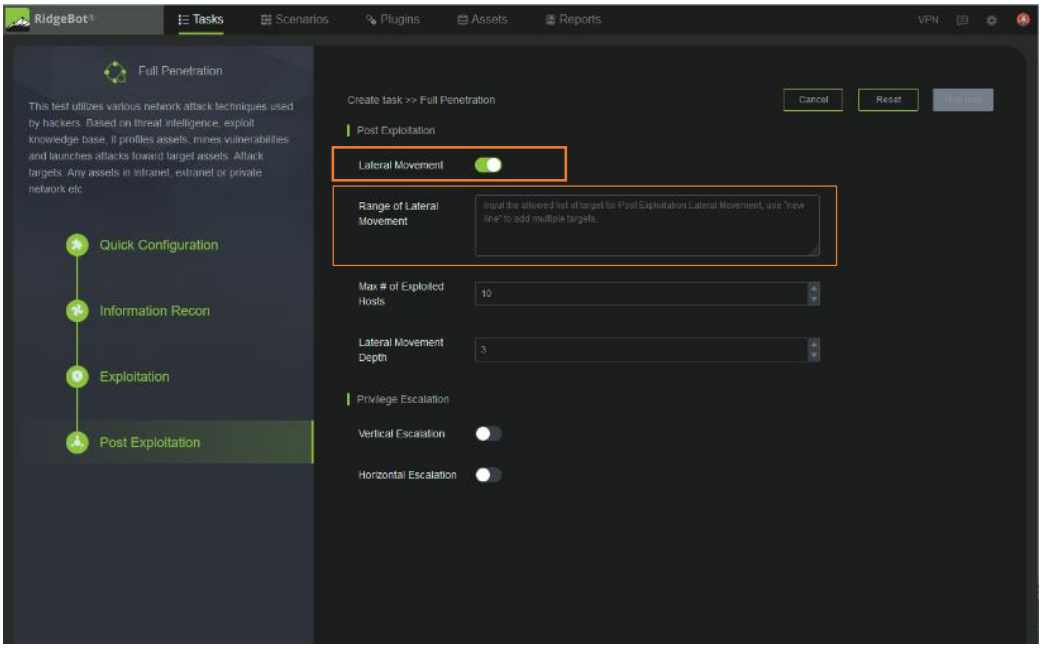


Figure 12: Post Exploitation Configuration for Lateral Movement

1. Post Exploitation

   a. **Lateral Movement**: This option is enabled by default. RidgeBot performs lateral movement based on potential targets listed in the Range of lateral movement.

   b. **Range of Lateral Movement**: Enter the targets to be exploited initiated from an exploited target.

   c. **Max # of Exploited Hosts**: Defines the limit of the number of hosts to be exploited by RidgeBot in a lateral movement.

d. **Lateral Movement Depth**: Defines the limit of the number of levels of hosts that can be exploited by RidgeBot in the lateral movement.

2. **Privilege Escalation**: Defines the privilege escalation approach taken by RidgeBot.
    a. **Vertical Escalation**: RidgeBot tries to get root privilege of the target.
    b. **Horizontal Escalation**: RidgeBot tries to get an escalated privilege on the exploited target in a lateral movement.

Task Configuration – Dictionary and Plugin

- **Brute-force dictionary**: As of version 3.9, a task only uses dictionary files defined at the system level. This brute-force dictionary is used for password matching.
- **Plugin**: As of version 3.9, the Plugin list is pre-defined in a set of system scenarios. User can create a custom scenario, and selects the desired plugins to be included.

Configuring an Attack Simulation Task

On the Task configuration page, the vertical sidebar shows the scenario description of the task and the configuration steps to follow.

To configure a task, you must follow the configuration steps shown in the vertical sidebar menu. In each step, there are required and optional fields to enter information.

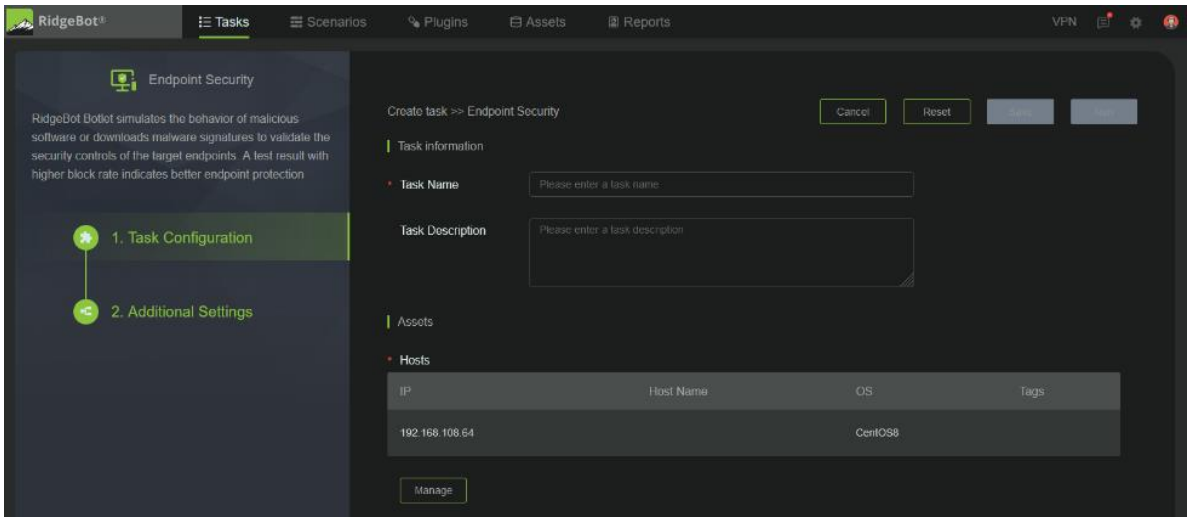


Figure 13: Attack Simulation Task Configuration

Configuration of an Attack Simulation task is organized into four sections: Task information, Assets, Task Schedule, and Notification.

Task Configuration

On the **Task Configuration** page, you specify values for basic task options.

1) Task Information
   a) **Task Name**: The name of the task is mandatory. Note that the task name is used as the title of the task report.
   b) **Task Description**: An optional field for the description of the task.
2) Assets
   a) **Hosts**: This section allows you to enter the targets of the attack. Click the "Manage" button to add host assets to the list. For a host to show up in the Available hosts lists, it must have a Botlet agent installed and online. For more information, see Chapter 3 Installing a Botlet.

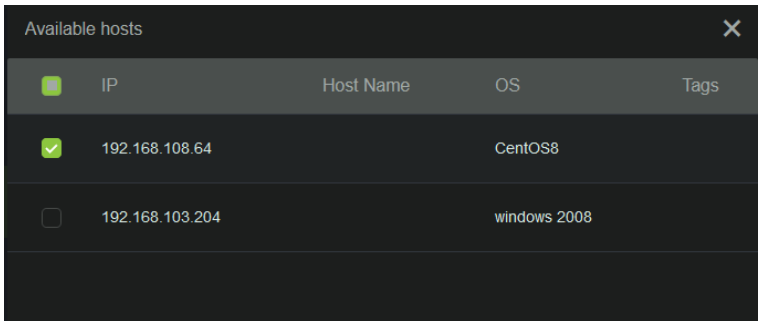


Figure 14: Selecting Hosts with Agents Installed

3) **Task Schedule**: The task schedule is set up in exactly the same way as for Penetration Test tasks, as described in Chapter 3 Quick Configuration.
4) **Notifications**: Task notifications are set up in exactly the same way as for Penetration Test tasks, as described in Chapter 3 Quick Configuration.

Additional Settings

On the **Additional Settings** page, you can choose the applicable **Assessment Tests** that you want to employ in your task from three categories: Threat Groups, Attack Tactics and Attack Techniques. The choices shown on the page depends on the scenario the task is based on. By default, all available choices are selected, and you can deselect any that you do not want RidgeBot to use.

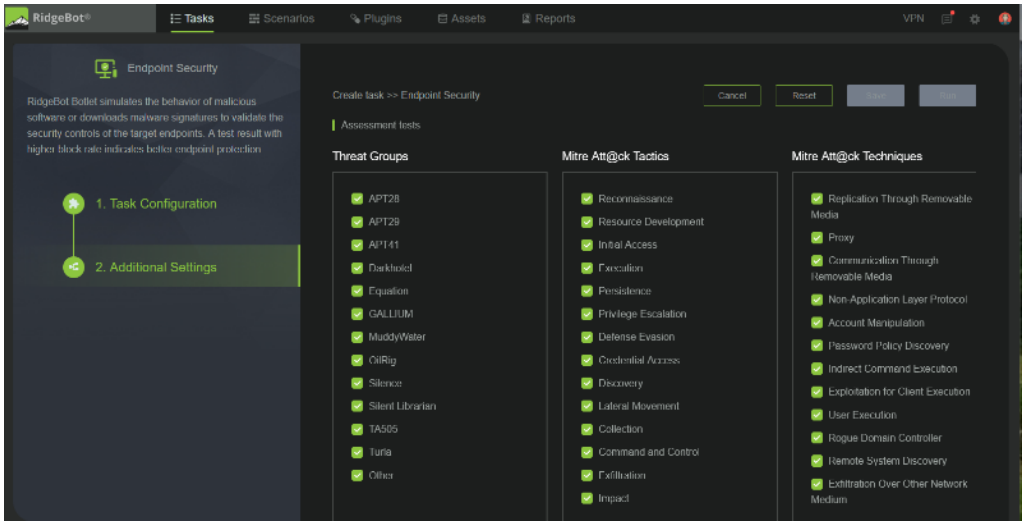


Figure 15: Attack Simulation Additional Settings Configuration

Installing a Botlet

While Penetration Testing tasks are agentless, Attack Simulation tasks require an agent (a Botlet) to be installed and running on the target. To install a Botlet agent, follow these steps:

- Select Assets from the Navigation Bar. Then choose **Hosts** from the drop-down box. If a host is not available in the **Assets > Hosts** list, you can add a host to the list by clicking on **Create** and fill in the information in the **Create Host** pop-up dialog box.

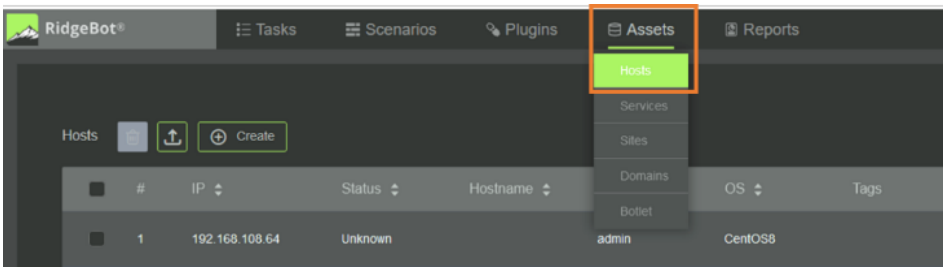


Figure 16: Entering a Botlet Configuration

- The above action displays a list of all your host assets as shown below. The "Botlet" column in the display shows an Online or Install status. **Online** means the Botlet is running on the target. **Install** indicates a Botlet must be installed in the target.

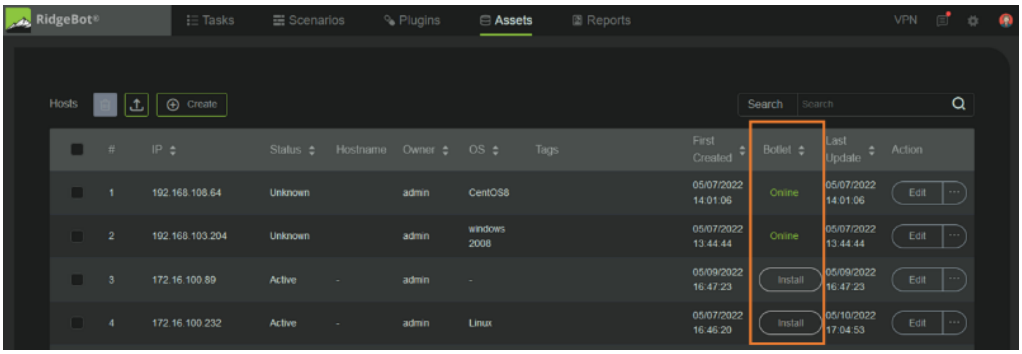


Figure 17: Host Asset List Showing Installed Botlets

- There are two options to download a Botlet:
  - i) Click on **Install** to download a Botlet to the selected host as shown above.
  - ii) Select Botlets from the Assets pull down menu as shown in the figure previous to the one above.
- The page below then appears where you can choose the host interface to be used for the download, as well as the operating system of the target machine.

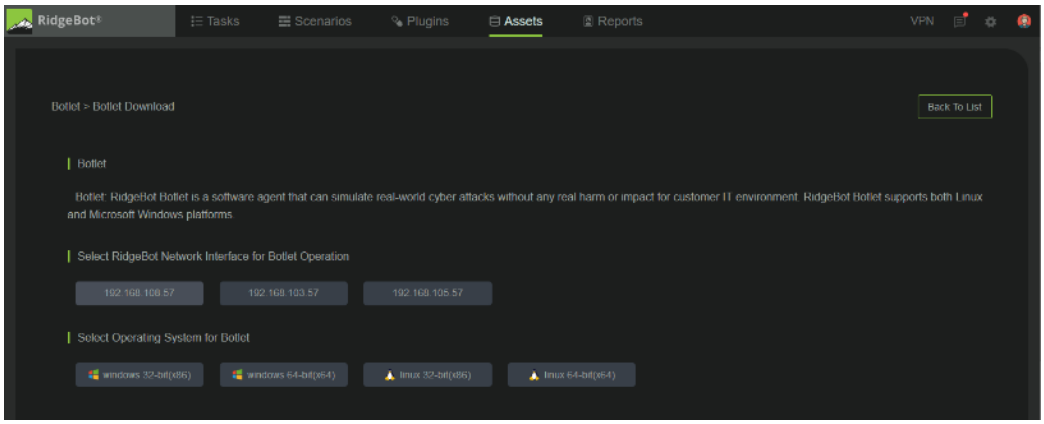
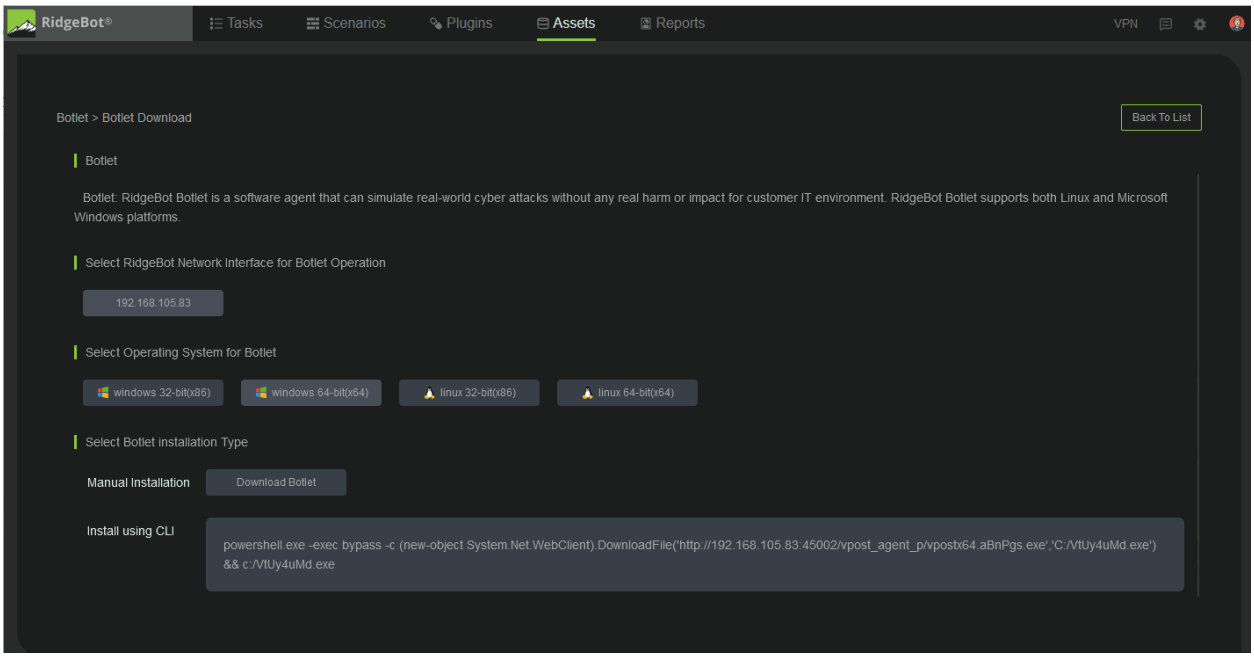


Figure 18: Installing a Botlet on a Target

When user selects the host machine OS, a Botlet installation Type selection is available for user to install a botlet using a download application or using CLI. Below is an example of the Botlet installation option for Windows Operating System.



To install using the Manual installation option, click on the **Download Botlet** button and follow the pop-up instructions

Note: If this is the first time downloading a Botlet, a security warning is popped-up as shown below. Click on **Accept the Risk and Continue** to initiate the download.

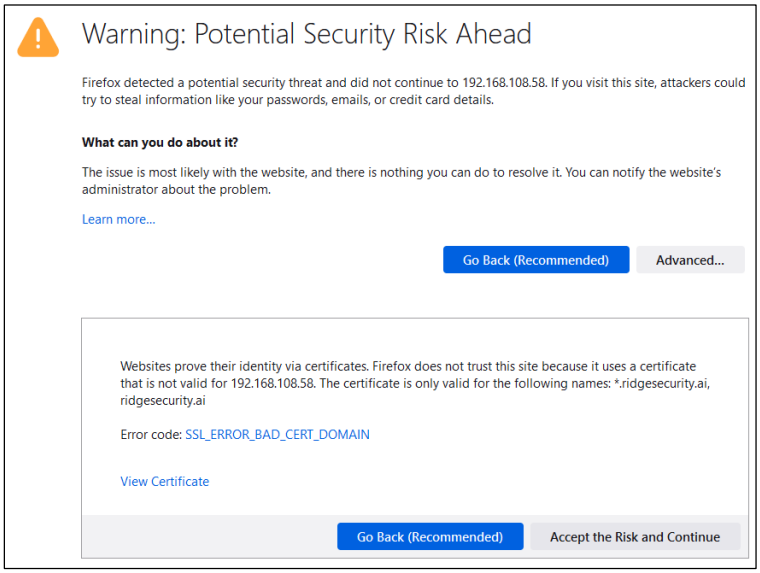


Figure 19: Security Warning when Downloading a Botlet

Upload the Botlet application to the windows server and launch the Botlet application.

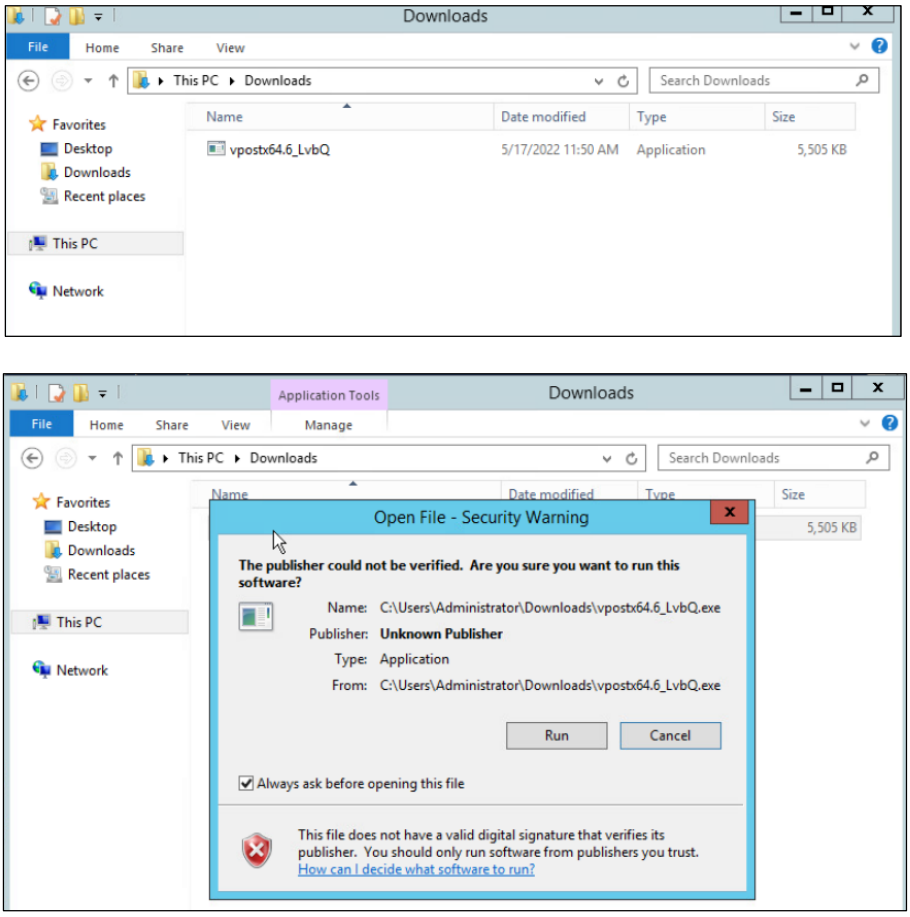


Figure 20: Downloading a Botlet onto a Windows Server

Click **Run**.

In Windows Task manager, confirm that the Botlet application is running.

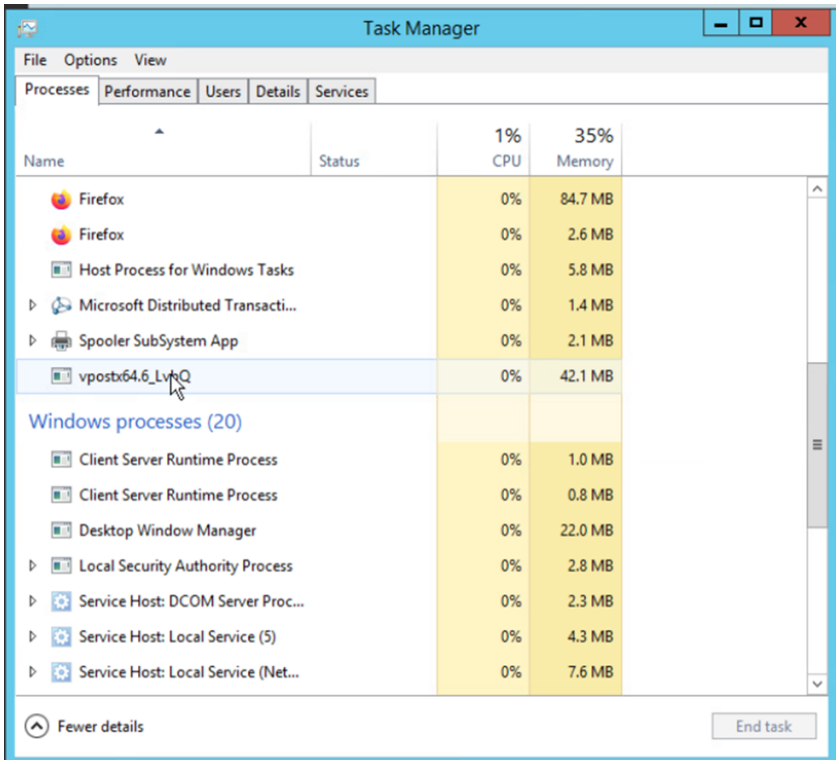


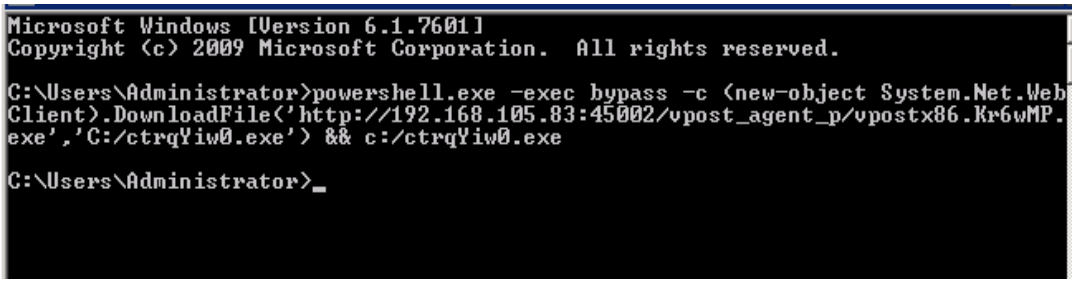
Figure 21: Windows Task Manager Shows the Botlet Application

To install Botlet in Windows using CLI.

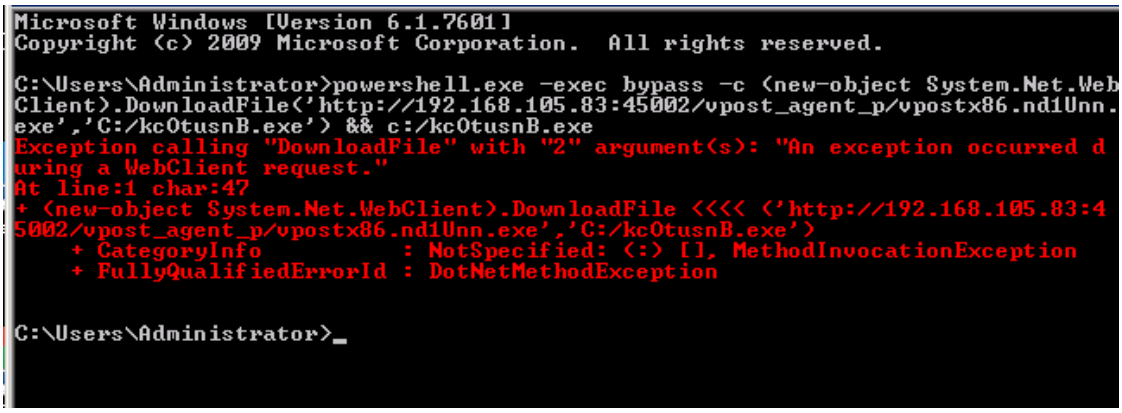
a. Copy the CLI command from RidgeBot

b. In the windows target, open a "Command Prompt" with Administrator privilege

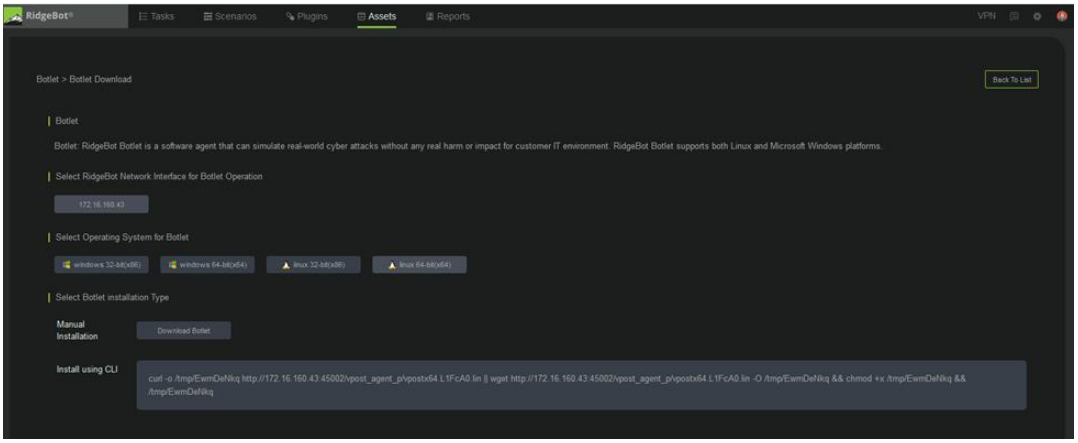
c. Run the CLI command in this command prompt terminal. Note: the CLI command will start with "powershell.exe -exec…."



d. If user encounters an error when running the CLI command as shown below. User can request a new CLI command from RidgeBot and rerun with the new CLI command.



To install a Botlet onto a Linux machine, copy the CLI command from the Botlet download page and run the entire command line on the Linux target machine.



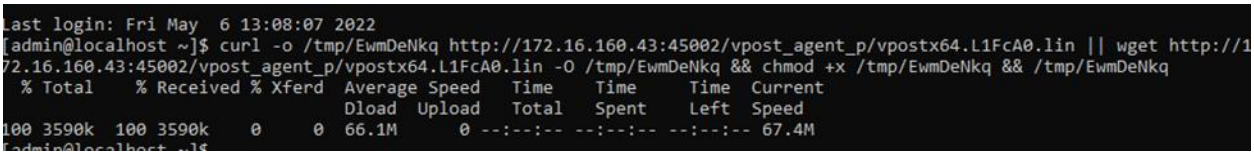


Figure 22: Installing a Botlet onto a Linux Machine

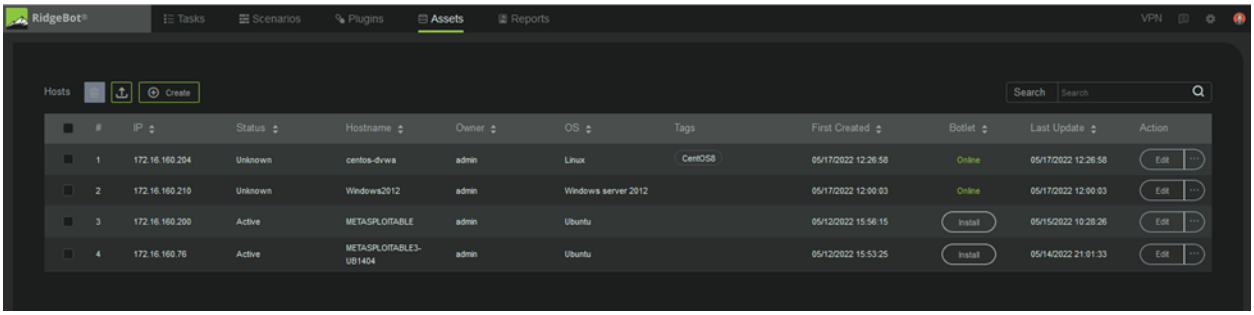
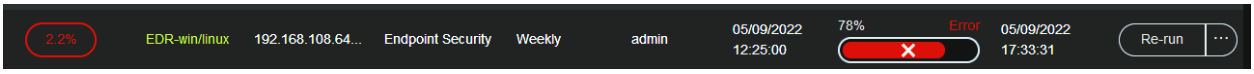


Figure 23: Assets Display Showing Online Botlet

Note: If an Attack Simulation task tries to run and the Botlet agent on the target machine cannot be contacted, or is no longer present or installed on the target, the task shows an Error status. If so, the Botlet must be reinstalled on the target machine.



Uninstalling a Botlet

If a Botlet has been previously installed on the target, and you want to remove (uninstall) it, follow these steps:

- On Windows machine, go to the Windows Task Manager. Select the Botlet name in the **Processes** Tab **Name** column and click **End Task** to terminate the Botlet.

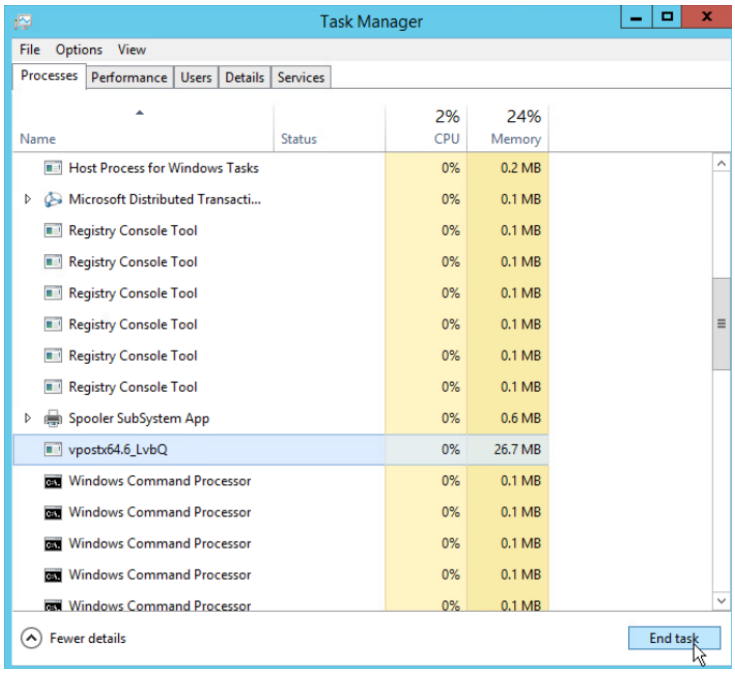


Figure 24: Windows Task Manager Display to End a Botlet Task

- On a Linux machine, use the **ps -ef** command to find the Botlet process id. Then run the **kill -9 process_id** command to terminate the Botlet process.
- Power cycling the target machine also uninstalls the Botlet.

Botlet Limitation

- Botlet can only be installed in Windows Operating System target with Microsoft anti-virus defender or off-the-shelf commercial anti-virus disable.

> Note: As a workaround, Botlet can be added to the antivirus exclusion list.

Working with Tasks

All tasks created in the system are displayed in the Task List. There are two lists: Penetration Test tasks (default display) and Attack Simulation tasks. Each entry in the list displays the task details, progress, results, and actions that can be taken.

A task can be managed from the menus in the **Action** column at the far right of the screen, and the available options depend on the status and progress of the task. The most likely action is displayed directly on the page, and you can click the … next to it for other available options.

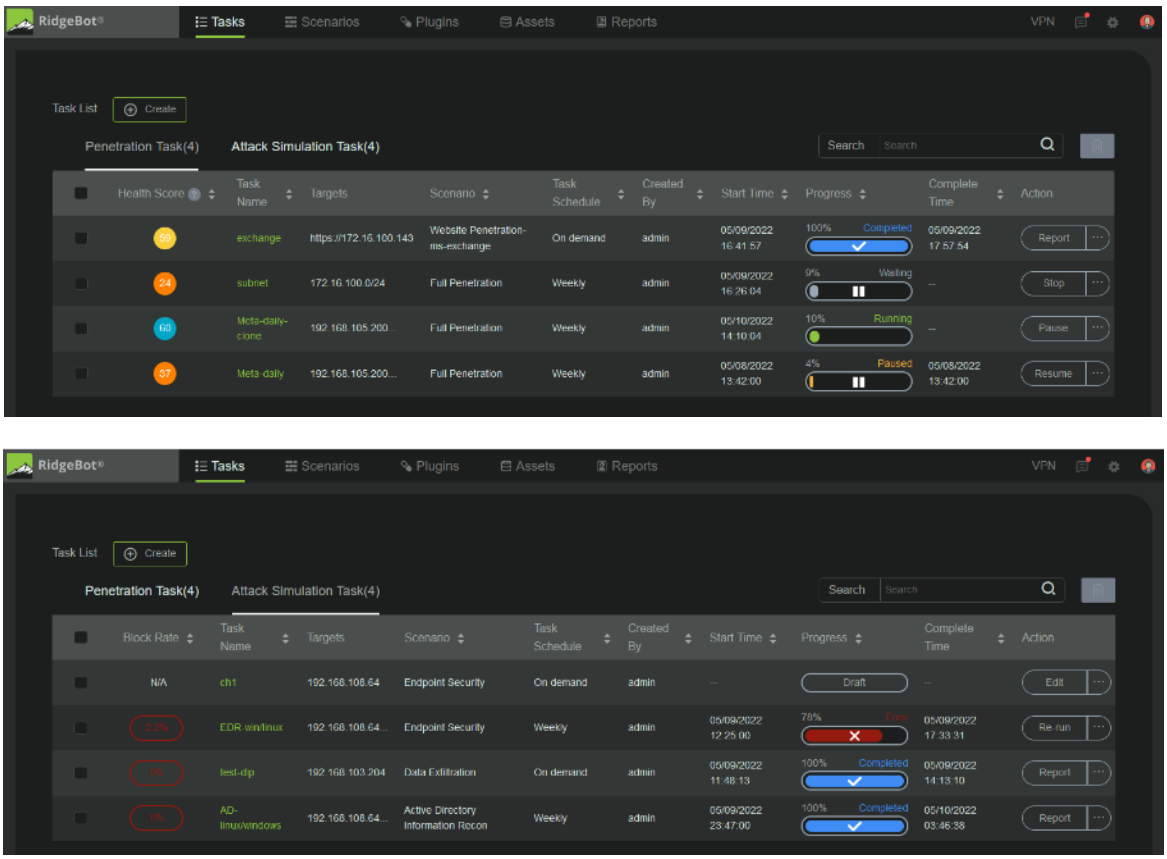


Figure 25: Penetration and Attack Simulation Task Lists

Viewing Task Details

Across the top of the task display is a series of task attributes that summarizes the tasks.

- **Health Score:** This attribute is applicable only to Penetration Tasks. The task health score is a color-coded rating based on a 100-point scale. It represents a comprehensive evaluation derived from multiple factors of the task targets, such as the number of risks, vulnerabilities and attack surfaces.
    - Severe Risk: Less than 20
    - High Risk: >=20 and <40
    - Elevated Risk: >=40 and <60

        - Guarded Risk: >=60 and <80
        - Low Risk: Great than, or equal to 80
- **Block rate:** This attribute is applicable only to Attack Simulation Tasks. The number shown indicates the percentage of attacks that were successfully blocked by the target. A low number represents severe risk and a higher number less risk.
- **Task Name**: The task name identifies the task and is used as the title of the report.
- **Targets**: The targets defined for this task to run attacks against. Mouse over the entry to see the full list of targets.
- **Scenario**: The scenario that the task is based on.
- **Task Schedule**: Specifies how often the task is run.
- **Created By**: The user that created the task.
- **Start Time**: The date and time when the next instance of this task will be started.
- **Progress**: Task status and percentage completion. Possible task statuses include Draft, Running, Paused, Cancelled, Pending, Waiting, Scheduled, Completed, or Error.
- **Complete Time**: The date and time when the task was completed or paused. No end time is shown for actively running tasks.

Task Actions

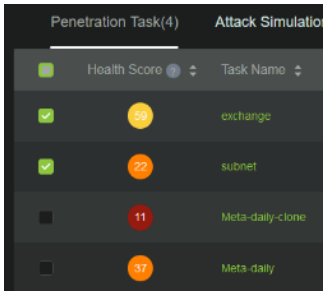
Many different actions can be taken on a task to view information about the task and its current results, or to change the status of a task.

- To view detailed information on a task, click on the task name.
- To generate a report for a completed task, click on the buttons in the Action column to select **Report**. A full report is only available for completed tasks, for more information, see the Reports and Report Management section. An interim report showing current results (but not final results) can be viewed for a running task by selecting Report Preview.
- In the **Action** column to the right of the task list display, available actions based on a task status are shown.
    - A running task can be **stopped** or **paused**.
    - Any task can be **deleted**.
    - A task in the Paused state, can be **resumed**.

- A task can be **cloned**. This makes a new version of the same task configuration which can then be edited and run as a new task with slightly different parameters.

- For a running penetration task in **Pending** status, go to the attack confirmation tab to confirm or ignore. A task in **Pending** state is waiting for additional input from the user before it can run.
- A non-running task can be restarted by selecting **Re-run**.
- To search for a certain task, enter a keyword into the **Search** box at the upper right of the page and click the search button.

- Select the checkmarks on the left of the task list to delete one or multiple selected tasks.



Batch Deletion of Tasks

RidgeBot provides a convenient batch task deletion function. To use this feature, follow these steps:

1. Select the tasks to be deleted by clicking the box to the left of the task in the Task List page. Selected tasks are marked with a green tick mark. To select all tasks, click on the box at the top of the column. Clicking on the box again cancels the selection.
2. Once you have selected all the tasks to be deleted, click on the  button at the top right of the screen.

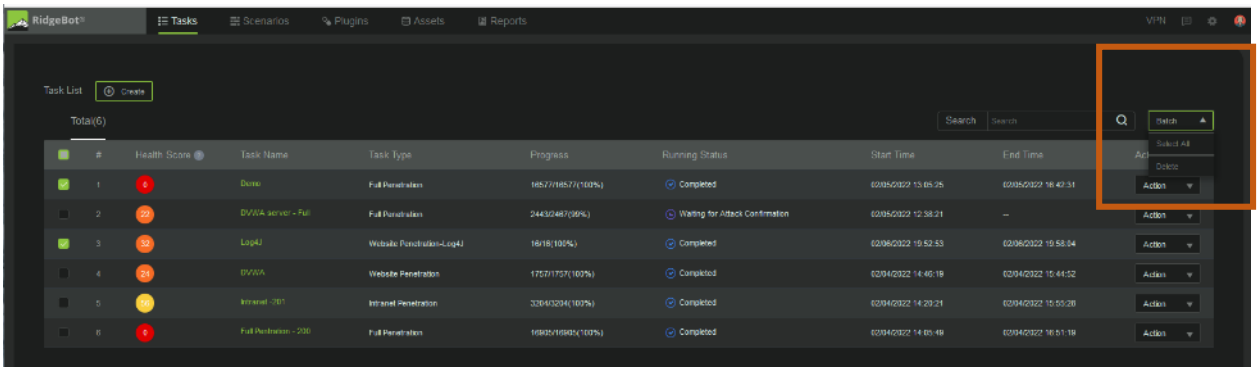


Figure 26: Batch Task Actions

Operating on a Penetration Task

To operate on a penetration task, click on **Tasks** in the Navigation Bar, and then on **Penetration Tasks** underneath it. This shows the task list of all penetration tasks defined in the system.

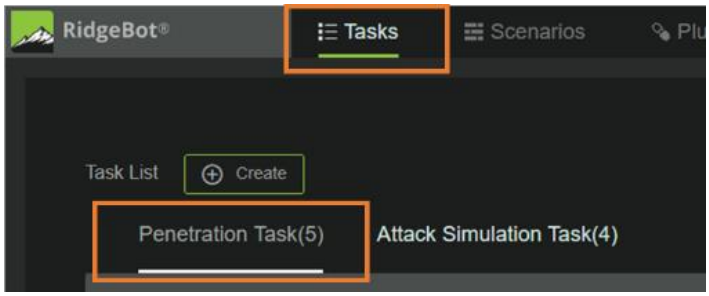


Figure 27: Viewing the Penetration Task List

Each task has multiple windows to display a variety information. There are two interactive displays: Navigation and Topology.

Viewing a Penetration Task – Task Tab Overview

By default, the Navigation view is displayed when you click on any penetration task name in the task list. Additional information about the task such as the topology view, task summary, attack information, asset information, vulnerabilities, and risks are organized in a Task Tab bar at the bottom of the screen. You can switch to any of the categories of information by clicking the associated icon on the Task Tab.

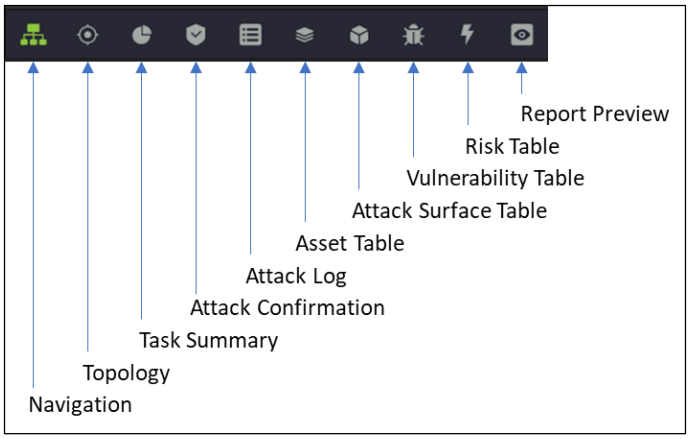


Figure 28: Penetration Task Tab Layout

The sections in the remainder of this chapter provide detail on each of the displays resulting from selecting an icon on the Task Tab.

Navigation View

The Navigation View of the task is displayed if you click on the task name in the task list, or if you click on the Navigation icon in the Task Tab. The Navigation display shows all the target nodes and their associations to another nodes. This view is useful in the Post-Exploitation phase with multiple exploited targets.

By mousing over a node in the display, you can view node details, the attack path, the attack surface, the vulnerability and the risk.

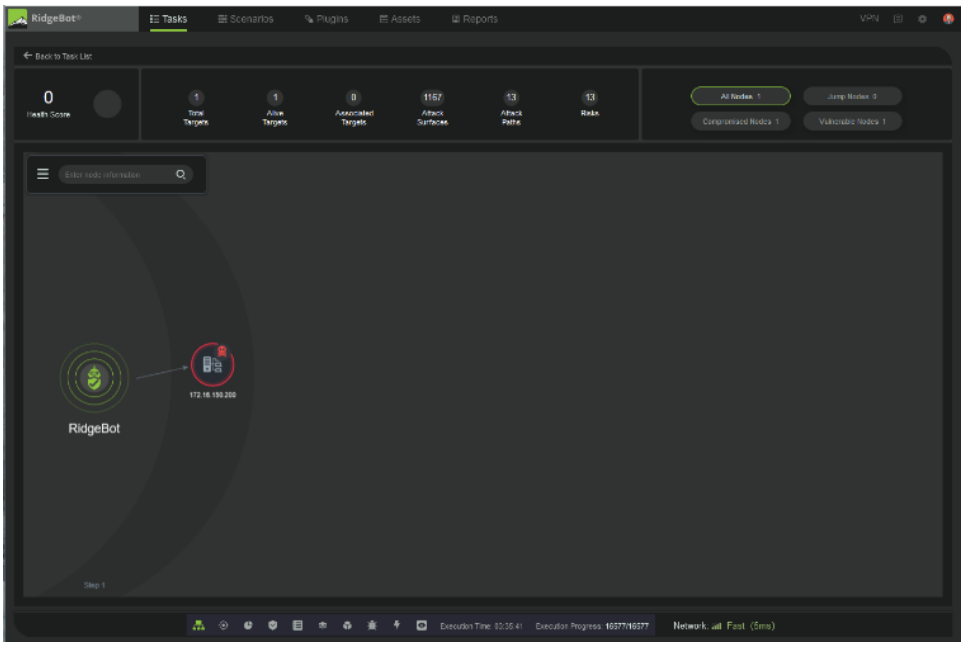


Figure 29: Task Navigation View

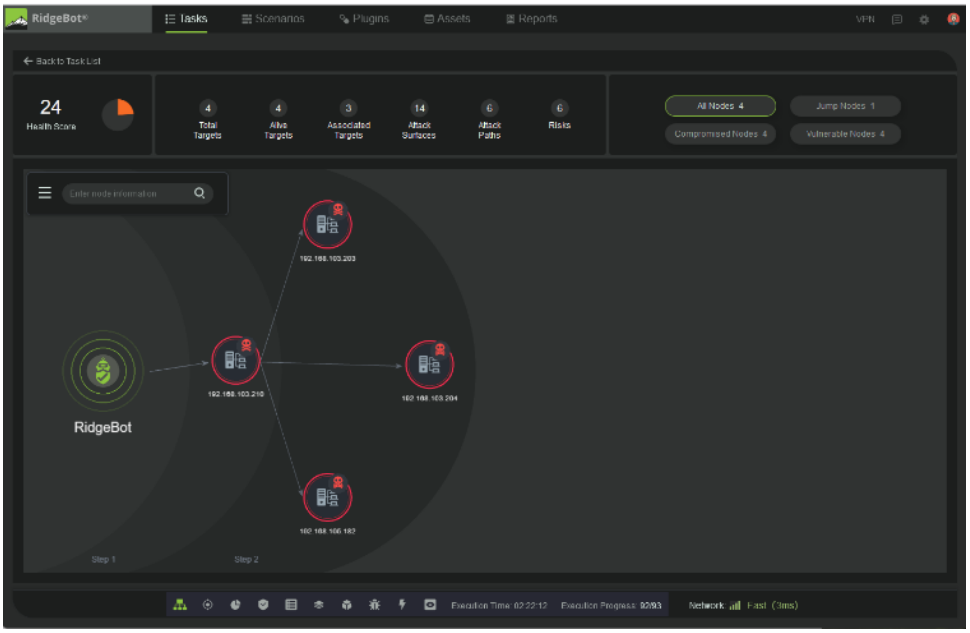


Figure 30: Navigation View with Multiple Nodes

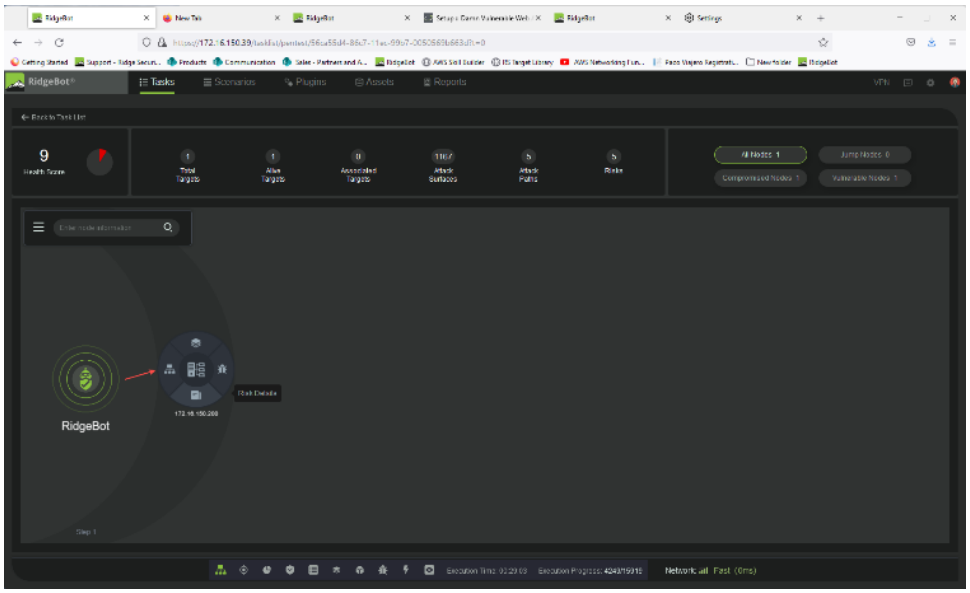


Figure 31: Node Details

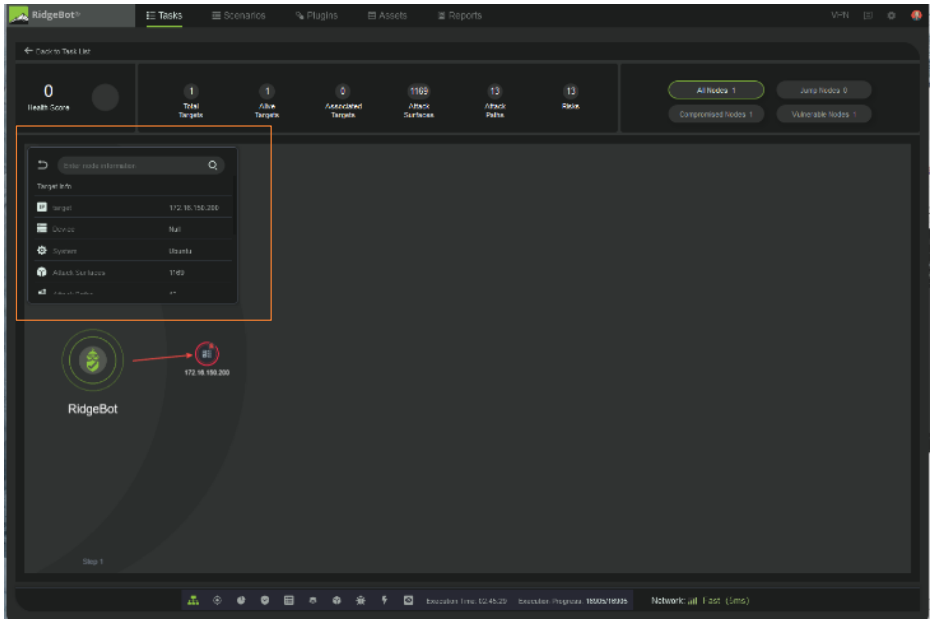


Figure 32: Node Details: Target Information

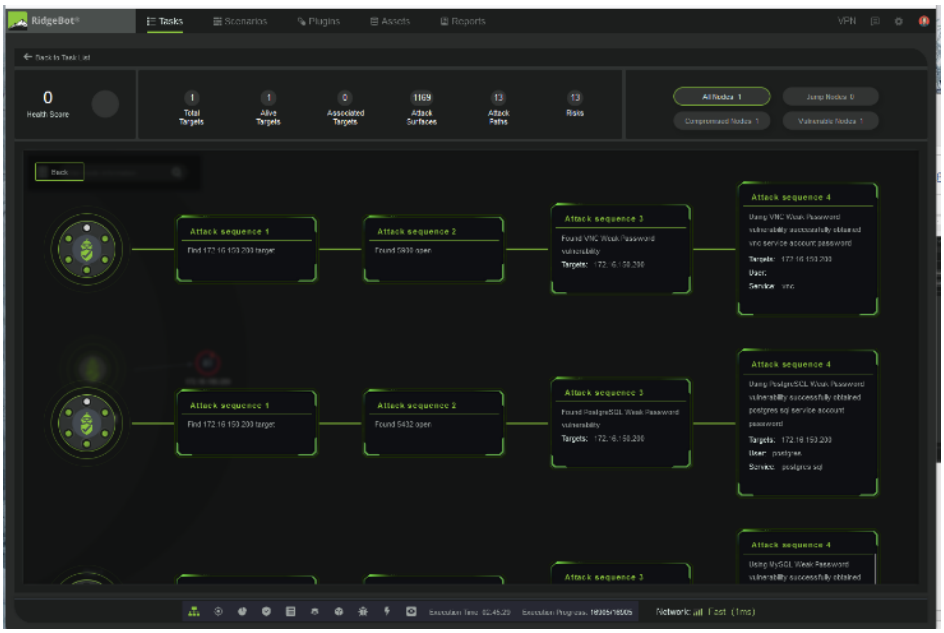


Figure 33: Attack Path Details

Topology View

The Topology view is the main display of the task. It shows the attack node information, real-time attack path, real time action event and risk. This page has two panels on the left and right of the page. The left panel shows Task Operation options, while the right panel shows the Risk detail including the Kill Chain, and each node's detail when you click on a node in the Topology View.

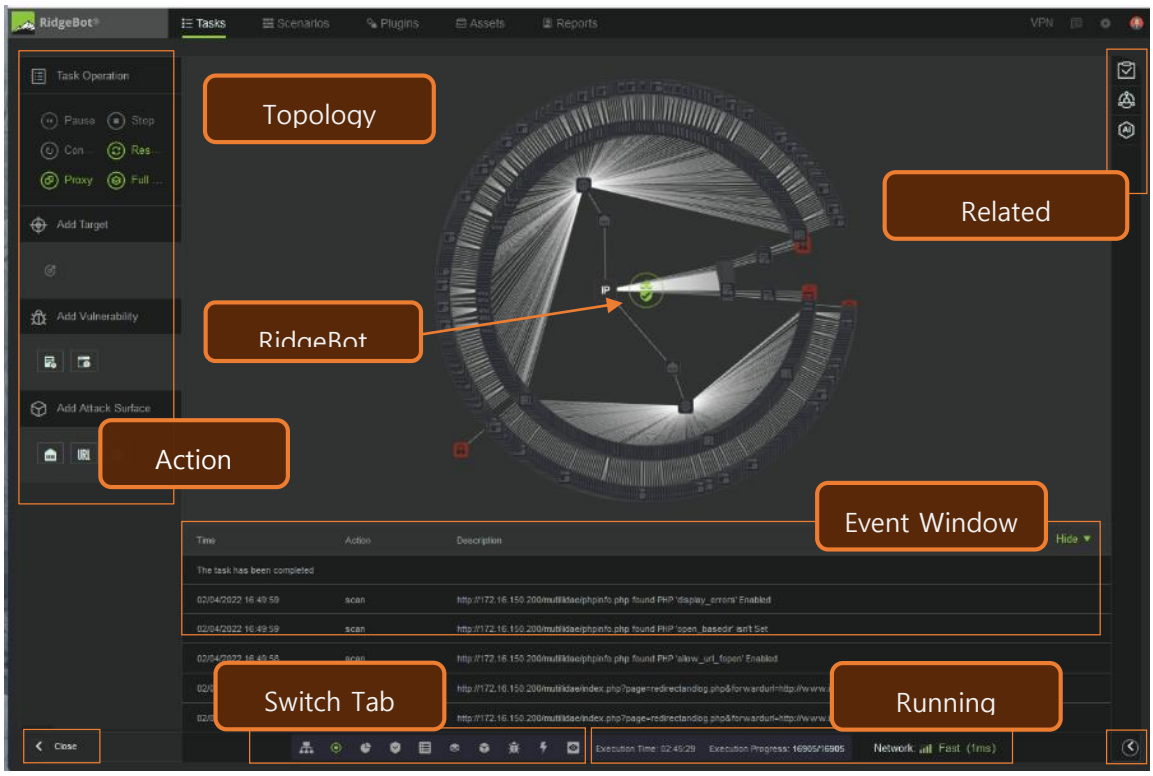
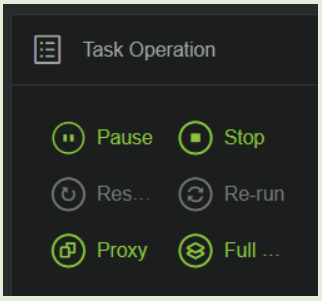


Figure 34: Task Detail Page

Action Pane

The **Action Pane** provides actions that can be taken on the current task. The table below provides descriptions of the actions:

Action Group	Description
	Click an icon to take an action on the task.

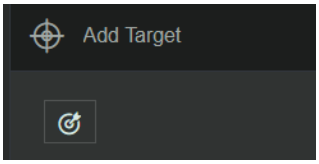
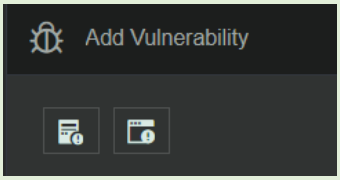
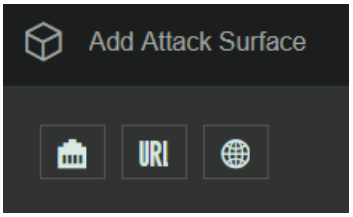
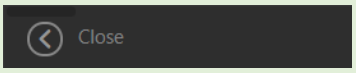
	Click on icons in this group to add targets while the task is running. After the targets are added, RidgeBot scans them. Multiple targets can be added.
	Click on icons in this group to add vulnerabilities while the task is running. **Note**: RidgeBot does NOT perform exploitation on added vulnerabilities.
	Click on the icons in the group to add attack surfaces while the task is running. After the attack surfaces are added, RidgeBot performs attacks on them.
	Click to fold/unfold the action pane.

Table 2: Task Action Pane

Steps to Add a Target

Follow these steps to add a target:

1. Ensure the task is running.
2. In the **Add Target** group, click and hold to select the **target** icon, drag the **target** icon to the RidgeBot icon in the topology, then release the mouse button.
3. Enter information in the text box at the node and click **Save**. Parameter values can be specified for the added target.

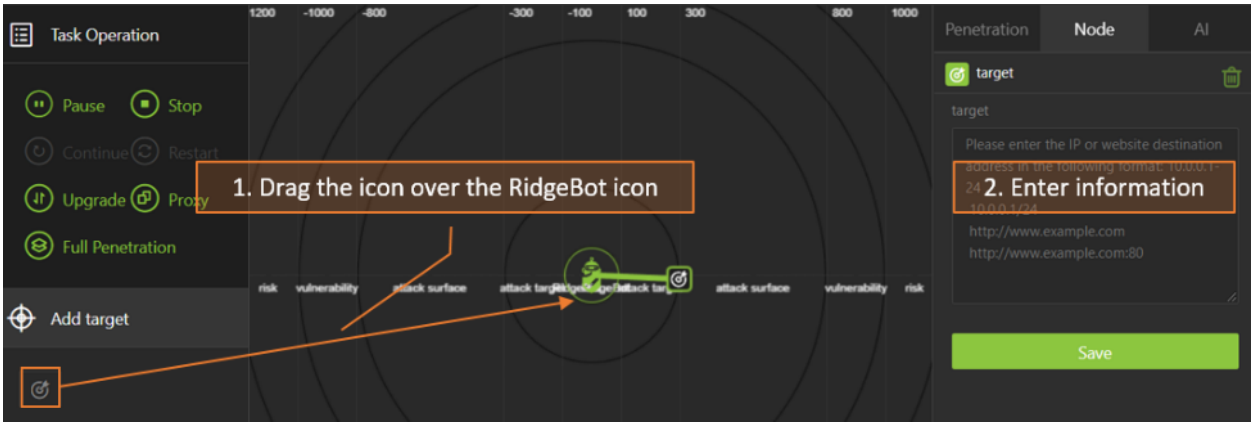


Figure 35: Add a Target

Added nodes can be deleted. To do so, select a node in the topology, and click the delete button at the right of the page.

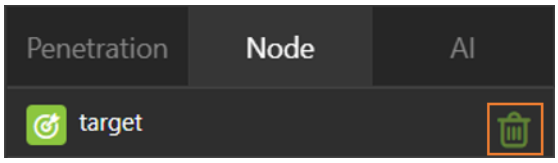


Figure 36: Delete an Added Target

Steps to Add a Vulnerability

Follow these steps to add a vulnerability:

1. Ensure the task is running.
2. In the **Add Vulnerability** group, there are options to select a Host Vulnerability or Web Vulnerability.
3. Adding a host vulnerability:
    a) Click and hold to select a Host Vulnerability icon, drag the **Host Vulnerability** icon to the **Target** icon in the topology, then release the mouse button.
    b) Enter information in the text box at the node and click **Save**. Parameter values can be specified for the added vulnerability.
4. Adding a web vulnerability:
    a) Click and hold to select a Web Vulnerability icon, drag the **Web Vulnerability** icon to the **Attack surface of the site** icon in the topology, then release the mouse button.
    b) Enter information in the text box at the node and click **Save**. Parameter values can be specified for the added vulnerability.

5. To delete the added vulnerability, click on to the added vulnerability icon, go to the Node and click on the green "trash can" icon.

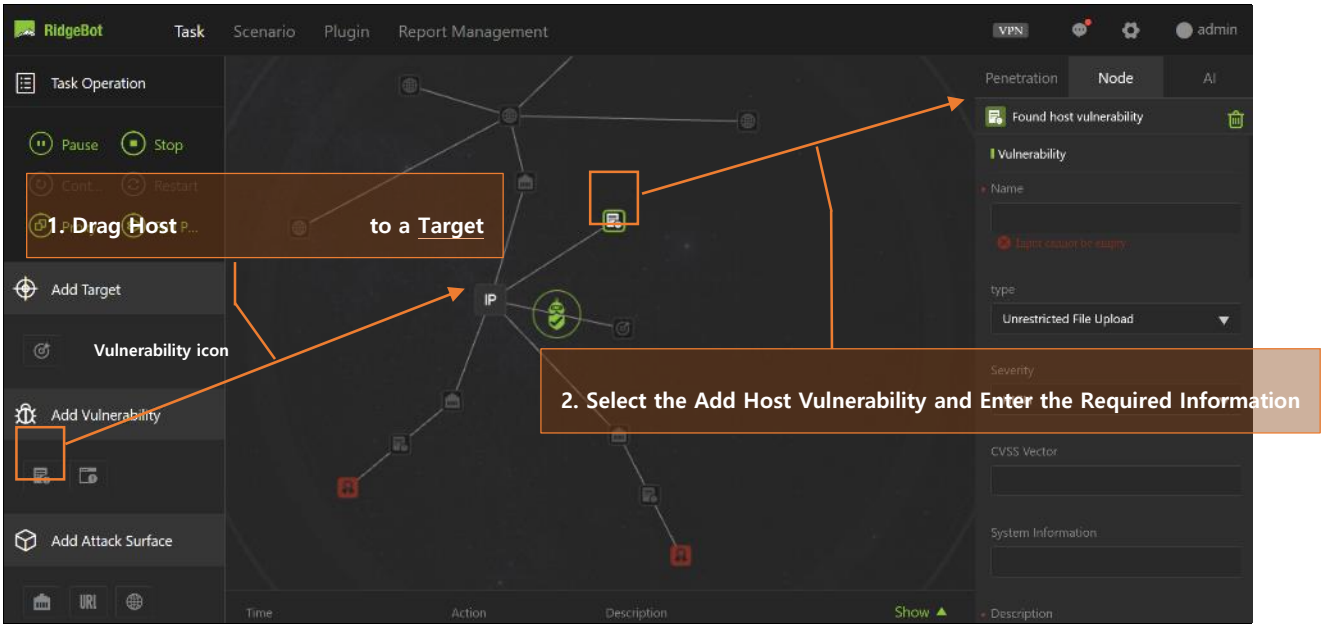


Figure 37: Add a Host Vulnerability to an IP Target

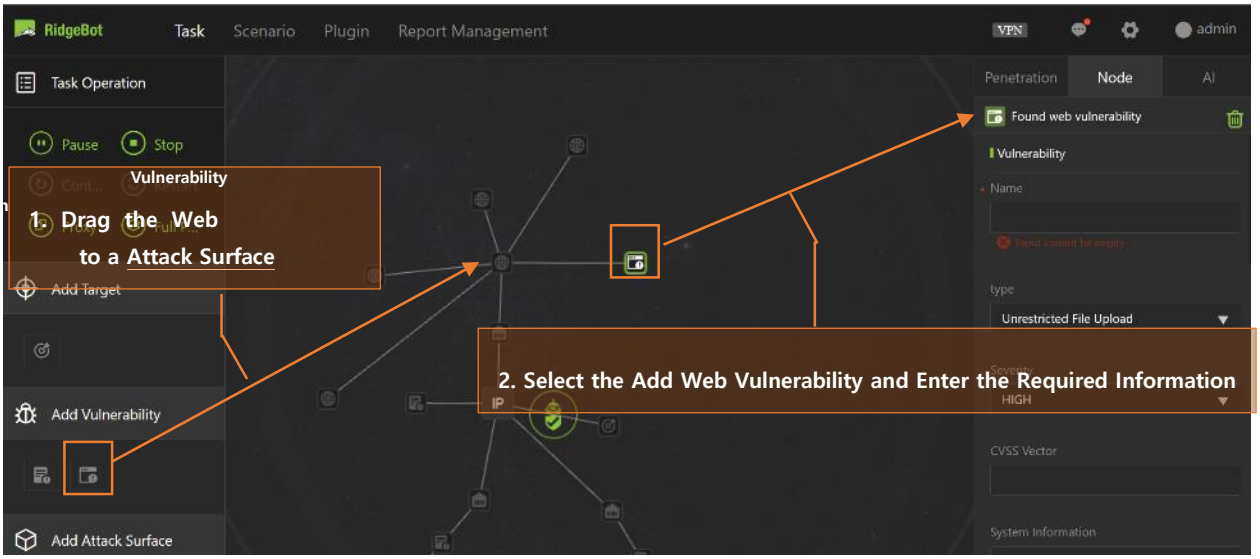


Figure 38: Add a Web Vulnerability to the Attack Surface of a Website

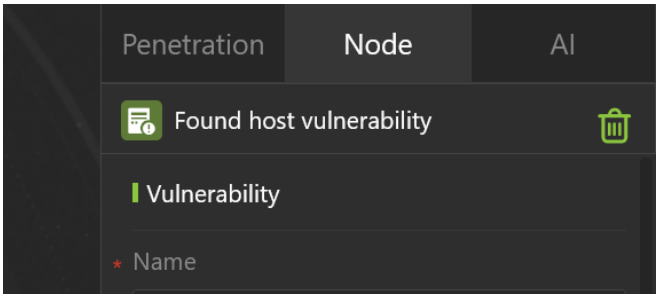


Figure 39: Delete and Added Host Vulnerability

Steps to Add an Attack Surface

Follow these steps to add an attack surface:

1. Ensure the task is running.
2. There are three types of attack surfaces: Port Attack Surface, URL Attack Surface and Site Attack Surface.
    a. A Port Attack Surface or a Site Attack Surface can only be added to a Target.
    b. An URL Attack Surface can be added to a Site Attack Surface.
3. Click and hold to select an Attack Surface icon, drag the **Attack Surface** icon to the **appropriate** icon in the topology, then release the mouse button.
4. Enter information in the text box at the node and click **Save**. Parameter values can be specified for the added vulnerability.

Topology – Attack View

The **Topology View** displays the attack topology with asset information. You can use the following methods to get information on the topology:

- Click on a node in the topology to highlight the corresponding attack path. Mouse over an asset node to the description.

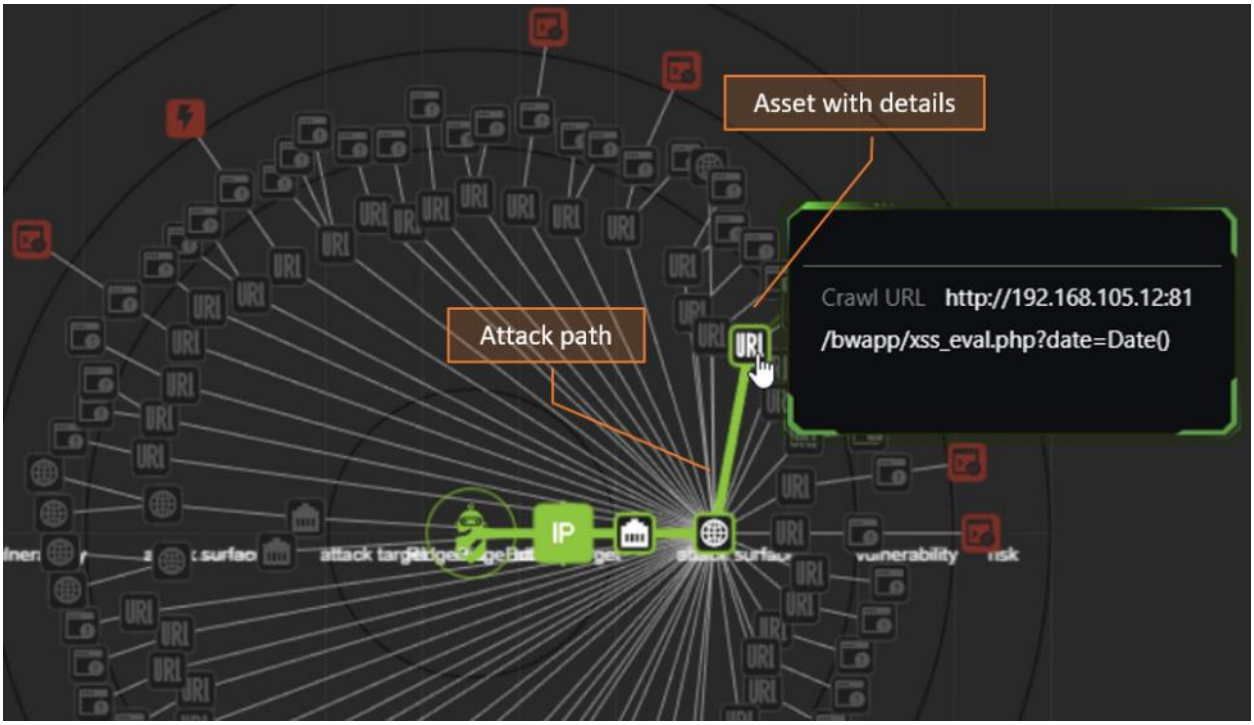


Figure 40: Topology View

- Click on a node in the topology to display its attack information, node information and other related information on the right side of the page.

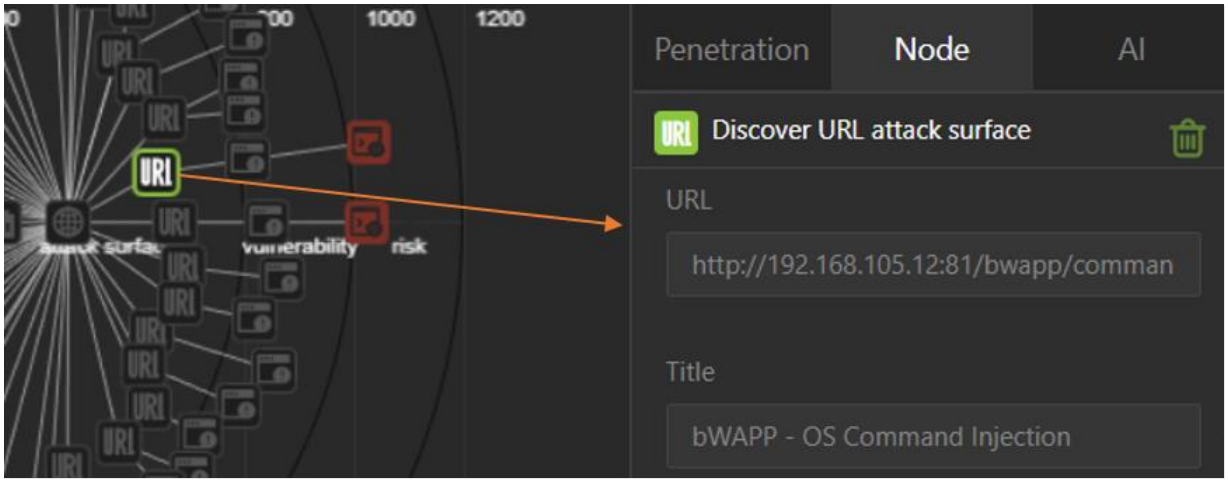


Figure 41: Information of a Selected Asset

Topology – Node View

When a task has Lateral Movement enabled in the Post Exploitation setting, the topology view switches to a node view. The Node view shows the target node-to-node connections and their relationship to RidgeBot. The targets and status are shown when mousing over the target icon.

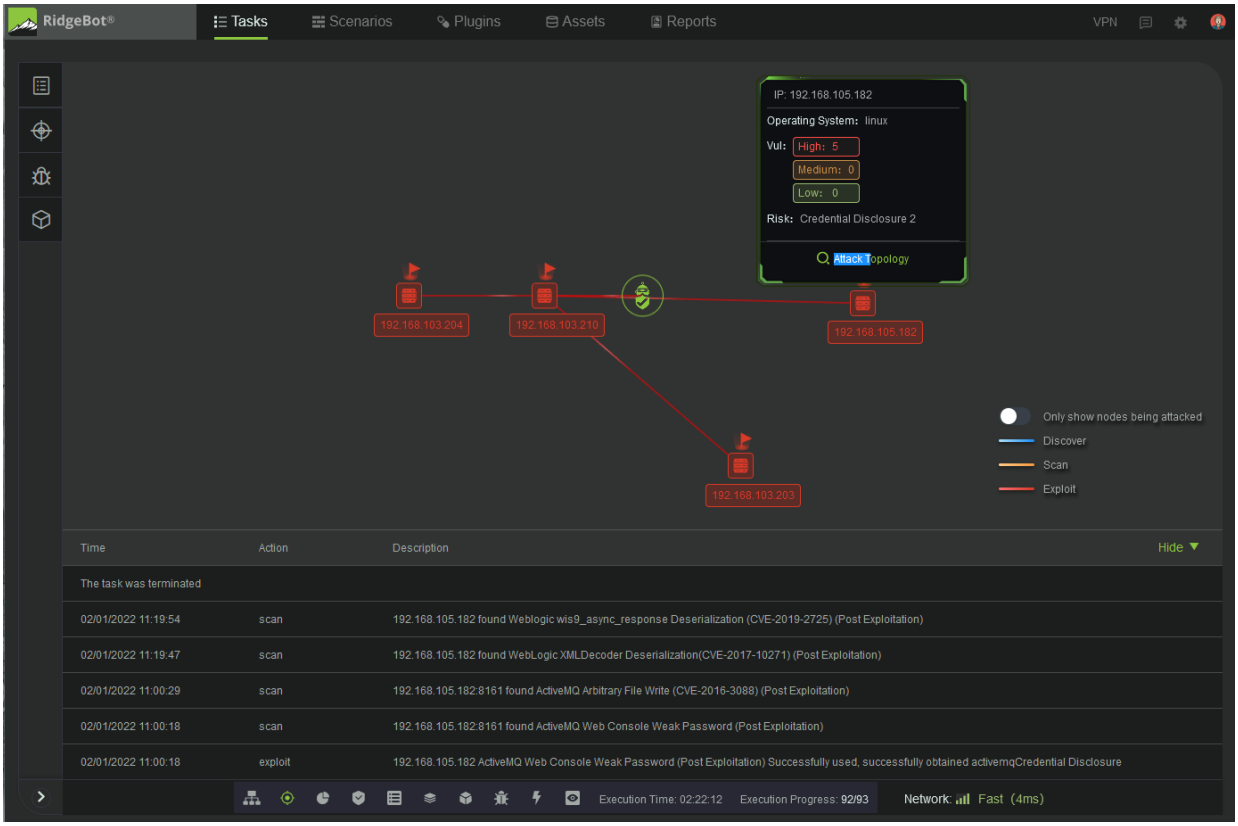


Figure 42: Topology Node View (Post-Exploitation Lateral Movement enabled)

Note: in the Node view, the penetration node menu is not available.

To view the attack topology, click on the Attack topology search icon in the target detail as highlighted. It shows the detail nodes in the attack path from RidgeBot to the specific target. When a node is selected, node information is shown, and the Node menu also provides more detailed information.

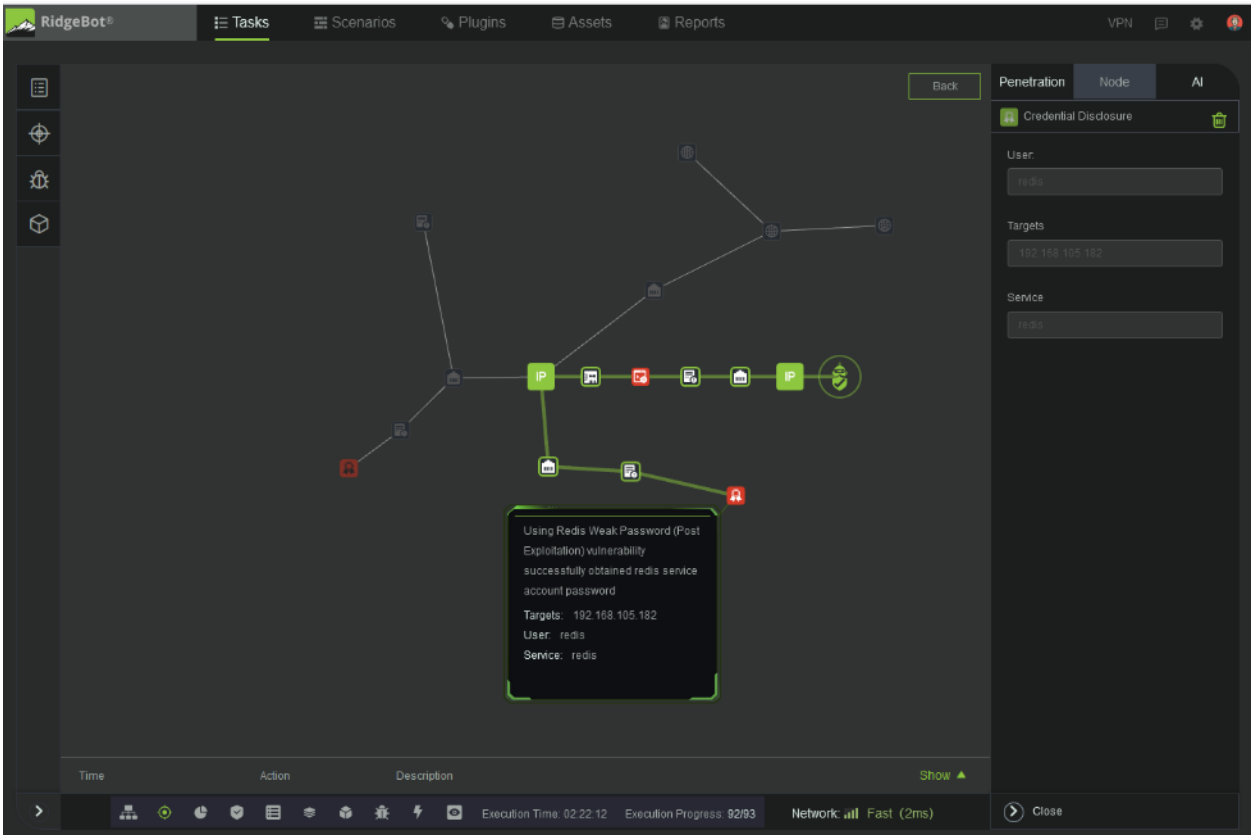


Figure 43: Target Node Details

The Penetration panel shows the list of specific successful exploitations of the targets along an attack path.

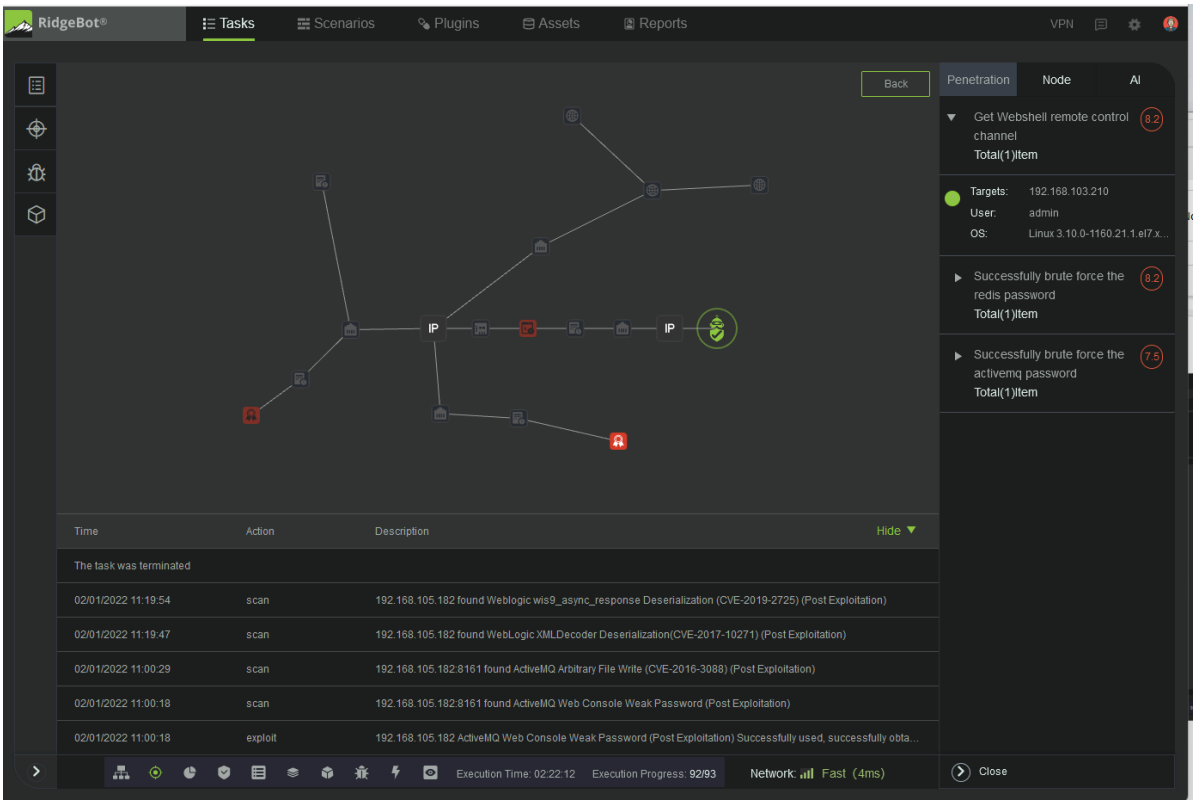


Figure 44: Target Penetration Details

The Attack Kill Chain shows the detailed step-by-step exploitation of the first target and then pivoting to exploit the secondary target in another subnet.

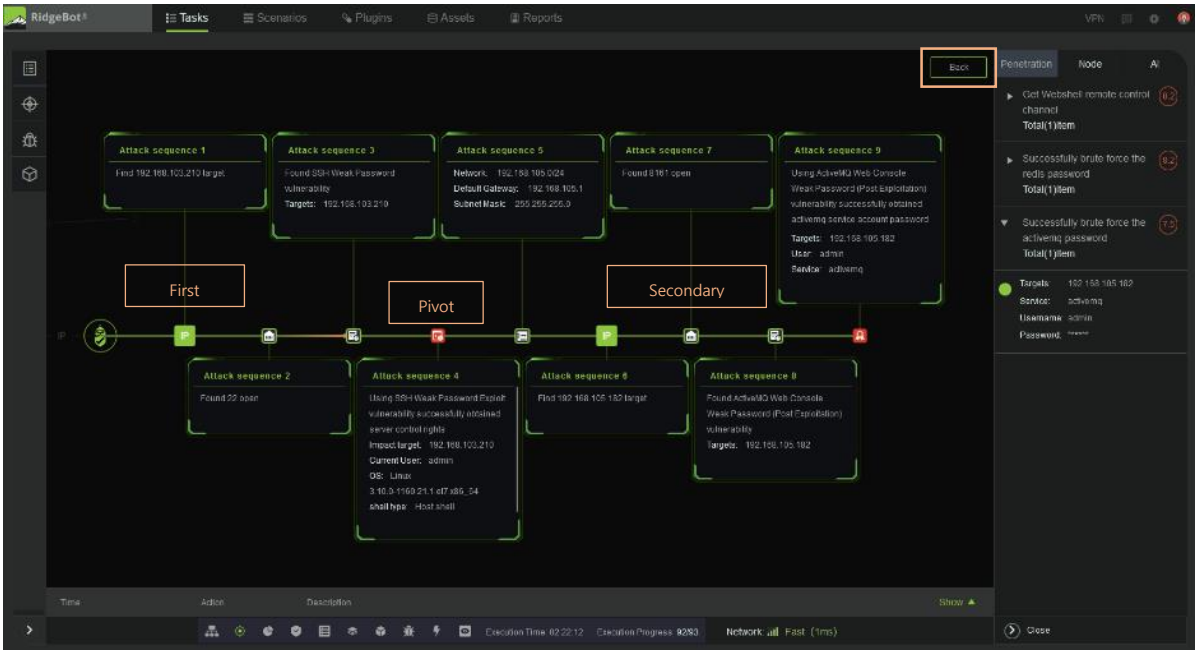


Figure 45: Lateral Movement Kill Chain Details

Clicking on the Back button returns to the top level of the Node view.

The Asset list, Surface Attack list, Vulnerability list and Risk list provide information on all the targets of this Task.

Task Summary

The **Task Summary**  icon on the Task Tab displays a comprehensive view of task execution results. A variety of statistics is collected and calculated, and is displayed in an easy-to-read format.

- **Task Basic Information**: This lists the general information of the current running task.
- **Total Health Score**: This is a security index of all targets in the task. The higher the score, the safer the targets.
- **Action Type**: This shows the distribution of jobs in the task doing discovery, scanning, or exploitation.
- **Task Progress Information**: This shows task execution progress. The number of jobs created refers to the total number of jobs in the current task, while the number of jobs completed refers to the jobs in the current task that have completed.
- **Task Execution Summary**: This lists the assets scanned by the task, giving statistics on nodes where vulnerabilities or risks are detected. In the case of vulnerabilities, RidgeBot list the number of High, Medium, Low, and Information only vulnerabilities according to the industrial stand criteria. In the case of Risks, RidgeBot list the number of Risk types, outlined in the Risk Table Section.

Attack Confirmation

When the task intervention mode in the configuration is set to "user intervention", RidgeBot awaits instruction before executing the impactful plugin shown the list. The task remains in "Pending" status until you confirm or ignore all the plugins.

Click on the  icon on the Task Tab and select the plugin—individually or "all" on the checkbox next to the Plugin Name. In the "Batch" pulldown menu on the right, you can then confirm or ignore the selected plugins.

Once a plugin is confirmed, RidgeBot proceeds with plugin execution. The Task can only finish once all plugins are either confirmed or ignored.

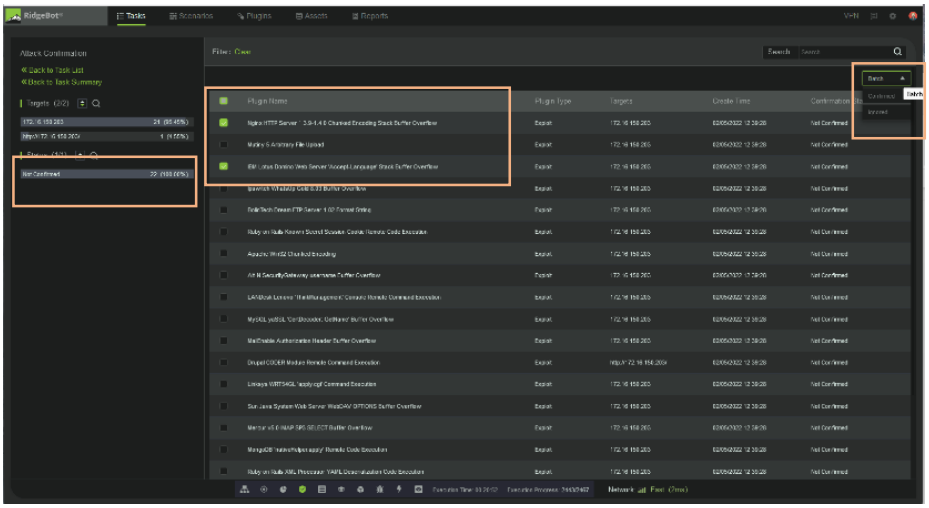


Figure 46: Attack Confirmation Table

Attack Log

Click on the Attack Log  icon on the Task Tab to access a log of the plugin attacks on a target's vulnerability.

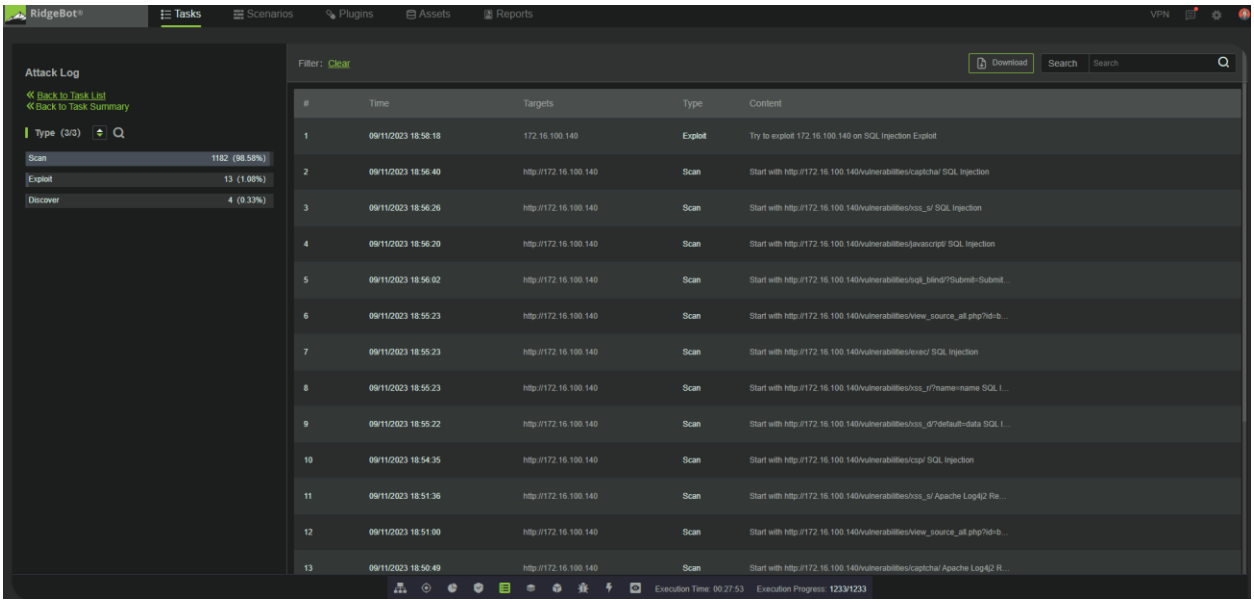


Figure 47: Attack Log Table

Click the "Download" button to download the Attack log in CSV format, named "attacklog.csv", a new feature introduced in V4.2.4.

Asset Table

Click the **Asset Table** icon In the Task Tab see a list of the assets of the targets attacked in the task.

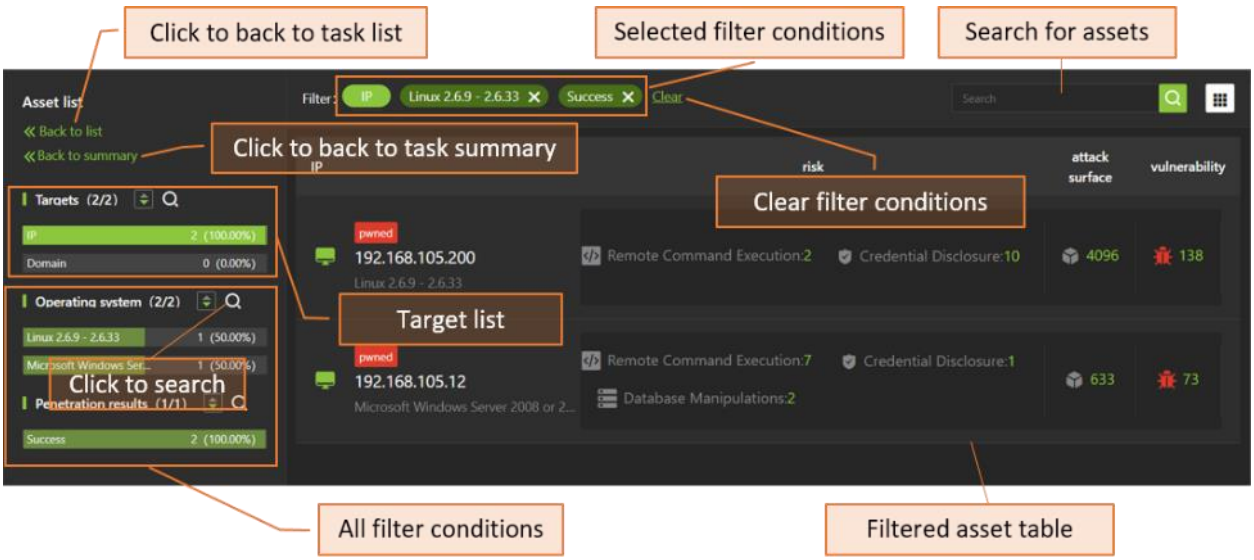


Figure 48: Asset Details Information Page

In the target list (targets are grouped by type), when you select a particular type of target, the corresponding filter conditions are listed below, and the corresponding targets are listed on the right. When you select filter conditions, the filtered assets are listed in the asset table.

Note: The available filter conditions vary based on the target type.

Attack Surface Table

Click on the **Attack Surface Table** icon on the Task Tab to see the attack surface page. Attack surfaces are the points where hacker attacks are performed.

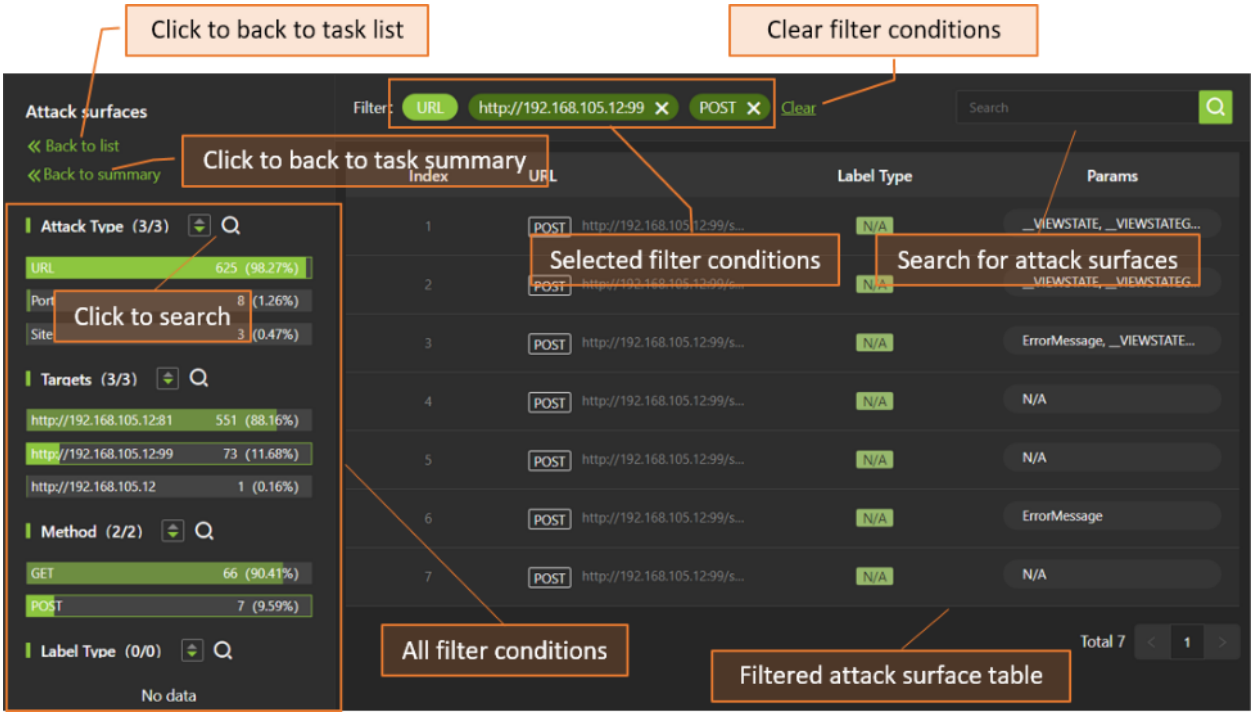


Figure 49: Attack Surface Detail Information Page

When you select an attack type from the attack type list, the corresponding attack surfaces are listed in the table on the right. You can filter the results by selecting targets in the targets list.

> **Note**: The available filter conditions vary based on the attack type.

Vulnerability Table

Click the **Vulnerability Table** icon on the Task Tab to see the vulnerability page. In the vulnerability table, you can click on an entry to see detailed information. You can label and validate the vulnerabilities to reflect your own requirements.

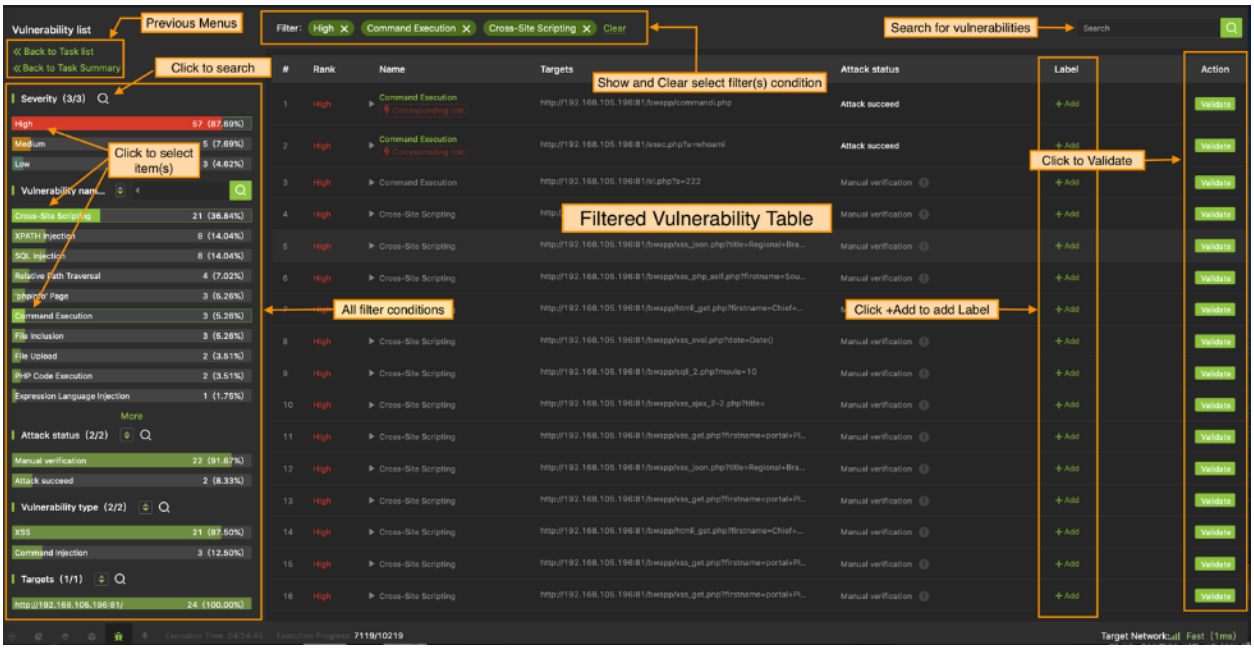


Figure 50: Vulnerability Details Information Page

When you select a severity level from the severity list, the corresponding vulnerabilities are listed on the right. You can filter the results by selecting targets in the targets list. You can filter the results by selecting other conditions listed in the all-filter conditions panel.

In the vulnerability list, you can click the expand icon to see more details.

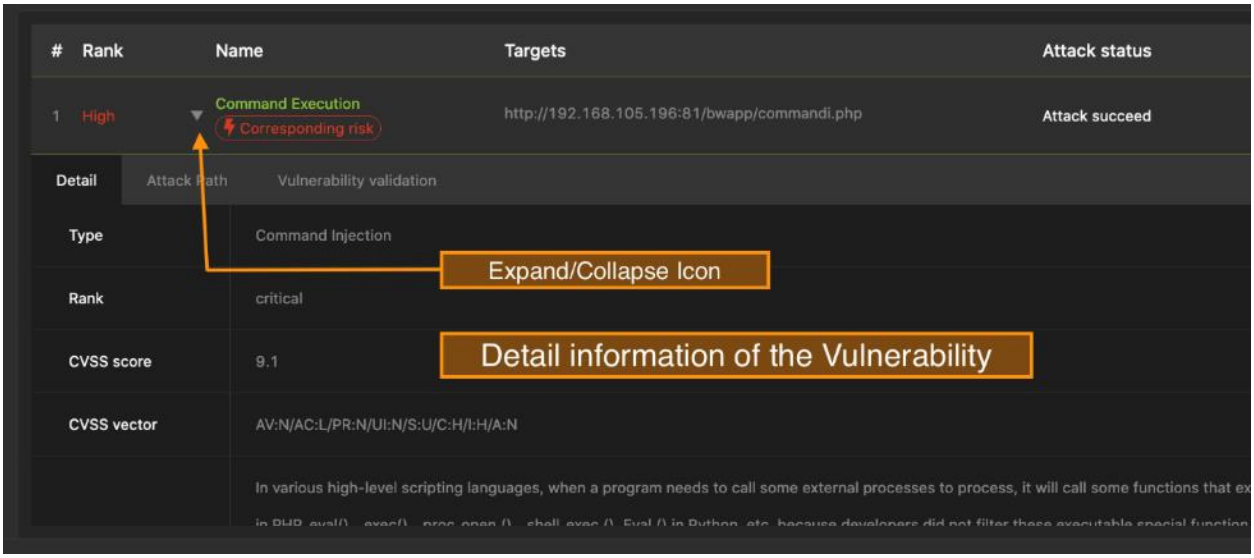
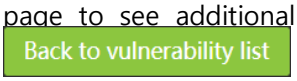


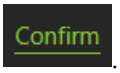
Figure 51: Vulnerability Details

In the vulnerability list, click on the **Corresponding risk** link 

to go to the risk page to see additional details. On the risk page, click on the **Back to vulnerability list** button 

at the upper right corner to go back.

To label a vulnerability, click 

in the **Label** column of the vulnerability table, then select the elements you want from the pop-up menu, and click 

.

Figure 52: Labeling a Vulnerability

To validate a vulnerability, click the 

button in the **Action** column of the vulnerability table, and then click the Validate button under the **Vulnerability validation** tab.

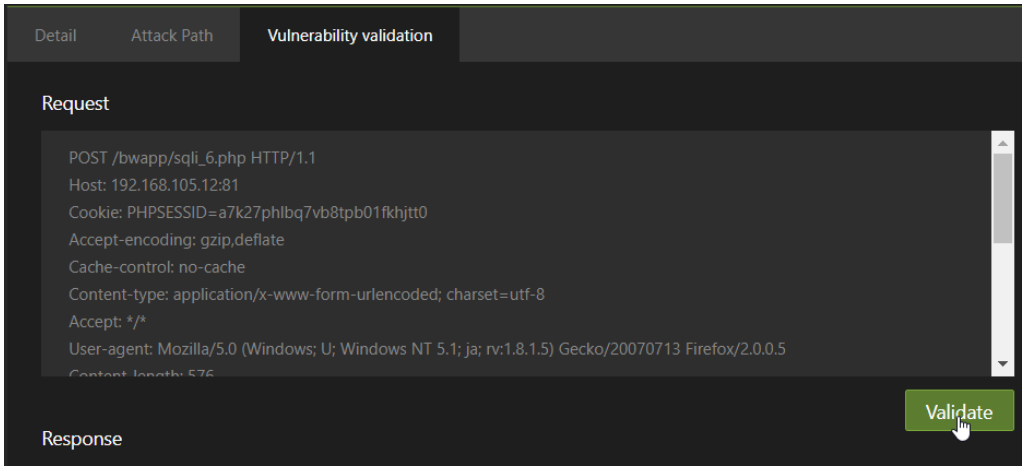
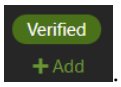


Figure 53: Validating a Vulnerability

The validated vulnerability is now labeled as Verified in the **Label** column 

.

Notes:

- The Vulnerability Validate action is only applicable to HTTP queries. Otherwise, you will get an error message such as "Failed to send request".
- The available filter conditions vary based on the severity selected.

Risk Table

Click the **Risk Table** icon on the Task tab to see the risk page.

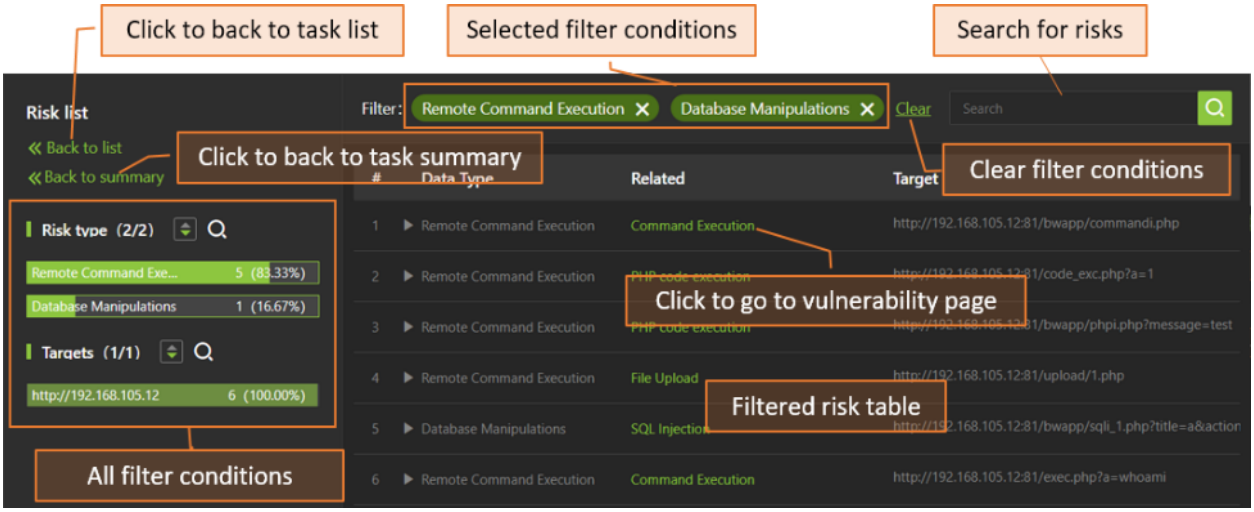


Figure 54: Risk Details

For RidgeBot, we label vulnerabilities as "Risks" when RidgeBot can exploit the test target and achieve one of the following four outcomes, and we can subsequently provide evidence of such an exploit to the customer:

- **Database Manipulation**
- **RCE (Remote Command Execution)**
- **Credential Disclosure**
- **Sensitive Information Leakage.**

While a significant number of vulnerabilities exist, only a small percentage can be exploited, and an even smaller percentage can be exploited from the network side, which is how RidgeBot operates. However, the vulnerabilities that can be exploited in this manner are typically the most critical and should be treated as top priority by customers, especially if RidgeBot identifies them as posing one of the aforementioned risks.

Some vulnerabilities, despite being potentially critical, might not be categorized as "Risks" by RidgeBot. This could be due to various reasons, such as the need for human intervention or a complex setup. Even if RidgeBot doesn't categorize them as risks, it will still mark their severity based on industry standards. Additionally, RidgeBot will provide detailed information, such as the payload sent to the test targets and the responses received. This information can aid customers in manually validating the vulnerabilities and implementing possible patches to mitigate them.

When you select a risk type from the list, the corresponding risks are listed on the right. You can filter the results by selecting other conditions listed in the all-filter conditions panel.

In the risk list, you can click the expand icon  to see more details. And click the collapse icon  to close the detail information table.

In the risk list, you can click on the vulnerability name (in green) to go to the vulnerability page for additional details; once there you can click the **Back to risk list** button 

at the upper right to return to the risk display.

Report Preview

Click the **Report Preview**  icon on the Task Tab to see the report preview page. For a task that is still running, the page shows a preview of tasks results up to the current time. For more information on report format and content, see Chapter 6 Reports and Report Management.

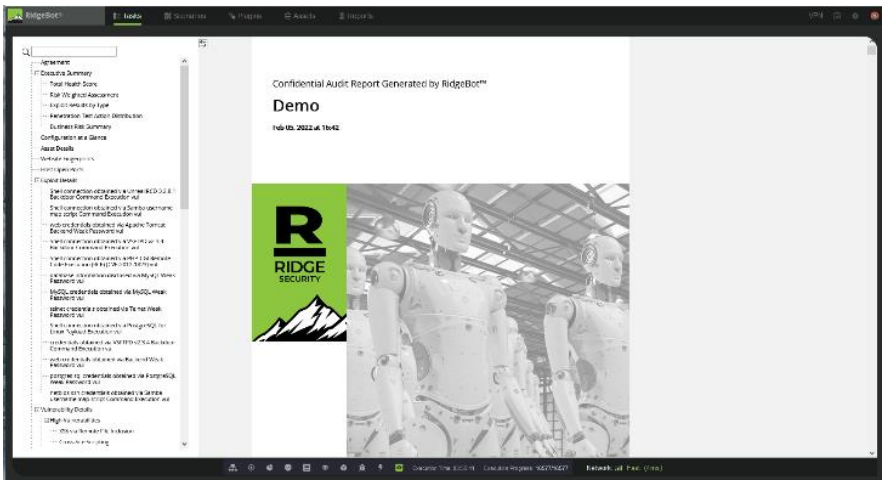


Figure 55: Report Preview

Operating on an Attack Simulation Task

To operate on an attack simulation task, click on "Tasks" in the Navigation Bar, and then on "Attack Simulation Tasks" underneath it. This shows a list of all attack simulation tasks defined in the system.

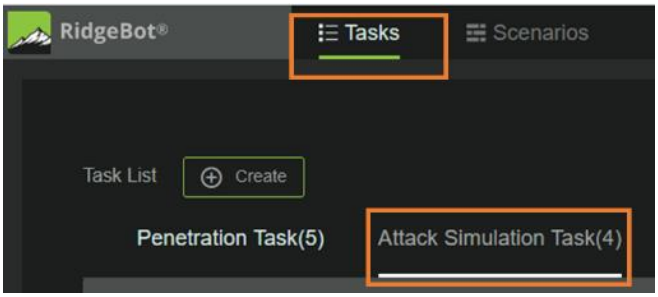


Figure 56: Viewing the Attack Simulation Task List

Viewing an Attack Simulation Task

An attack simulation task is generally run repeatedly (daily or weekly) to provide you with the latest ongoing results on your security posture. If you click on the name of an attack simulation task, a summary of the most recent runs of the task is displayed at the top of the page, and if you scroll to the bottom of the page, you can see more details about the scenario, targets and resulting block rates of the various scripts.

Attack Simulation tasks require an agent (a Botlet) to be installed and running on the target. For more information, see Chapter 3 Installing a Botlet.

Security Posture Trend

The top of the page displayed when you click on an attack simulation task name shows a series of one or more candles drawn against a percentage scale. These candles represent the block rates resulting from the test runs, and the date and time of each test run is shown below the candle. The series of candles provide an easy visual of the trend of your security posture over time as the same task is run repeatedly.

The height of the candle—a percentage—tells you how many of the RidgeBot attacks launched during the run were successfully blocked by the target machine. Thus, the higher the candle, the safer the target machine. The example below shows a target machine that has a very poor block rate of about 9%, which means 91% of attacks against this system were successful.

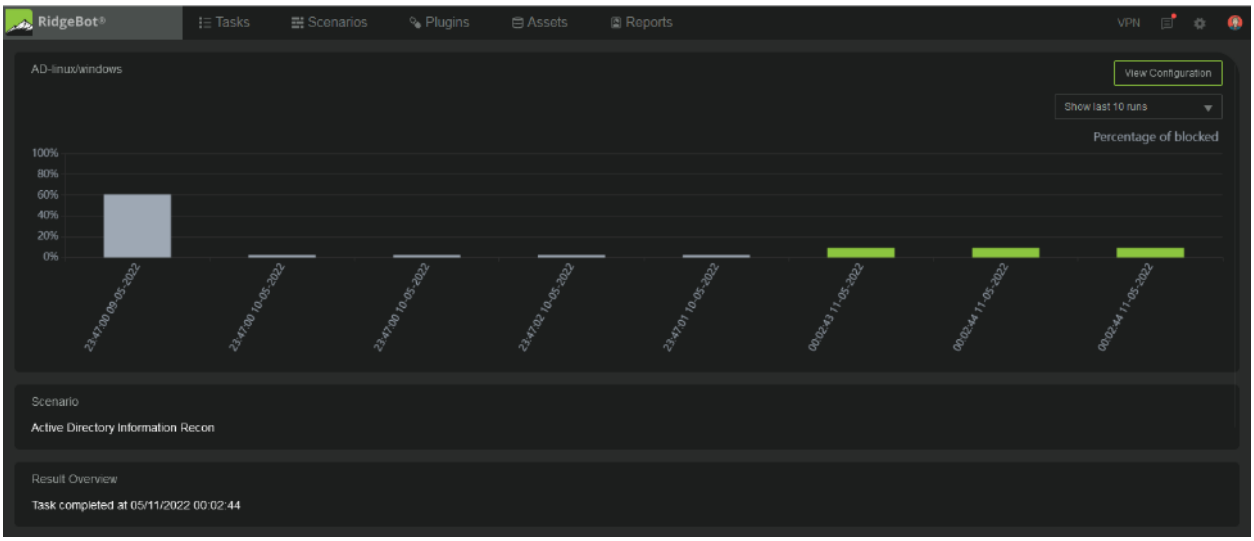


Figure 57: Trend Display of the Most Recent Runs of an Attack Simulation Task (top of screen)

Other information available on this screen includes:

- **View Configuration**: If you click this button (top right of the screen), you can easily access the configuration of the task.
- **Show Recent Runs**: By default, the display shows the results of the last 10 runs of this task, or it shows all the runs available (if less than 10 runs have been executed). You can click the button to select only the last 5, or to show all available. These choices illuminate the trend of the security posture of the target.
- **Scenario**: The scenario on which this task is based.
- **Completion time**: The timestamp when the most recent run of this task completed.

Block Rate Results

The bottom of the page displayed when you click on an attack simulation task name shows various views of the block rate of the attacks launched by the task.

Figure 58: Block Rate Details Display for an Attack Simulation Task (bottom of the screen)

- **Result Overview by Botlet**: The top left display shows the block rate of attacks per target machine (per Botlet). In the example shown above the target on the left is extremely vulnerable with a 0% block rate, while the target on the right is moderately safe with a 66.7% block rate.
- **Result Overview by Threat Group**: The top right display shows the block rate per threat group. The green bar represents the number of attack scripts blocked, while the red bar represents the attack scripts that penetrated the target.
- **Result Overview by Tactic**: The bottom left display shows the block rate per attack tactic. The green in the bars represent the number of attack scripts blocked, while the red bars represent the attack scripts that penetrated the target. The tactics refer to Mitre Att@ck Tactics.
- **Result Overview by Technique**: The bottom right display shows the block rate per attack technique. The green in the bars represent the number of attack scripts blocked, while the red bars represent the attack scripts that penetrated the target. The techniques refer to Mitre Att@ck Techniques.
- **Overall**: A summary of attack targets, scripts and results is given across the very bottom of the screen. In the example shown above, there are:

- 2 targets.
- 76 total scripts.
- 4 blocked scripts. If you click on the arrow next to the number, a list of successfully blocked scripts is displayed.
- 40 not blocked scripts. If you click on the arrow next to the number, a list of scripts that were **not** successfully blocked is displayed.
- 32 scripts that were not applicable to the chosen targets, perhaps due to the operating system present on the target machine. If you click on the arrow next to the number, a list of scripts is displayed.
- 9.1% calculated overall block rate. This is figure is derived by 76 – 32 = 44 applicable scripts. 4 / 44 = 0.091 of the scripts were successfully blocked, giving an overall block rate of 9.1%.

In any of the lists of scripts (blocked, not blocked, not applicable), you can click anywhere in the script entry and get additional details.

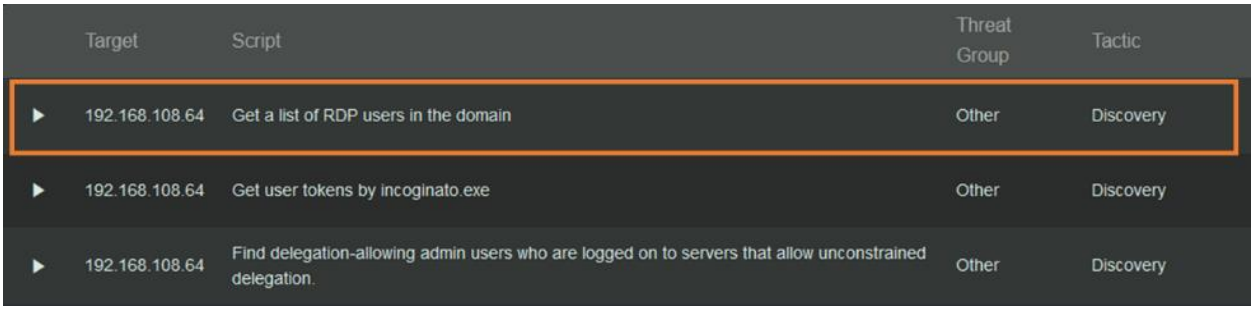


Figure 59: Click on a Script in a List

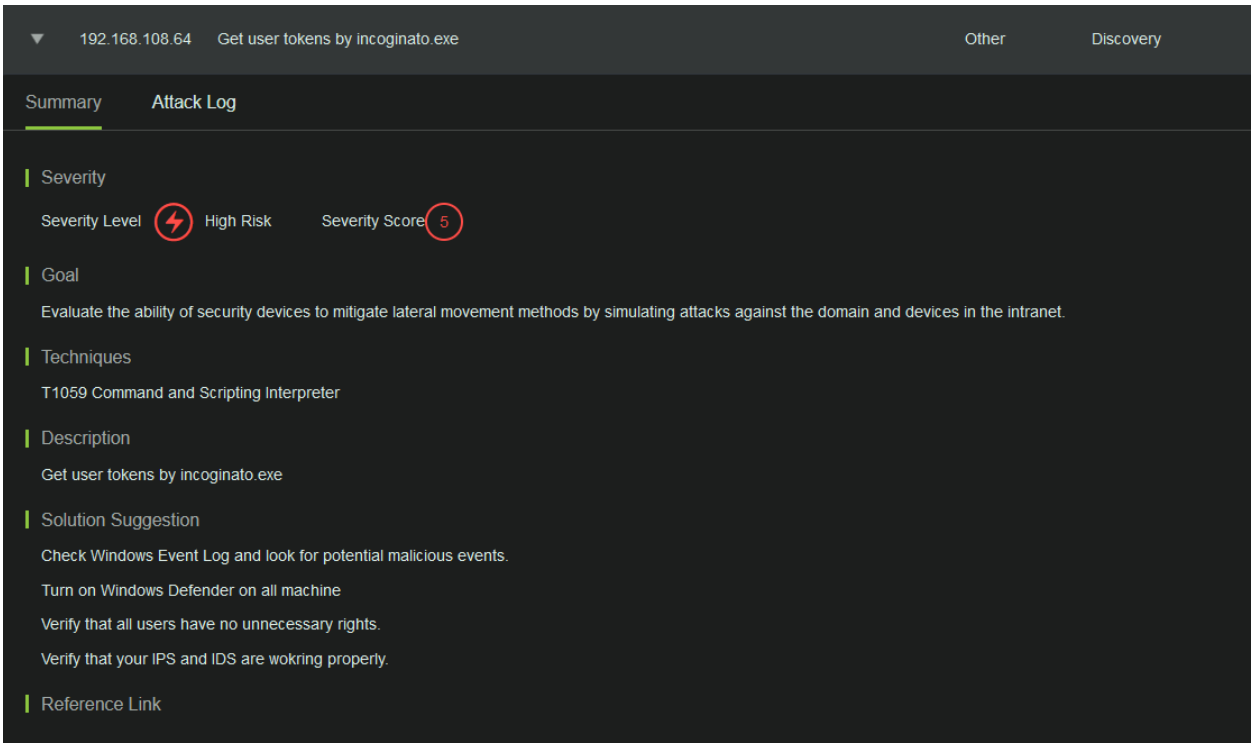


Figure 60: Script Details Display

Chapter 4 Scenarios

Scenarios contain the basic settings for a penetration or attack simulation test to be performed by RidgeBot. A task is built on a scenario. Two kinds of scenarios are provided:

- **System Scenario**: Provides several commonly used scenarios to simplify initial user configurations.
- **Custom Scenario**: Defines user-customized values for the basic setting options and saves it as a new scenario template to be used later during task definition.

This chapter discusses scenario configuration, and has the following sections:

Note: While several different pre-defined scenarios are provided, the options in the customized scenarios are the same as in the pre-defined scenarios. Only the values chosen for the options may differ. The option descriptions are therefore listed only once in the Configuring a Custom Scenario section of the document.

Introducing System Scenarios

A System Scenario has a set of pre-defined settings to do different Penetration or Attack Simulation testing. Each scenario defines the settings and plugins for a task based on that scenario. There are eight pre-defined scenarios included in the System. You can select any of these scenarios if it meets your Penetration Testing requirements. And if it doesn't, you can build a custom scenario based on the pre-defined scenario.

On the **Navigation Bar**, click **Scenario** to display the scenario page. As of version 4.0, the **System Scenario** tab shows all the Penetration Test and Attack Simulation Test system scenarios given in the tables below. As of version 3.9, a scenario includes the scan type in its configuration and cannot be

modified. A scenario also sets the configuration and license requirements to run each task. In version 4.1.1, a new intranet ransomware scenario is introduced and a new intranet penetration scenario which is a combination of the Full Penetration and Intranet Penetration in the earlier release. See system scenario table below for description and the license requirement for each scenario.

System Scenario Table for Penetration Tests

Scenario	Scenario Description	Scan Type	Required License	Task Recon Configuration
Attack Surface Identification	This scenario launches asset profiling to identify the target machine's OS type, open ports, active services as well as websites' domain names/sub-domain names, encryption key information, web frameworks and external URL/URI exposures.	Host	Required a valid license on RidgeBot. ***Does not required IP license to run this task**	Service Detection
Website Penetration	This test launches cyber-attacks against target websites, web applications and all the related attack surfaces. The attack targets include self-developed or CMS based websites.	Website and Web application	Web	Crawler Configuration
Host Penetration	This scenario uses port scanning to profile targets' attack surface exposures and utilizes various network attack techniques to discover vulnerabilities and exploit risks of the targets.	Host	IP	Service Detection

Intranet Penetration (IP + Default Crawler)	This scenario uses port scanning and default web crawler to profile targets' attack surface exposures and utilizes various network attack techniques to discover vulnerabilities and exploit risks of the targets. If user needs to customize web crawler or want to use crawler+proxy mode to bypass website login, please select web related scenarios for the task.	Host and Host management Interface only	IP	Service Detection
Weak Credential Exploit	This test launches cyber attacks based on the sensitive information collected via weak credentials or unauthorized access exploits. Attack targets include but not limited to various application logins, web logins, Redis, Elasticsearch, ActiveMQ, Database etc.	Host	IP	Service Detection
3rd Party Framework Penetration Testing	This test launches cyber attacks against commonly used 3rd party framework such as Struts 2, Spring, Fastjson, ThinkPHP and many others.	Web application	Web	Crawler Configuration
Ransomware Penetration	This test utilizes various techniques frequently used by APT groups to perform ransomware attacks such as server remote command execution (RCE) attack, windows remote desktop protocol (RDP), brute-force attack and etc.	Host and Web application	IP and Web	Service Detection
Intranet Ransomware Penetration	This test utilizes various techniques frequently used by APT groups to perform ransomware attacks such as windows remote desktop protocol (RDP), windows	Host and Host management interface	IP	Service Detection

	remote command execution (RCE) attack, weak password brute-force attack and etc.			
3rd Party Scanning Result Validation	This test allows RidgeBot user to upload a 3rd party vulnerability test report, then launch a full penetration task to validate its result	Host and Web application	IP and Web	Service Detection

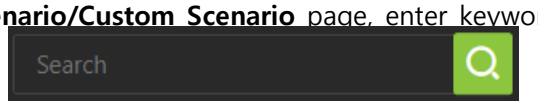
Table 3: Penetration Tests Pre-Defined System Scenarios

System Scenario Table for Attack Simulation Tests

Scenario	Scenario Description
Endpoint Security	In this scenario, the RidgeBot Botlet simulates the behavior of malicious software, or it downloads malware signatures to validate the security controls of the target endpoints. A test result with a higher block rate indicates a safer endpoint.
Data Exfiltration	In this scenario, the RidgeBot Botlet simulates unauthorized movement of data from a server. A test result with a higher block rate indicates attack methods for data theft can be detected and prevented.
Active Directory Information Recon	In this scenario, the RidgeBot Botlet simulates an attacker to gather useful resources in Windows Active Directory for elevated privilege, persist, and plundering information. A test result with higher block rate indicates the Windows AD server gets better protection in place.

Table 4: Attack Simulation Pre-Defined System Scenarios

If you mouse over any scenario, the full description is displayed. You can choose the appropriate scenario for each of your tasks.

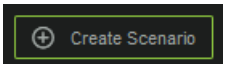
RidgeBot also provides a search function to find a scenario quickly. To search for a scenario, on the **System Scenario/Custom Scenario** page, enter keywords in the search text box, and then click the search icon. 

Configuring a Custom Scenario

The pre-defined system scenarios can be used directly to define tasks. If you have any specific requirements for your environment, you can define a custom scenario to make subsequent task creation based on the scenario more convenient.

Penetration Test Custom Scenario

To create a customized Penetration Test scenario, follow these steps:

1. On the **Navigation Bar**, click **Scenario** to display the Scenarios page. Next to the "Scenario Center", click on the **"Create Scenario"** 

icon. A page appears with the scenarios listed as templates. Choose the appropriate Penetration Test template (green diagonal in top-left corner) to start.

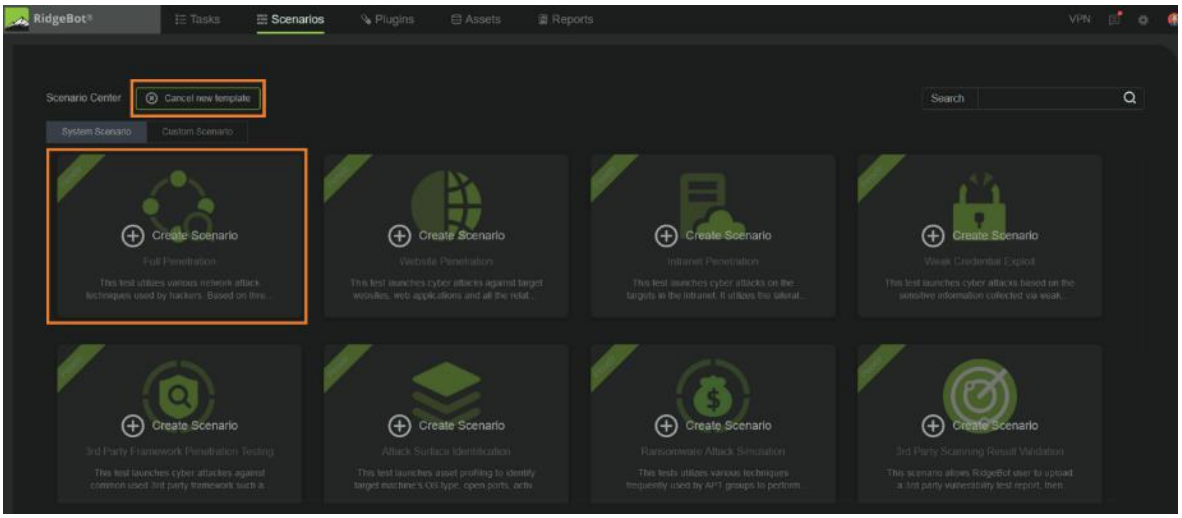


Figure 61: Select a Penetration Test Template for a Custom Scenario

2. When the custom template is displayed, follow the vertical sidebar workflow to create a custom scenario.
3. In the **Basic Configuration**, specify values for the basic options for the task.

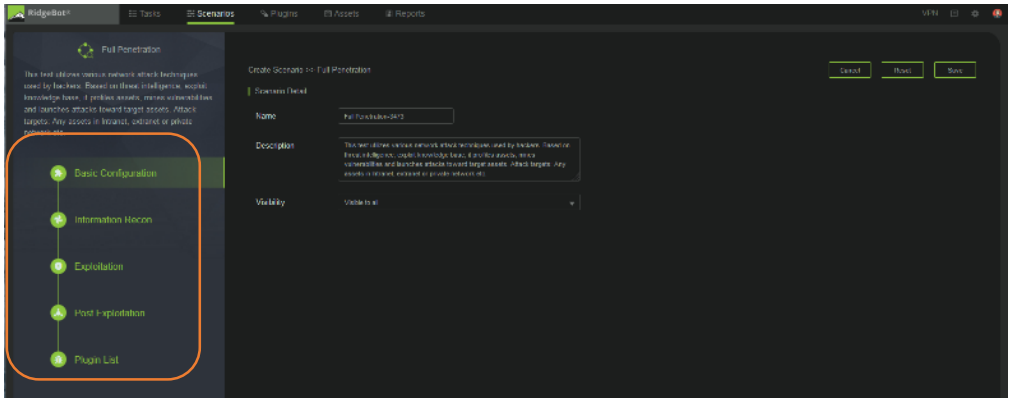


Figure 62: Creating a Custom Scenario: Basic Configuration

- **Name**: The name of the scenario. This is a mandatory field.
- **Description**: The description of the scenario. This is an optional field.
- **Visibility**: This assigns a user privilege level to the scenario. By default, the scenario is visible to all users, or you can choose to make it visible only to yourself.

4. Click **Information Recon** on the vertical sidebar menu. This page specifies the Service Detect configuration or the Crawler configuration to be used to attack targets. You can mouse over the question mark icon following each option to view help.

    1. **Service Detect**: On this page, you configure the network connection timeouts and retries. Configure the values of HTTP header fields (cookies should be set here); specify the port scan mode for open port detection and port range; specify the max concurrent connection number; and select the flow control mode. The flow control specified here can be used to enable rate limiting on network interfaces.

or

    2. **Crawler Configuration**: The Crawler Mode default is "Intelligent". Other options include static or dynamic. Intelligent mode allows the crawler to select Static or Dynamic based on the webpage. Static mode is applicable to a static webpage. A Dynamic crawler is typically applicable to a website using dynamic update webpages such as Single Page Application (SPA).

    See Chapter 3 Configuring a Penetration Task for a more detailed description of crawler parameters.

5. Click **Exploitation** on the vertical sidebar menu. This page sets the default for the Exploitation policy. The default setting is recommended.

6. Click **Post Exploitation** on the vertical sidebar menu. This page is available for Host-based scenario templates. The default setting is recommended.
7. Click **Plugin List** on the vertical sidebar menu. The RidgeBot system embeds a wealth of vulnerability scanning plugins for different assets and vulnerabilities. Once the plugins are selected and enabled, the system automatically scans and detects vulnerabilities and subsequent attacks to identify the risks.
8. After completing the above steps, click the **Save** button. The custom scenario is now listed in the **Custom Scenario** tab.

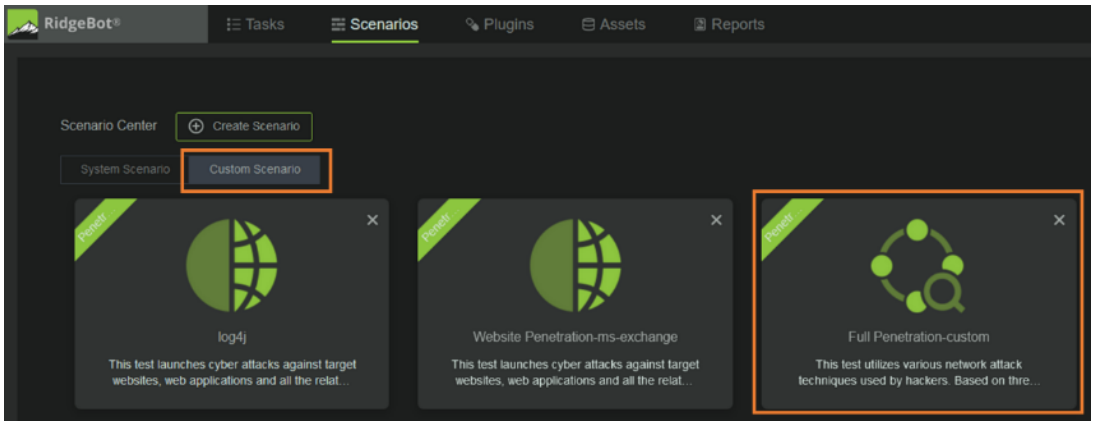


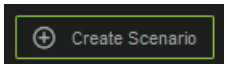
Figure 63: Custom Scenario List

At any step, you can click the **Reset** button to restore the original values from the scenario template, allowing you to reconfigure the options.

At any step, you can click the **Cancel** button to return to the **System Scenario** page, abandoning any unsaved changes.

Attack Simulation Test Custom Scenario

To create a customized Attack Simulation scenario, follow these steps:

1. On the **Navigation Bar**, click **Scenario** to display the Scenarios page. Next to the "Scenario Center", click on the **"Create Scenario"** 

icon. A page appears with the scenarios listed as templates. Choose the appropriate Attack Scenario Test template (orange diagonal in top-left corner) to start.

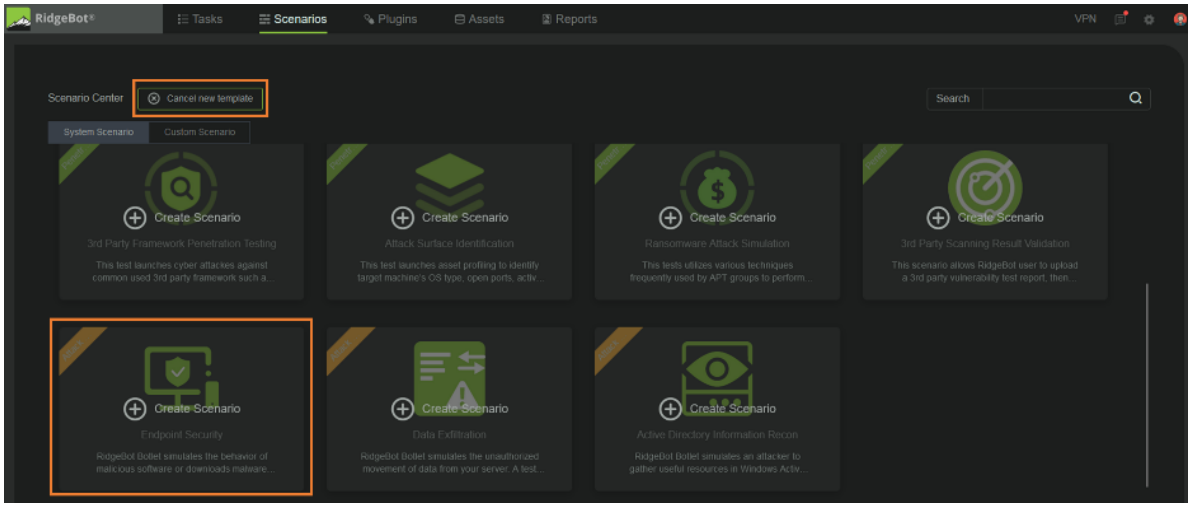


Figure 64: Select an Attack Simulation Template for a Custom Scenario

2. When the custom template is displayed, click **Script Configuration** on the vertical sidebar workflow to create a custom scenario, then specify values for the options of the scenario.

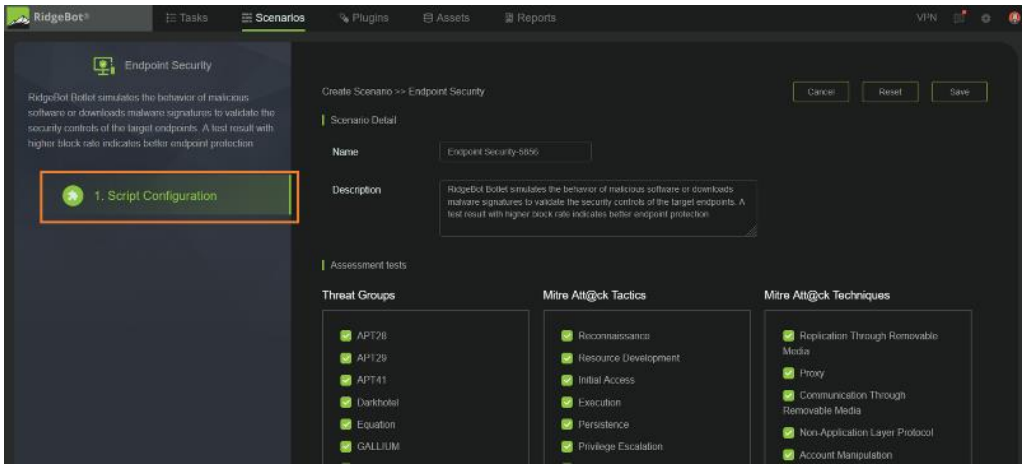


Figure 65: Script Configuration

- **Name**: The name of the scenario. This is a mandatory field.
- **Description**: The description of the scenario. This is an optional field.

3. Under the **Assessment Tests** section, you can choose the applicable tests that you want to employ in your custom scenario from three categories: Threat Groups, Attack Tactics and Attack Techniques. The choices shown on the page depends on the scenario template you chose. By default, all available choices are selected, and you can deselect any that you do not want RidgeBot to use.

4. After completing the above steps, click the **Save** button. The custom scenario is now listed in the **Custom Scenario** tab.

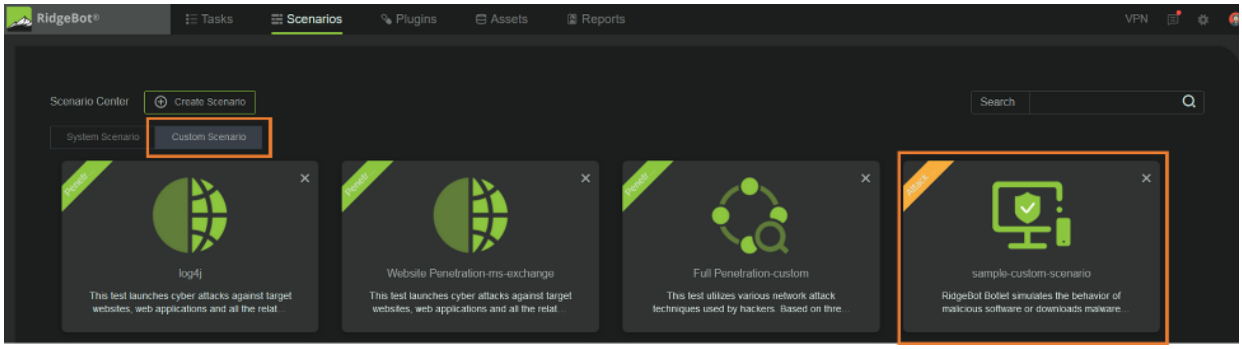


Figure 66: Custom Scenario List

At any step, you can click the **Reset** button to restore the original values from the scenario template, allowing you to reconfigure the options.

At any step, you can click the **Cancel** button to return to the **System Scenario** page, abandoning any unsaved changes.

Modifying and Deleting a Custom Scenario

To modify a customized scenario, follow these steps:

1. Under the **Custom Scenario** tab, click the scenario you want to modify.
2. Edit the option values on each page.
3. Click the **Save** button.

To delete a customized scenario, under the **Custom Scenario** tab, click the delete icon (X) of the scenario you want to delete, as shown in the figure below.

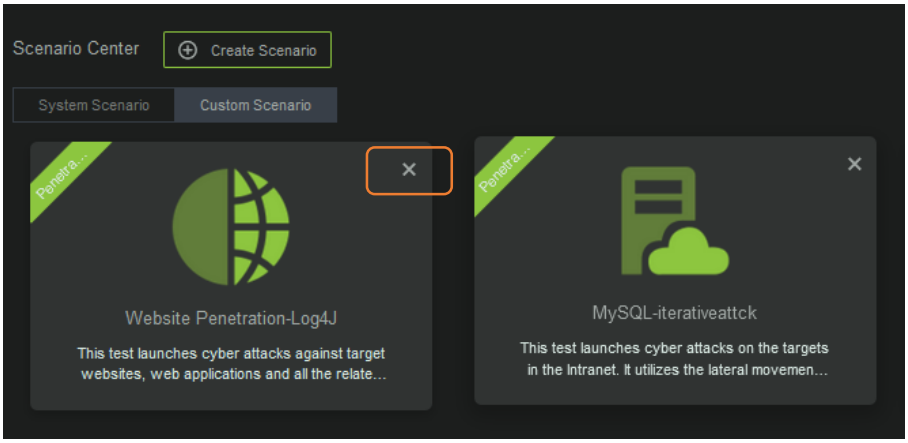


Figure 67: Deleting a Customized Scenario

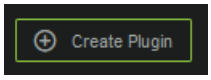
Chapter 5 Customized Plugins

With RidgeBot, you can create your own plugins. This allows you to create your own Web POC (Proof of Concept) program to detect/exploit specific vulnerabilities of interest to you.

This chapter discusses how to create, manage and use customized plugins, and has the following sections:

Creating a Customized Plugin

To create a customized plugin, follow these steps:

1. On the **Navigation Bar**, click **Plugins** to see the Plugins page. Click the **Create Plugin** button 

at the upper left corner to see the **Plugin submit** page.
2. In the **Vulnerability** section, specify values for the vulnerability related options. The vulnerability information described here is displayed in the vulnerability table and report.
3. In the **Fingerprint** section, specify values for the fingerprint related options. The fingerprint options tell RidgeBot when the plugin should be operated.
4. In the **Editing Rule** section, you can create rules and their corresponding responses. RidgeBot uses the rules to create the payload and to check the corresponding response.

Before configuring a rule, it is important to understand the relationship between the rule elements, as illustrated in the graphic below. A rule contains requests and matching conditions. The types of the matching conditions include a status code, a response header and a response body. Requests are evaluated by the operators "!", "&&" and "||" as well as by the matching conditions. The matching conditions help RidgeBot to determine whether or not the vulnerability is detected.

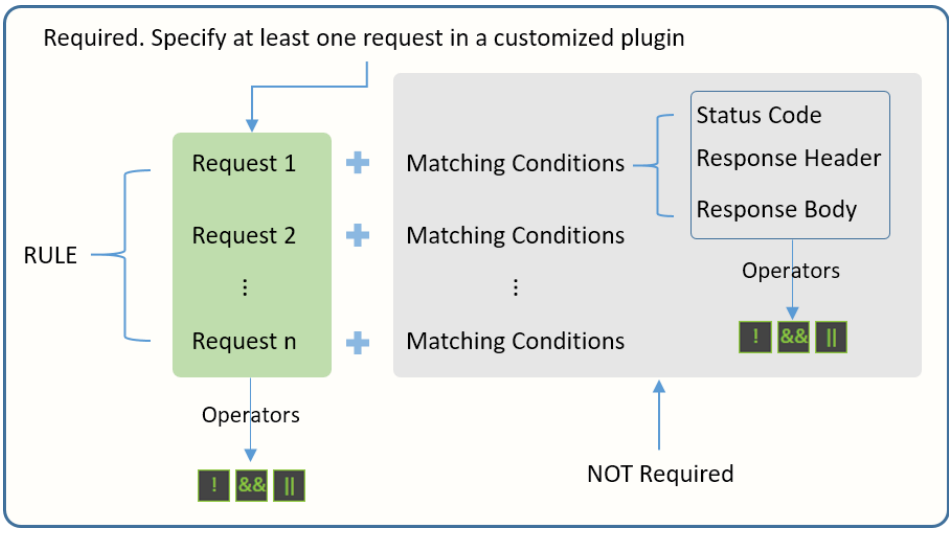
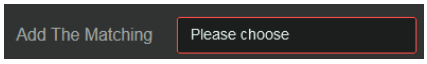


Figure 68: Relationship of Rule Elements

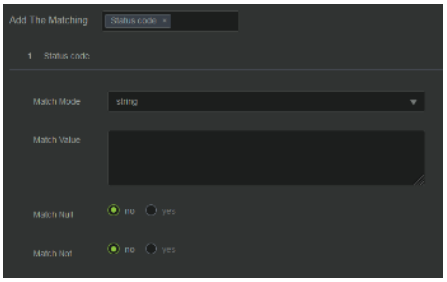
Follow these steps to create rules:

a) Mouse over the plus icon and choose number 1 from the pop-up menu  . "1 Request" area appears.

b) Specify values in the request area.

c) If matching conditions are needed, click on **Please choose** 

and then select the desired type of condition and provide values for the options.



d) If more than one matching condition is added, in the Match expression section, specify the evaluation method for the conditions.

e) Repeat the above steps to add more requests.

f) If more than one request is specified, at the top of the **Editing rule** section, specify the evaluation method for the requests.

To specify an evaluation method, mouse over the plus icon, 

then select the desired operator.

To delete a request, at the top line of the **Editing rule** section, mouse over the request number to be deleted, and then click the X icon. 

5. Click the **Submit** button at the upper right corner to save your configuration.

The configured customized plugin is now listed on the Plugin list page.

Editing/Deleting/Viewing a Customized Plugin

On the **Navigation Bar**, click **Plugin** to see the plugin page. All the configured customized plugins are displayed in a table on this page.

To edit a plugin, click the **Edit** link 

in the last column of the plugin page.

To delete a plugin, click the **Delete** link 

in the last column of the plugin page.

To view the details of a plugin, click the **View** link 

in the last column of the plugin page. On the detailed plugin page, you can see the plugin information in XML format by clicking the  icon.

Plugin info(Plugin ID:47001)

```
<rule id="47001">
    <fingerprint>
        <product>Apache</product>
        <version>5.0</version>
        <os><value>0</value><value>1</value><value>2</value></os>
    </fingerprint>
    <vulnerability_profile>
        <name><value>CPlugin1</value></name>
        <severity>2</severity>
        <influence>1</influence>
        <type>INFO_DISCLOSURE</type>
        <cvss_vector>AV:N/AC:L/Au:N/C:N/I:N/A:C</cvss_vector>
```

Figure 69: Plugin Information Display

Using Customized Plugins in a Task

Once a customized plugin is successfully configured, it is automatically added to the plugin database, and you can select it when creating a task.

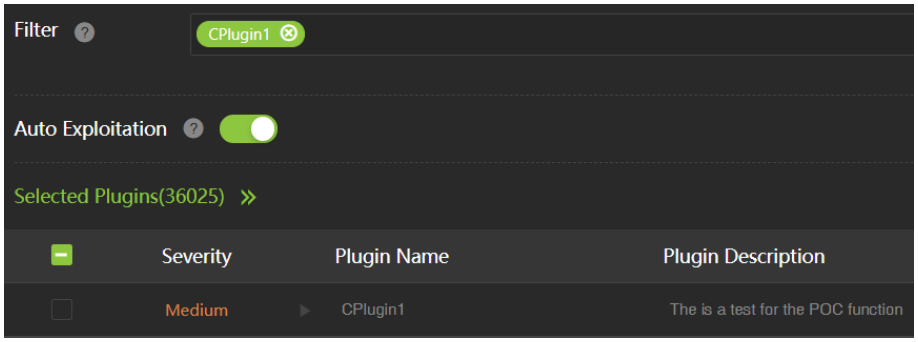


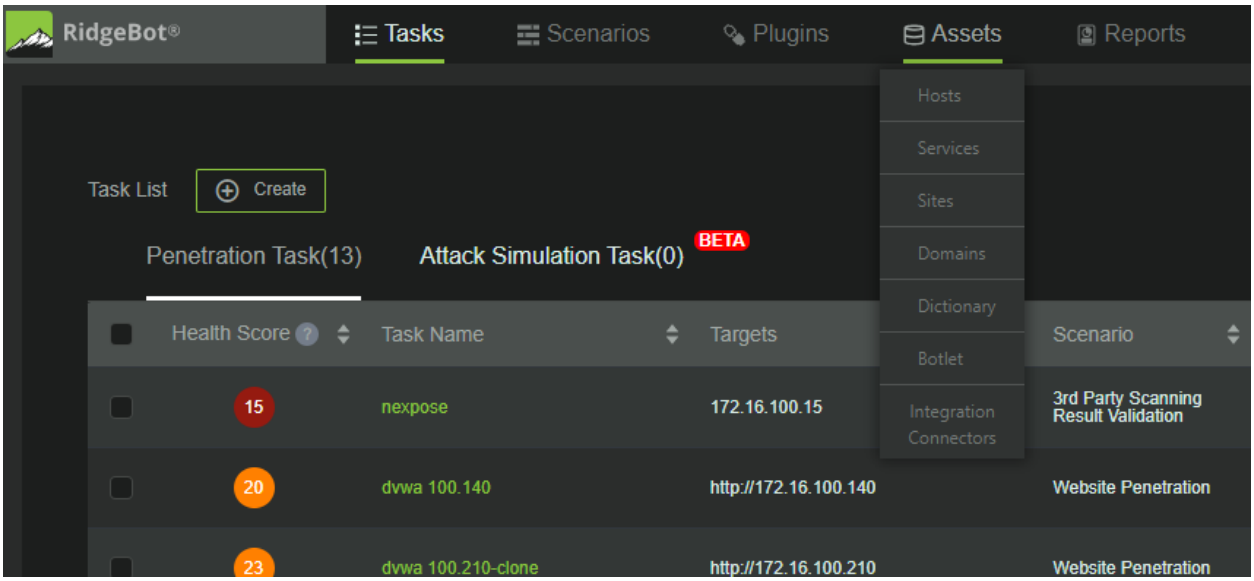
Figure 70: Selecting a Customized Plugin when Creating a Task

Chapter 6 Assets

This section describes the Asset management tab of RidgeBot navigation bar in following sections:

- Hosts
- Services
- Sites
- Domains
- Dictionary
- Butlet Refer to Chapter 3 Tasks, section Configuring an Attack Simulation Task
- Integration Connectors. This section will be described in a separated Chapter

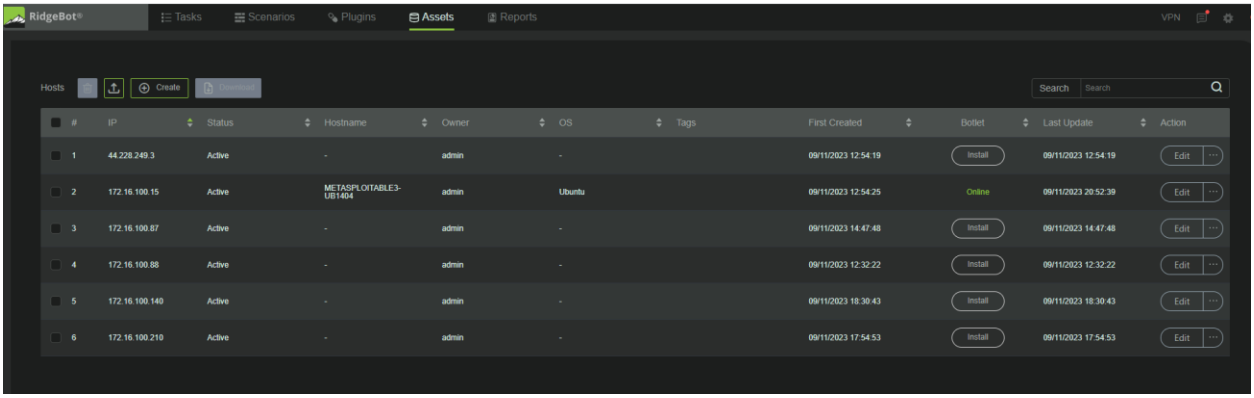
Whenever the tasks are running, the RidgeBot discovers the assets either the hosts, the services, the websites, or domains, and store them the system and can be viewed in the Asset tab. Hover the pointer over the Asset tab, a selection menu will show up. The following sections describe these menu items.



Hosts

Select the "Hosts", the list of the hosts discovered by the RidgeBot is displayed. It shows the IP address, hostname, OS type, and among other information. It also shows whether a Botlet is installed in that host. The sort of the list by column can be changed by click the correspondent column header. Click

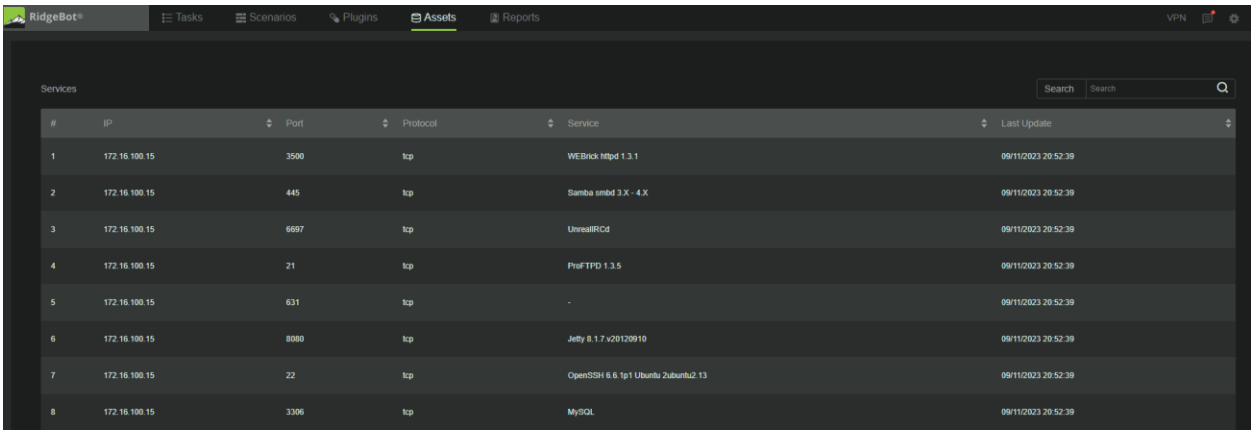
the same column header another time will change the order from ascending to descending and vis versa.



You can update the host table attribute by upload a file by click the upload button. You can also modify the host attribute by click the edit button at right site of each row. You can also manually create a host by click the "Create" button. If one or more hosts are selected, you can download the host table in CSV format by click the "Download" button. The name of the downloaded file is "hosts.csv" Or, you can delete the selected hosts by click the delete button (the garbage can icon).

Services

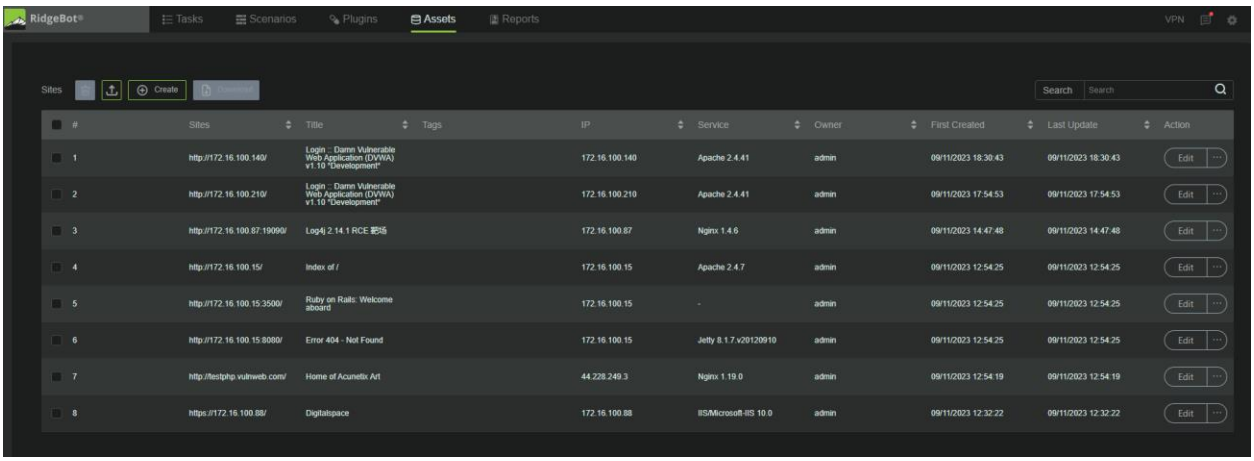
Click the Service, the list of the services discovered will show in the service table. It shows the IP addresses, Port numbers, Protocols, and the name of the services. The sort of the list by column can be changed by click the correspondent column header. Click the same column header another time will change the order from ascending to descending and vis versa.



The service table cannot be modified or downloaded.

Sites

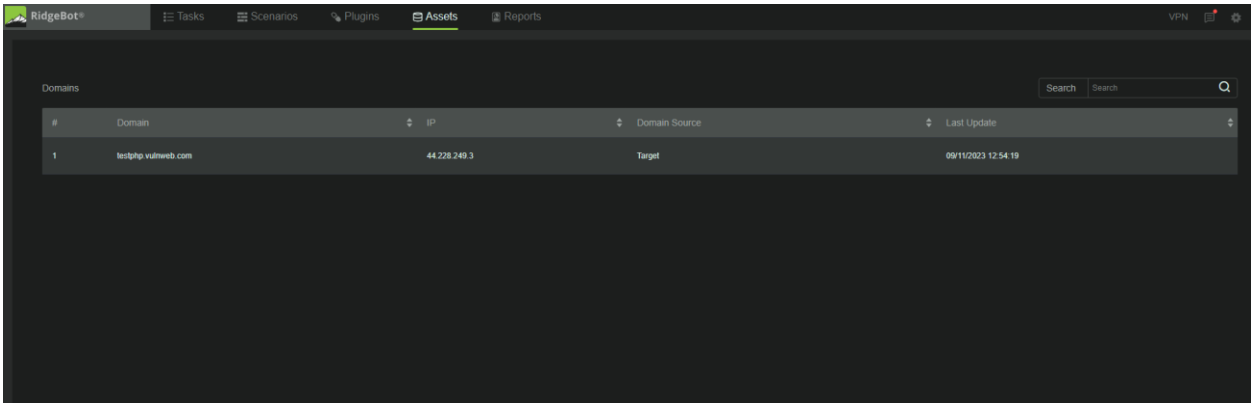
Select "Sites", the list of discovered websites will show up in the site table. It shows the website URL, title of the page, IP address, name of the service, and so on. The sort of the list by column can be changed by click the correspondent column header. Click the same column header another time will change the order from ascending to descending and vis versa.



You can update the site table attribute by upload a file by click the upload button. You can also modify the site attribute by click the edit button at right site of each row. You can also manually create a website by click the "Create" button. If one or more websites are selected, you can download the website table in CSV format by click the "Download" button. The name of the downloaded file is "websites.csv" Or, you can delete the selected hosts by click the delete button (the garbage can icon).

Domains

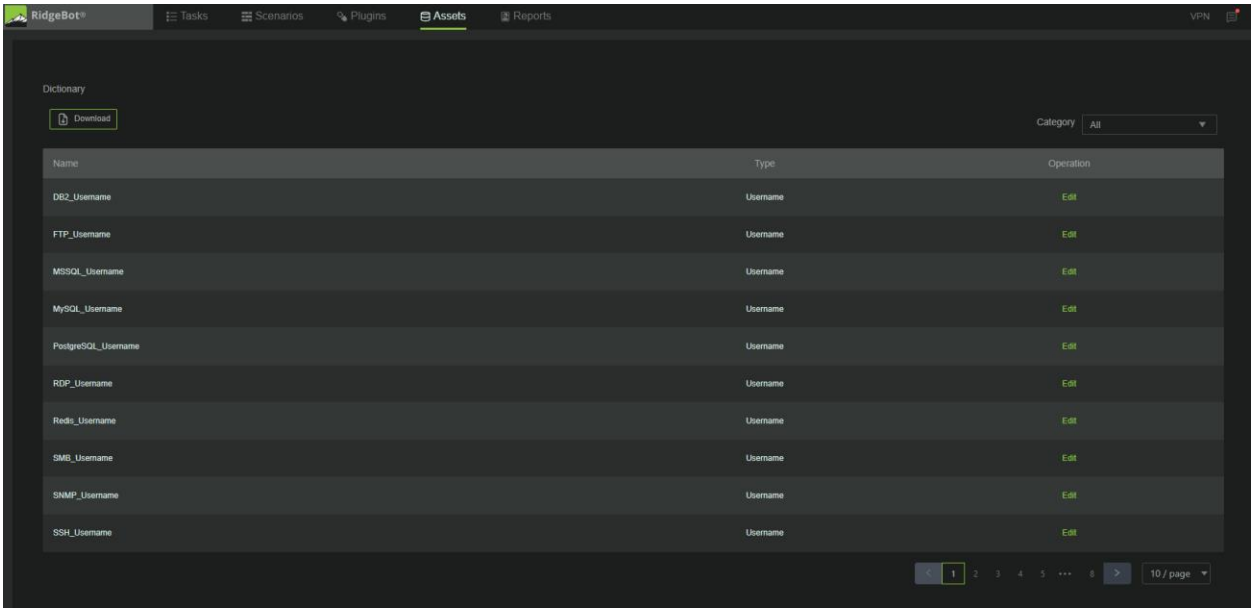
Click the "Domains", a list of scanned web domains will show up in the domain table. It will show the domain name, IP address, Domain Sources. The sort of the list by column can be changed by click the correspondent column header. Click the same column header another time will change the order from ascending to descending and vis versa.



The Domain table cannot be modified or downloaded

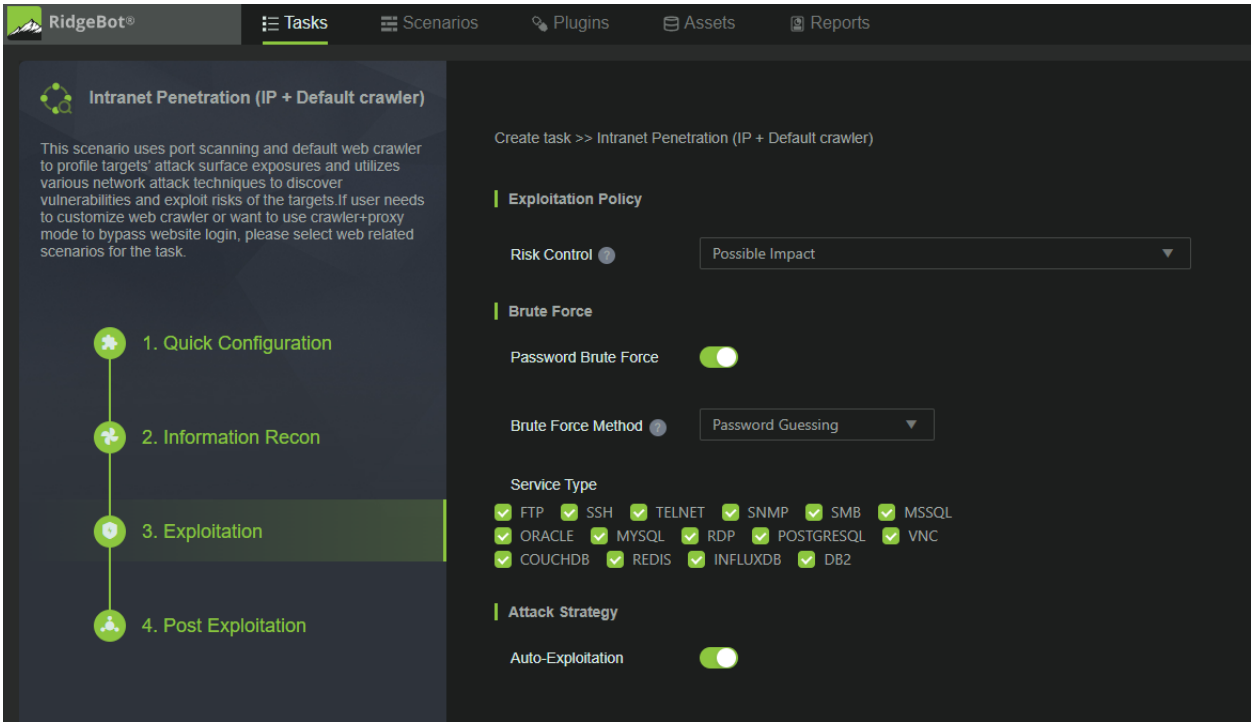
Dictionary

The Dictionary page contains the dictionary of username and password for different service types.

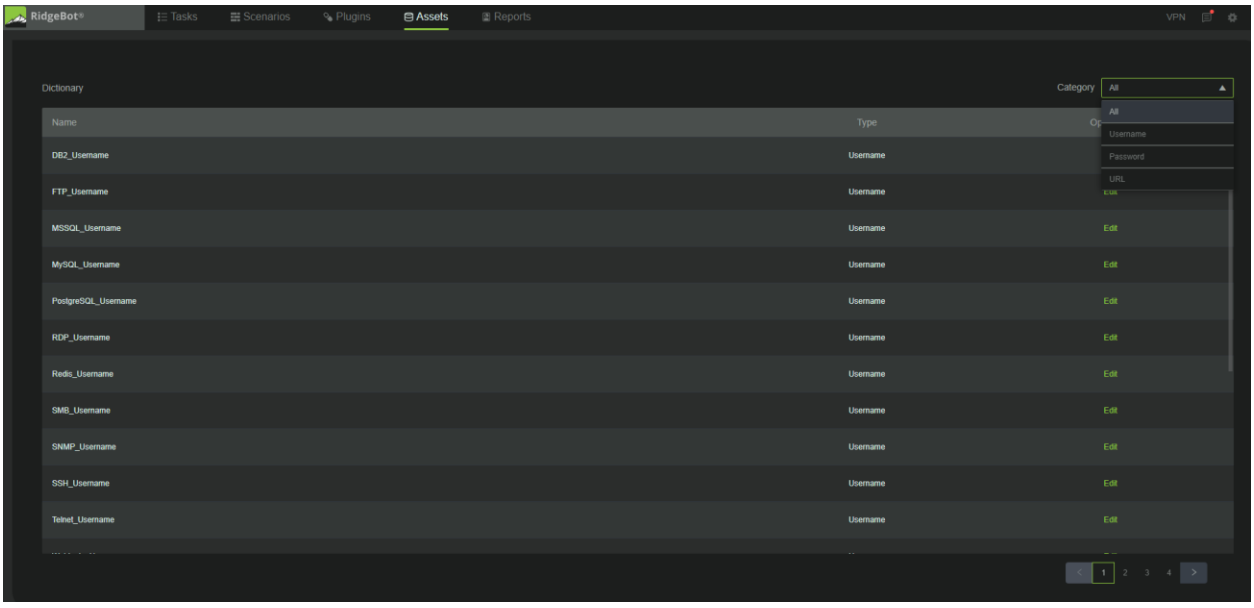


The dictionary only has a small subset of commonly used username and password. RidgeBot will use the credential from the appropriate dictionary during a brute-force attack. Ridgebot supports two type brute-force password matching options: password guessing or password spray. Password guessing method is to match one username with many passwords. Password spray method is to match one password with many usernames.

The dictionary service type can be selected in a Task's Exploitation configuration page. The service type option is shown based on the selected scenario. The below screenshot is an example of the service type options from a Intranet Penetration scenario.



The Category pull-down menu provides access to specific dictionaries: All, username, password, and URL.



To modify the contents in the System Dictionary, follow these steps:

1. On the Navigation Bar, mouse over the Assets tab, and select Dictionary from the drop-down menu. The Dictionary page is displayed.

2. Click the Category drop-down menu, and filter the dictionary contents by selecting the category you're interested in. Detailed contents of the selected category are then listed on the page.

3. From the table, click Edit on the far right of the entry you want to change, then the Edit Dictionary dialog box is shown.

4. Click the Upload File button, select the appropriate content file and then click Save. The file type of the uploaded file must be in .txt in UTF-8 format, and each line in the file may not exceed 100 characters.

Note: Users are highly recommended to update these dictionaries with the commonly used credentials in their organization.

Botlet

Refer to the Install Botlet subsection of Chapter 3 Tasks, section Configuring an Attack Simulation Task on how to install Botlet

Integration Connectors

Refer to Chapter 12 Integration

Chapter 7 Reports and Report Management

This chapter discusses reports and report management in the following sections:

- Viewing and Managing Reports
- Downloading and Encrypting Reports
- Generating a Report for a Penetration Task
- Generating a Report for an Attack Simulation Task

Once a task has completed running, a **Report** option is shown in the task list.

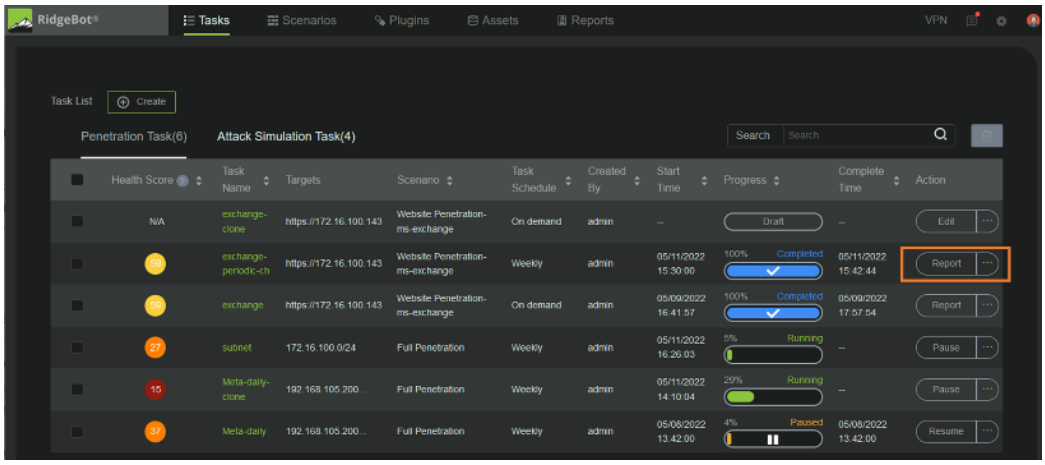


Figure 71: Generate a Report from the Action Column for the Task

Click on the **Report** icon to generate a report. A dialog box pops up providing some options to choose from. Click **Generate** at the bottom right of the dialog box to generate the report.

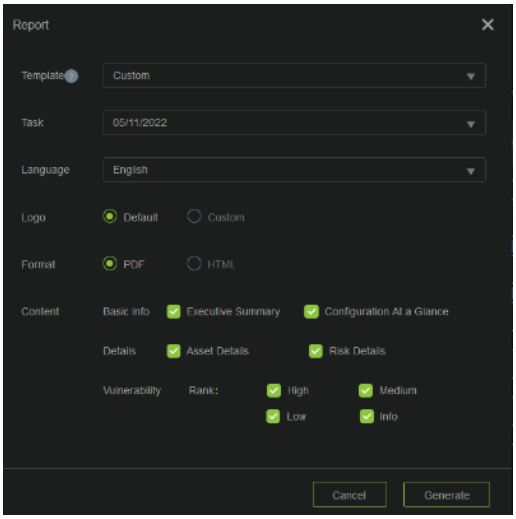


Figure 72: Generate Report Dialog Box

Viewing and Managing Reports

Selecting the **Reports** tab on the Navigation Bar shows a list of reports. Each entry shows the name of the report which is the Task name appended with a timestamp reflecting when the report was generated. Other fields on the display show the Template, Format, Progress status, Finished Time and Actions for the report. Once the report is completed (the progress field shows 100%), you can choose **Download** or **Delete** in the Action column.

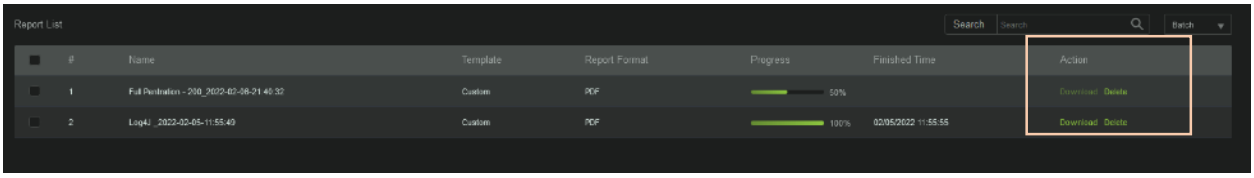


Figure 73: Report Management List

> **Note**: The report management display only lists the reports created by the user currently logged in, unless the login user is **admin**.

Reports applicable to Attack Simulation tasks contain **Default** in the Template column of the reports list display. All values other than "Default" in the Template column indicate Penetration task reports.

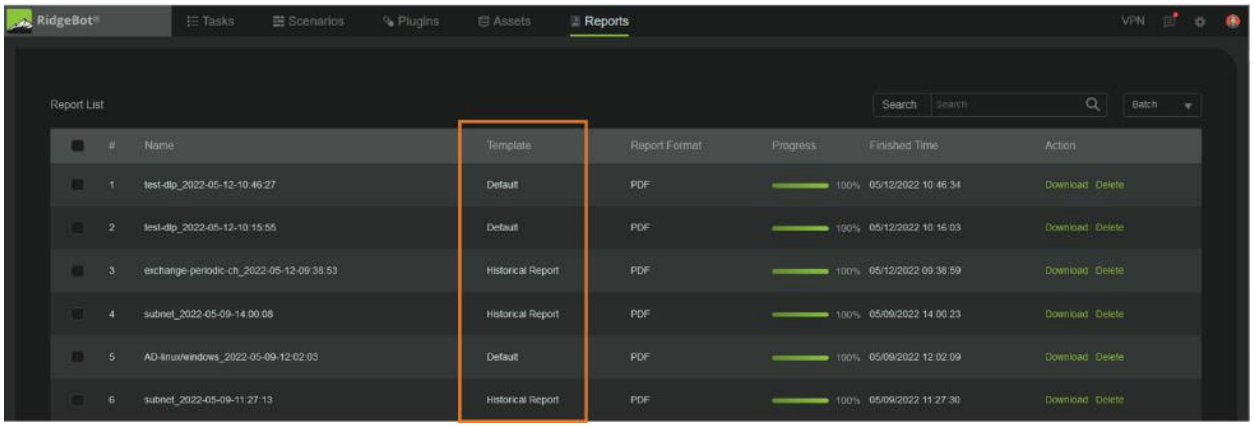


Figure 74: Reports List Display

Downloading and Encrypting Reports

If you select a report for **Download**, there is an option to encrypt the report, with a default of No. If No is selected, the report opens on your screen. If Report Encryption = Yes is selected, an encrypted report is created in zip file format.

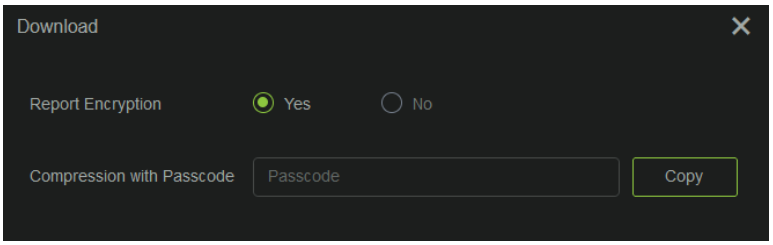


Figure 75: Report Download with Encryption

Note: The **Passcode** that you enter as the encryption key is not stored in the system. You **must** copy or remember the password you enter to later open and retrieve the content of the report. There is no password recovery mechanism.

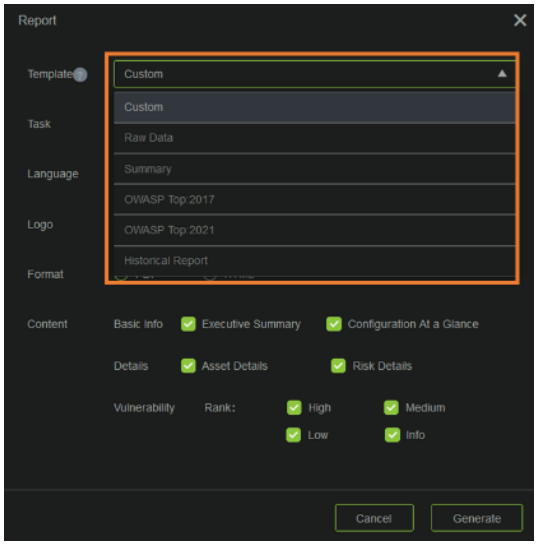
Generating a Report for a Penetration Task

Generating a report for a Penetration task requires a selection of various options as discussed below.

Report Templates

To create a report, select a Template in the dialog box. The template defines the report type such as Custom, Raw or Summary.

- The **Custom** and **Summary** templates allow the selection of the report format in PDF or HTML as well as the detailed sections of the report content.
- The **Raw** template generates a report with task results in a .csv file format.
- The **OWASP Top 10** templates generate a report with website penetration test results including the vulnerabilities found that are listed in the OWASP Top 10 2017 and 2021 specifications.
- The **Attack Surface** report is available for tasks using the Attack Surface Identification scenario.
- An **Historical** report is available for tasks that run on a repeated schedule and includes trend analysis for results over different runs of the same task.



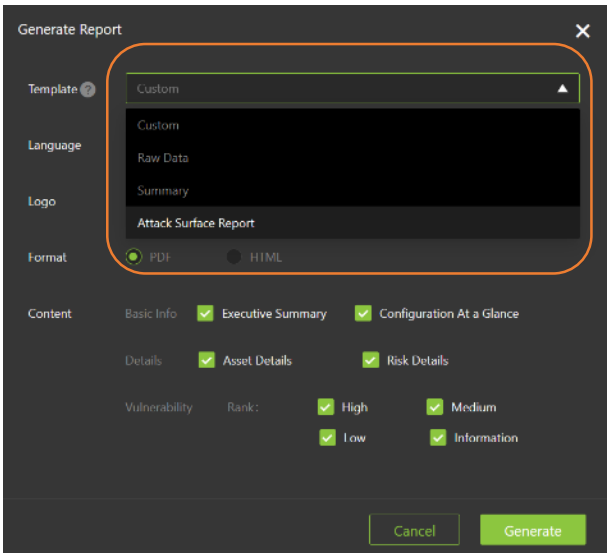


Figure 76: Report Template Selection Options

Notes:

- The OWASP Top-10:2017 and OWASP Top-10:2021 report templates are only available when a task is using the Website Penetration Scenario.
- The Attack Surface Report template is only available when a task is using the Attack Surface Identification Scenario.
- The Historical report template is only available for tasks that run on a repeated schedule (daily, weekly, or monthly).

Report Localization

As of version 3.5, a report can be generated in different languages. Select the desired report language from the **Language** option pull-down menu. The default language is English, other options include Korean and Spanish.

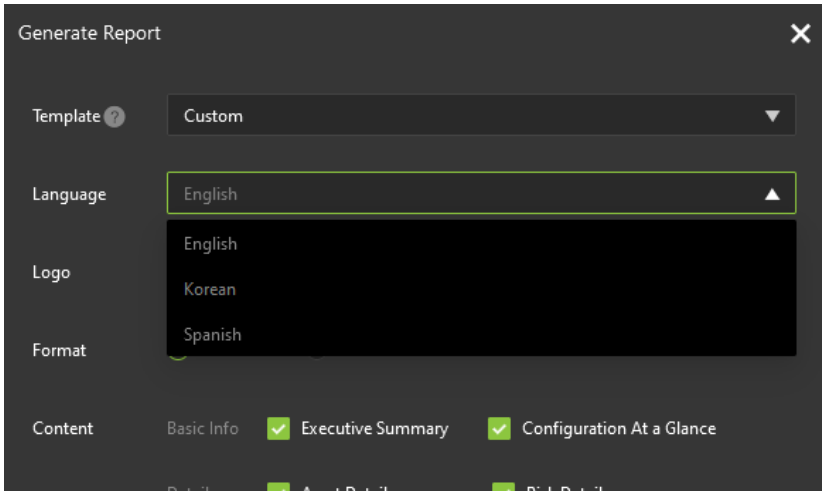


Figure 77: Report Language Selection Options

Note: General text in the report is shown in the selected language. Technical information is always shown in English.

Report Co-Branding

To insert a Partner Logo into a report, select **Custom** or **Summary** in the Template field, then select the **Custom** radio button in the **Logo** field. Click on the **+** icon to upload an Approved Partner Logo file provided by Ridge Security.

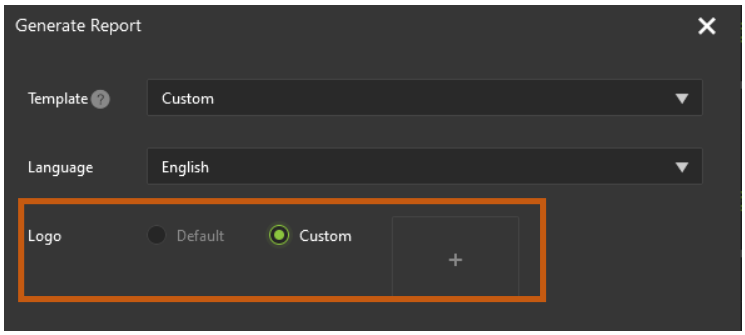
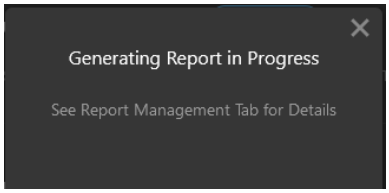


Figure 78: Co-Branding Selection

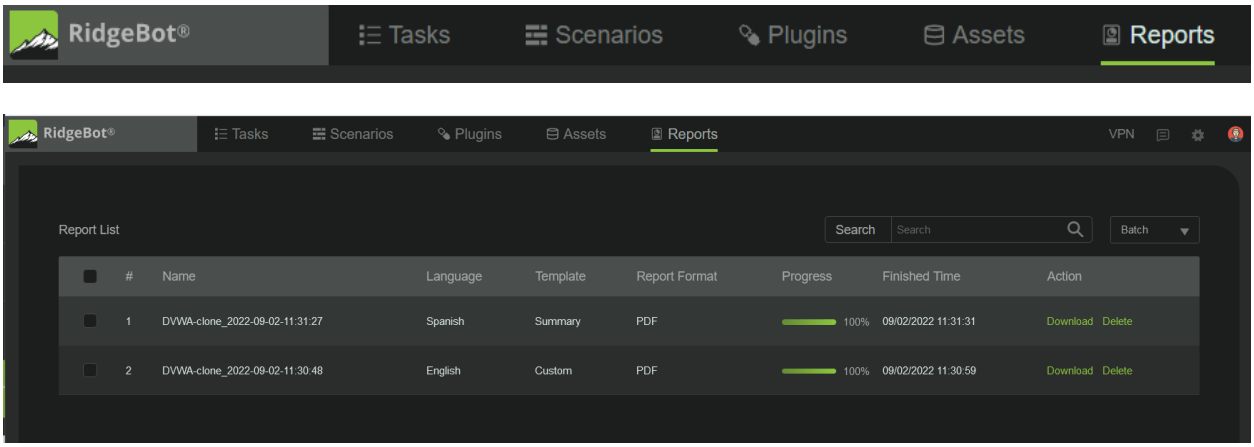
Note: Report Co-Branding is only available to MSSP partners approved by Ridge Security. An MSSP Partner can send a request to support@ridgesecurity.ai to initiate the process.

Generating a Report

Once the report parameters are selected, click on **Generate** to create a report. An acknowledgement dialog box pops up.



The generated report is available in the **Reports** tab of the main RidgeBot Navigation Bar.



Example of the Report List from version 4.1

Report Content

RidgeBot Penetration task reports can be generated in PDF, HTML, or CSV format. Report content can be customized.

The report starts with a summary including a Total Health Score and Risk Weight Assessment. This section provides a threat overview of the test target(s). The Total Health Score is a RidgeBot score like CVSS. The Risk Weight Assessment is a bubble chart that displays Critical Business Risks and Vulnerabilities in visual form.

The Critical Business Risk includes the vulnerabilities that were successfully exploited by RidgeBot. This risk is the most urgent security gap requiring immediate attention to resolve.

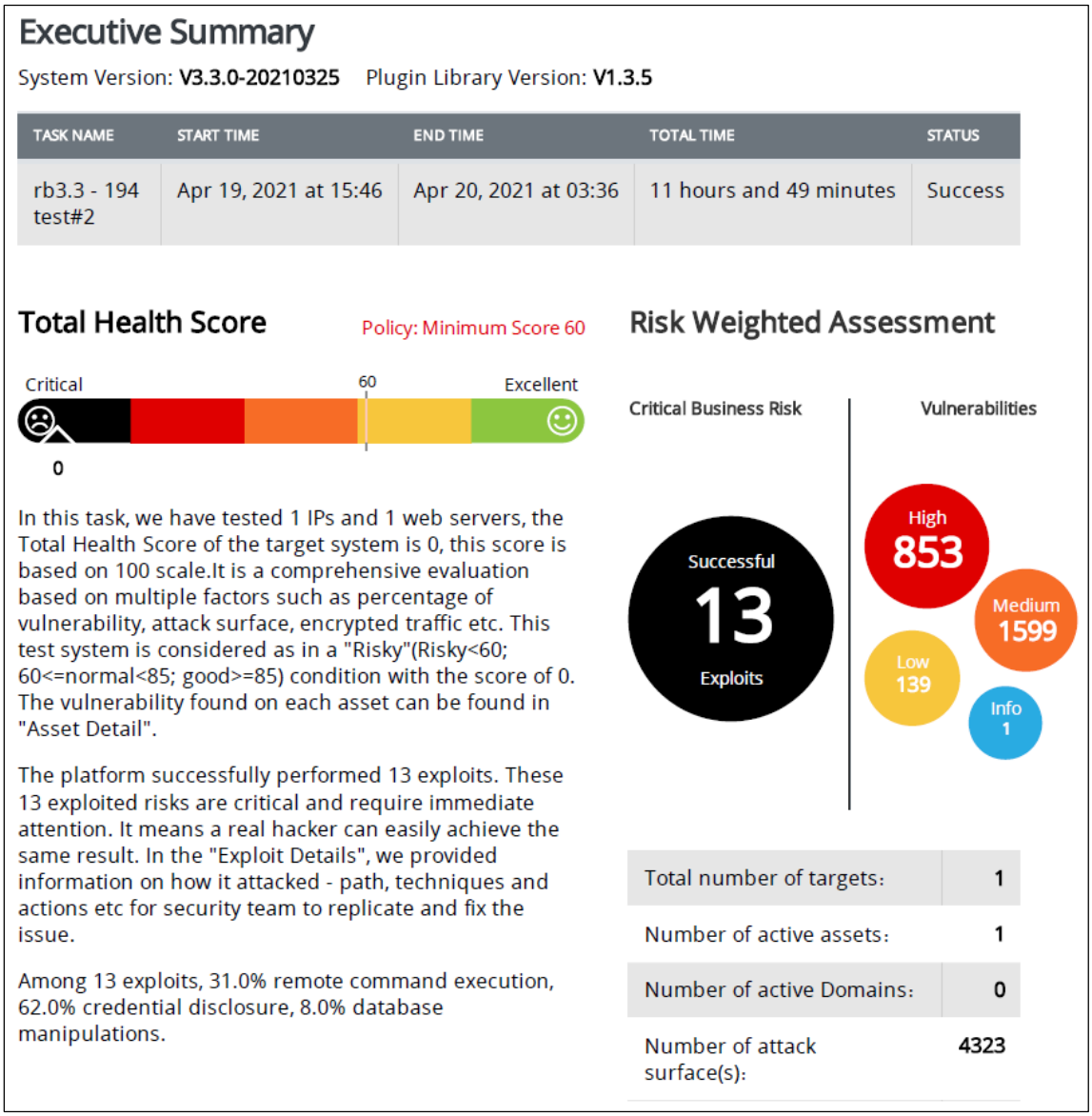


Figure 79: Example of an Executive Summary

If selected before generation, the report includes full details of the Critical Business Risk, Asset Details, Website Fingerprints, Host Open Ports, Attack Surfaces and Vulnerabilities

For each security risk discovered by the Penetration Test, a suggested solution is provided to improve the level your security posture.

Historical Report Content

As of version 4.0, historical reports can be generated for tasks that have run repeatedly (daily, weekly or monthly). Once the task has run multiple times, over a specific time period, a historical report provides trend information on the test results found during successive test runs.

A historical report is generated by choosing **Historical** in the report Template options.

The report starts with summary information regarding the configuration and asset details, and then provides a series of trend graphs including Health Score, Validated Risks, Total Vulnerabilities, Attack Surfaces, Open Ports, and URL Attack Surfaces.

The graphed trends are helpful to assess how the security posture of the target changes over time; whether it has improved (older vulnerabilities were resolved), or regressed (new vulnerabilities have been introduced, perhaps by upgrades, new application installations or unsafe browsing).

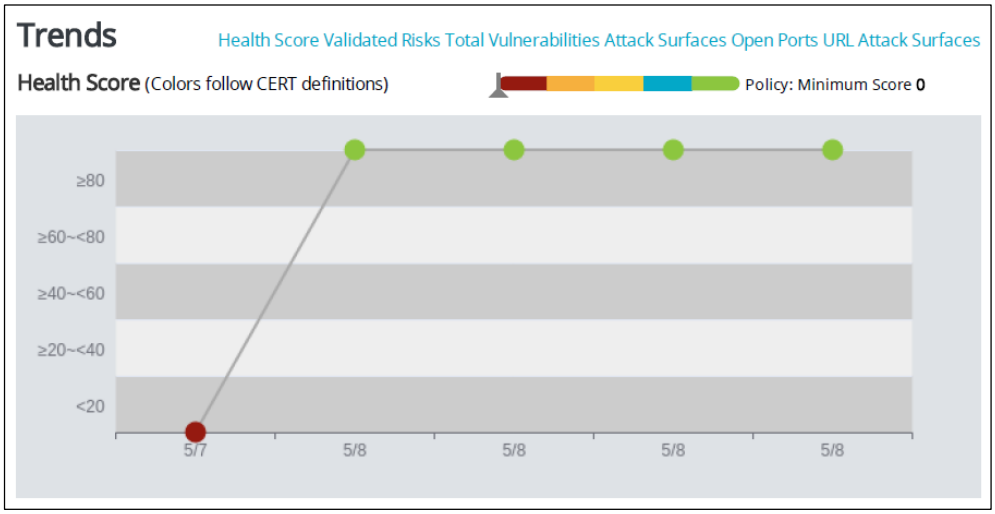


Figure 80: Example of Health Score Trend Graph in an Historical Report

The final section of the report provides a Risk Summary.

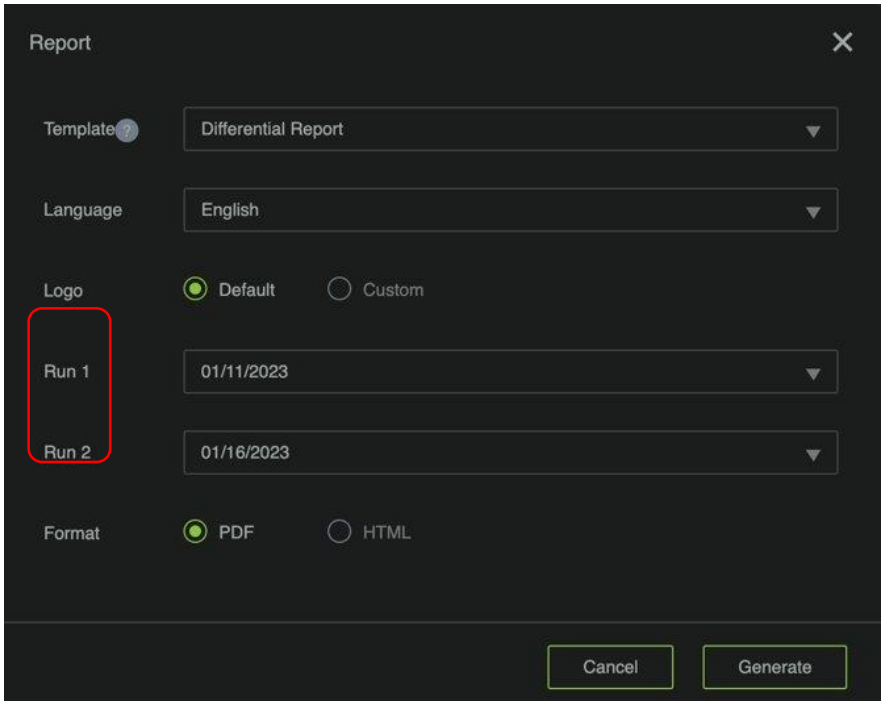
DATE	RISK TYPE	DESCRIPTION	TARGET
05/07/2022 16:26:00	Remote Command Execution	UnrealIRCD 3.2.8.1 Backdoor Command Execution	172.16.100.119
	Remote Command Execution	Samba 'username map script' Command Execution	172.16.100.119

Figure 81: Example Risk Summary in an Historical Report

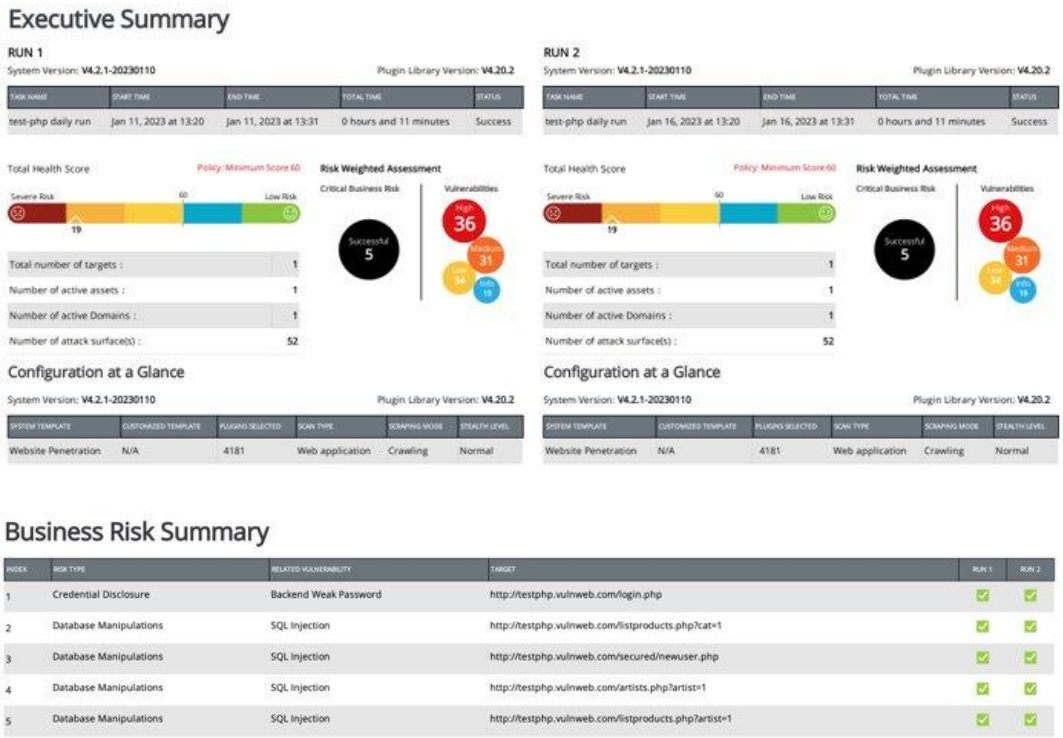
Differential Report

The differential report is to compare the values of Executive Summary, Asset Details, Business Risks, Website Fingerprints, Open Ports, Attack Surfaces and Vulnerability List of two runs of a periodic schedule task.

Differential Report setting



Sample Report



Executive Summary

RUN 1

System Version: **V4.2.1-20230110** Plugin Library Version: **V4.20.2**

TASK NAME	START TIME	END TIME	TOTAL TIME	STATUS
test-php daily run	Jan 11, 2023 at 13:20	Jan 11, 2023 at 13:31	0 hours and 11 minutes	Success

Total Health Score — Policy: Minimum Score 60

Severe Risk — 60 — Low Risk

19

Total number of targets :	1
Number of active assets :	1
Number of active Domains :	1
Number of attack surface(s) :	52

Risk Weighted Assessment

Critical Business Risk: Successful 5

Vulnerabilities: High 36, Medium 31, Low 34, Info 19

Configuration at a Glance

System Version: **V4.2.1-20230110** Plugin Library Version: **V4.20.2**

SYSTEM TEMPLATE	CUSTOMIZED TEMPLATE	PLUGINS SELECTED	SCAN TYPE	SCRAPING MODE	STEALTH LEVEL
Website Penetration	N/A	4181	Web application	Crawling	Normal

RUN 2

System Version: **V4.2.1-20230110** Plugin Library Version: **V4.20.2**

TASK NAME	START TIME	END TIME	TOTAL TIME	STATUS
test-php daily run	Jan 16, 2023 at 13:20	Jan 16, 2023 at 13:31	0 hours and 11 minutes	Success

Total Health Score — Policy: Minimum Score 60

Severe Risk — 60 — Low Risk

19

Total number of targets :	1
Number of active assets :	1
Number of active Domains :	1
Number of attack surface(s) :	52

Risk Weighted Assessment

Critical Business Risk: Successful 5

Vulnerabilities: High 36, Medium 31, Low 34, Info 19

Configuration at a Glance

System Version: **V4.2.1-20230110** Plugin Library Version: **V4.20.2**

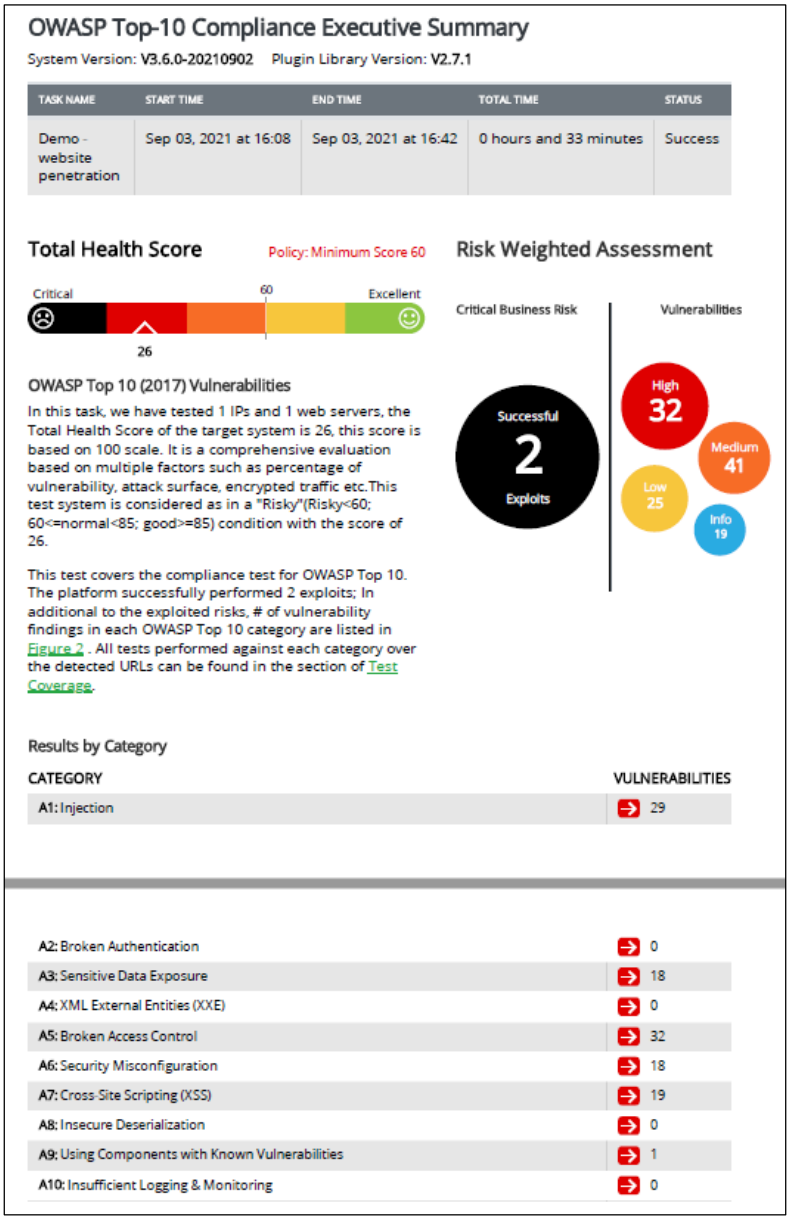
SYSTEM TEMPLATE	CUSTOMIZED TEMPLATE	PLUGINS SELECTED	SCAN TYPE	SCRAPING MODE	STEALTH LEVEL
Website Penetration	N/A	4181	Web application	Crawling	Normal

Business Risk Summary

INDEX	RISK TYPE	RELATED VULNERABILITY	TARGET	RUN 1	RUN 2
1	Credential Disclosure	Backend Weak Password	http://testphp.vulnweb.com/login.php	☑	☑
2	Database Manipulations	SQL Injection	http://testphp.vulnweb.com/listproducts.php?cat=1	☑	☑
3	Database Manipulations	SQL Injection	http://testphp.vulnweb.com/secured/newuser.php	☑	☑
4	Database Manipulations	SQL Injection	http://testphp.vulnweb.com/artists.php?artist=1	☑	☑
5	Database Manipulations	SQL Injection	http://testphp.vulnweb.com/listproducts.php?artist=1	☑	☑

OWASP Top 10 Report Examples

Vulnerabilities Shown in OWASP Top 10:2017 Categories



OWASP Top-10 Compliance Executive Summary

System Version: V3.6.0-20210902 Plugin Library Version: V2.7.1

TASK NAME	START TIME	END TIME	TOTAL TIME	STATUS
Demo - website penetration	Sep 03, 2021 at 16:08	Sep 03, 2021 at 16:42	0 hours and 33 minutes	Success

Total Health Score

Policy: Minimum Score 60

Critical 60 Excellent

26

Risk Weighted Assessment

Critical Business Risk

Successful 2 Exploits

Vulnerabilities

High 32

Medium 41

Low 25

Info 19

OWASP Top 10 (2017) Vulnerabilities

In this task, we have tested 1 IPs and 1 web servers, the Total Health Score of the target system is 26, this score is based on 100 scale. It is a comprehensive evaluation based on multiple factors such as percentage of vulnerability, attack surface, encrypted traffic etc.This test system is considered as in a "Risky"(Risky<60; 60<=normal<85; good>=85) condition with the score of 26.

This test covers the compliance test for OWASP Top 10. The platform successfully performed 2 exploits; In additional to the exploited risks, # of vulnerability findings in each OWASP Top 10 category are listed in Figure 2 . All tests performed against each category over the detected URLs can be found in the section of Test Coverage.

Results by Category

CATEGORY	VULNERABILITIES
A1: Injection	29
A2: Broken Authentication	0
A3: Sensitive Data Exposure	18
A4: XML External Entities (XXE)	0
A5: Broken Access Control	32
A6: Security Misconfiguration	18
A7: Cross-Site Scripting (XSS)	19
A8: Insecure Deserialization	0
A9: Using Components with Known Vulnerabilities	1
A10: Insufficient Logging & Monitoring	0

Figure 82: Example of an OWASP Top10:2017 Compliance Executive Summary

Vulnerabilities Shown in OWASP Top 10:2021 Categories

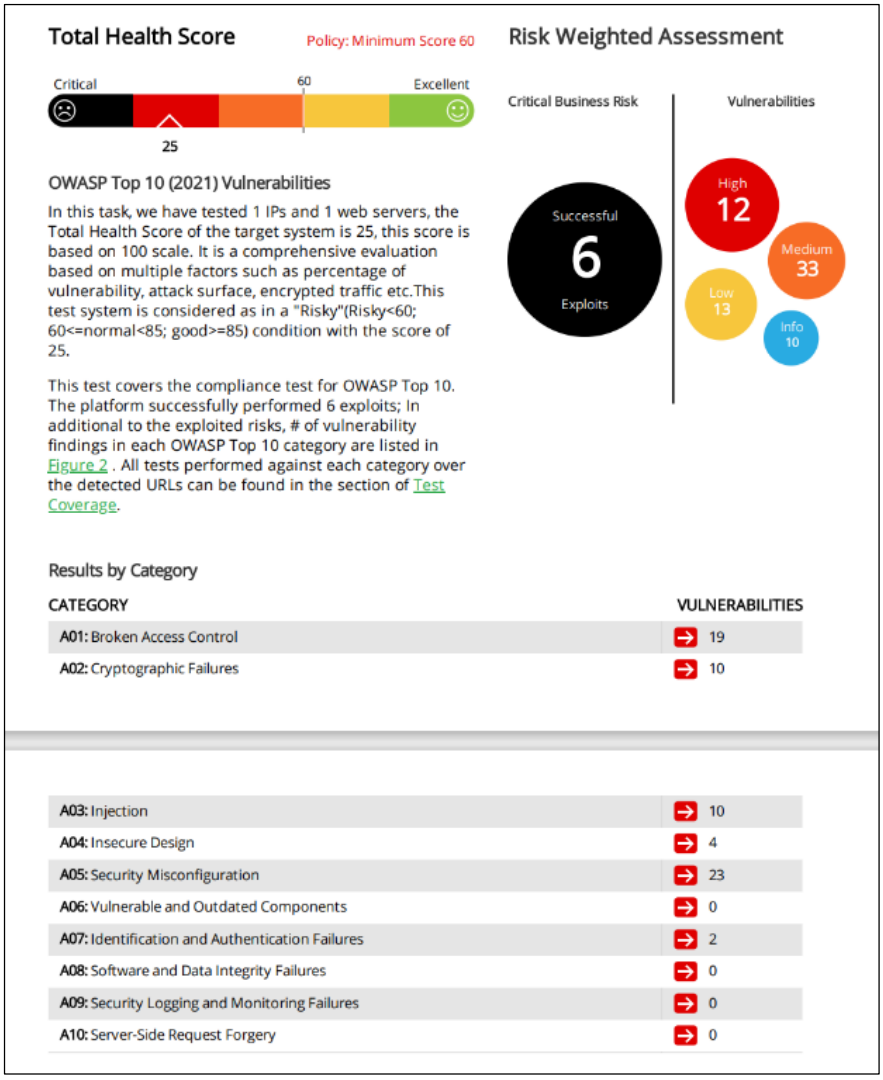


Figure 83: Example of an OWASP Top10:2021 Compliance Executive Summary

3rd Party Scanning Result Validation Report Example

The 3rd Party validation report is the CSV file that contains the Nessus Pro test result and additional columns and rows inserted by RidgeBot to verify the CVE that are found by Nessus Pro. RidgeBot only validates the 3rd party found vulnerability only if the vulnerability has a CVE number.

Column definition:

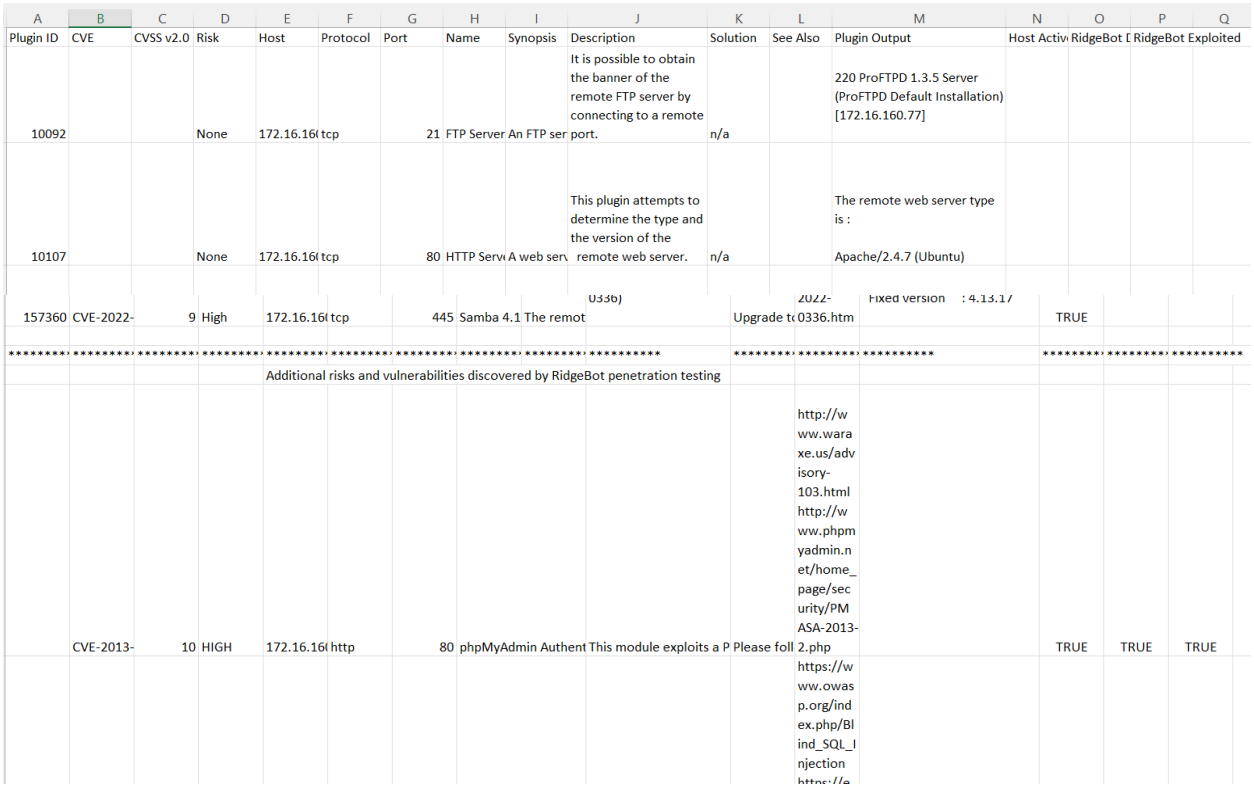
- Column A-M: the original CSV output from the 3rd party.
- HOST Active: Host is active
- RidgeBot Discovered: A vulnerability found by RidgeBot

- RidgeBot Exploited: A vulnerability exploited by RidgeBot

Row definition:

- ******** : This is a divider. Any rows below this divider are the additional risks and vulnerabilities discovered by RidgeBot during the PT validation task.

Sample CSV file output:



Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output	Host Activ	RidgeBot E	RidgeBot	Exploited
10092			None	172.16.16(	tcp	21	FTP Server	An FTP ser	It is possible to obtain the banner of the remote FTP server by connecting to a remote port.	n/a		220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.16.160.77]				
10107			None	172.16.16(	tcp	80	HTTP Serv	A web ser	This plugin attempts to determine the type and the version of the remote web server.	n/a		The remote web server type is : Apache/2.4.7 (Ubuntu)				
									0336)		2022-	Fixed version : 4.13.17				
157360	CVE-2022-	9	High	172.16.16(	tcp	445	Samba 4.1	The remot		Upgrade t(	0336.htm			TRUE		
********	********	********	********	********	********	********	********	********	**********	********	********	**********	*********	********	********	*********
				Additional risks and vulnerabilities discovered by RidgeBot penetration testing												
											http://www.waraxe.us/advisory-103.html http://www.phpmyadmin.net/home_page/security/PMASA-2013-2.php						
	CVE-2013-	10	HIGH	172.16.16(	http	80	phpMyAdmin Authent	This module exploits a P	Please foll					TRUE	TRUE	TRUE
											https://www.owasp.org/index.php/Blind_SQL_Injection					

Generating a Report for an Attack Simulation Task

Generating a report for an Attack Simulation task requires only the selection of file format (PDF or HTML) as discussed below.

Generating a Report

Select **Tasks** on the Navigation Bar and then click **Attack Simulation Tasks** to see a list of tasks. Click on the on the **Report** icon for a task (on the far right) to generate a report for an attack simulation task.

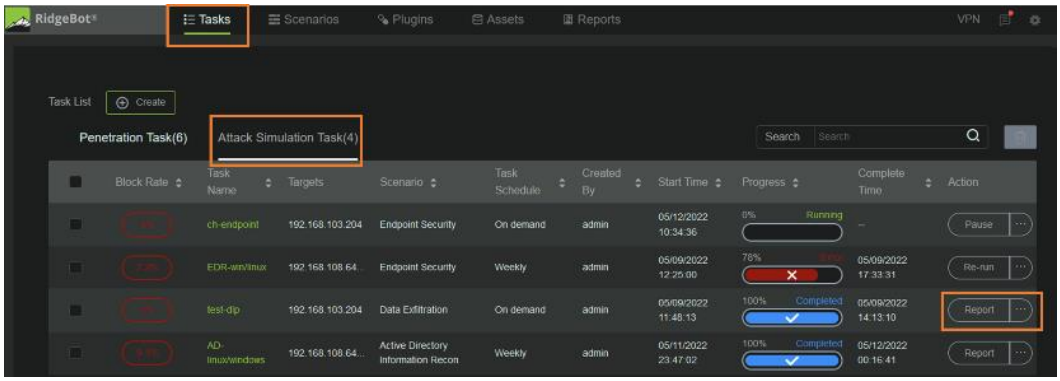
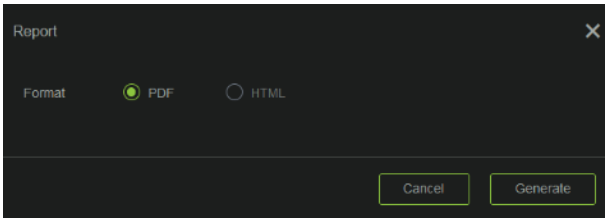
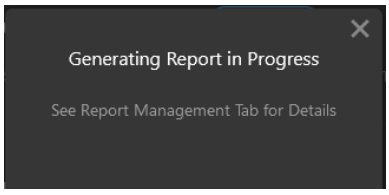


Figure 84: Generating a Report for an Attack Simulation Task

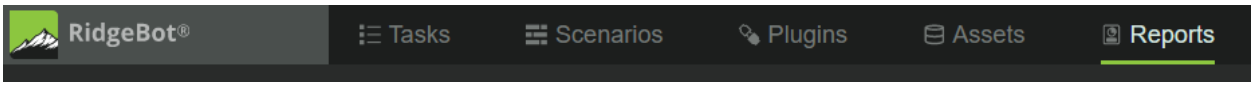
A dialog box pops up providing file format options including PDF or HTML. Only a single default report format is supported for Attack Simulation tasks in version 4.0. The language, customer logo and other customization options supported for Penetration task reports are not yet supported for Attack Simulation reports. Click **Generate** at the bottom right of the dialog box to create the report.



An acknowledgement dialog box pops up.



The generated report is available in the **Reports** tab of the Navigation Bar.



Report Content

RidgeBot Attack Simulation task reports can be generated in PDF or HTML formats. Report content cannot be customized, a default system report template is provided.

The report starts by defining a series of terms used in the report, then provides a set of quick links to take you directly to various sections of the report.

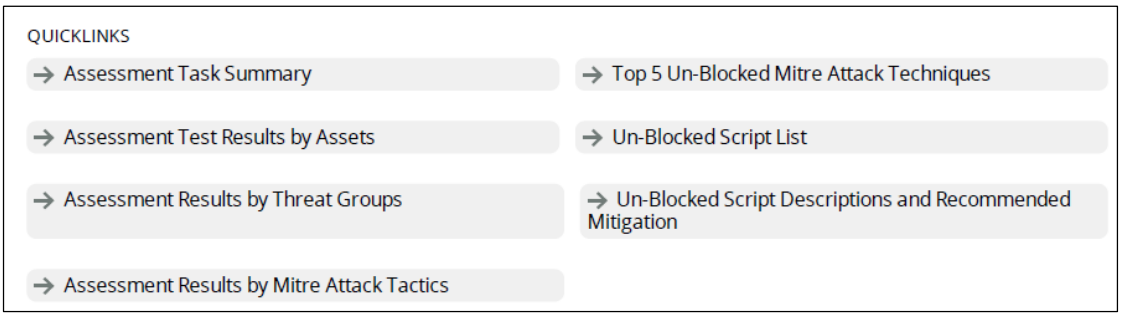


Figure 85: Quick Links to Sections in an Attack Simulation Report

The first sections of the report provide assessments of the test results in summary form, as well as by Assets, Threat Groups, Mitre Attack Tactics, and Mitre Attack Techniques.

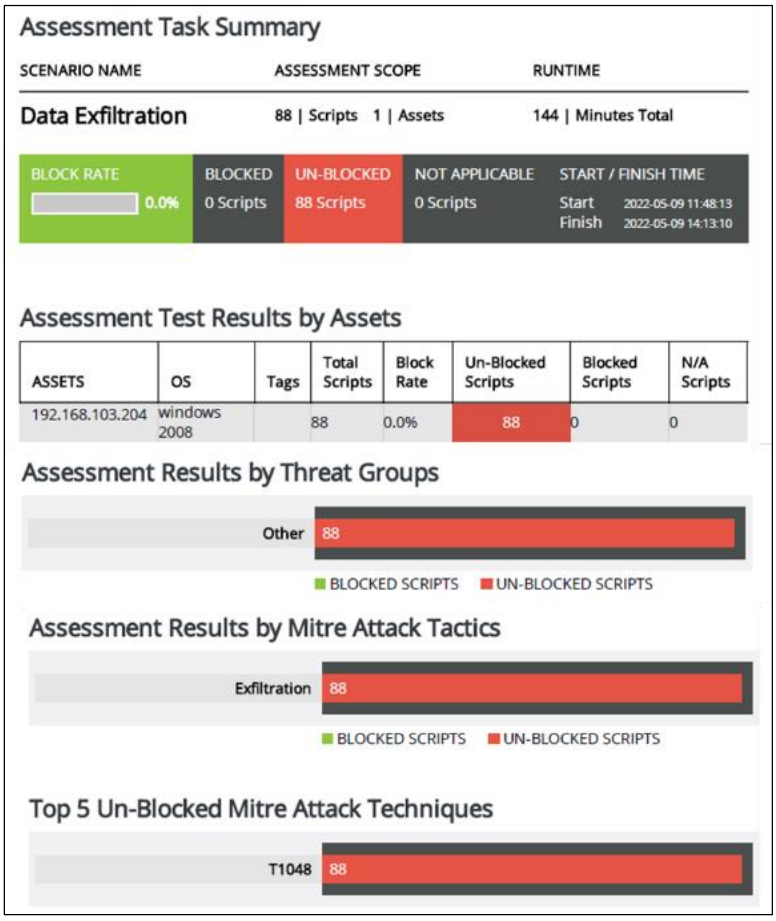


Figure 86: Example of a Summary Assessment in an Attack Simulation Report

The report further lists all the scripts that were not blocked during the test—that means all the scripts that indicate an unresolved vulnerability in the target.

For each non-blocked script discovered during the test, the next section of the report gives a description, a severity score and mitigation advice on how to resolve the vulnerability.

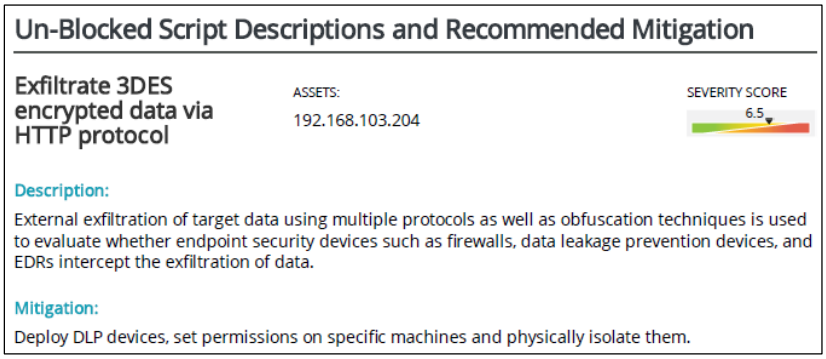


Figure 87: Example of a Non-blocked Script in the Report

Chapter 8 Considerations and Procedures

This chapter has the following sections:

Ransomware Attack Simulation Scenario

The Ransomware Attack Simulation Scenario includes the plugins for the vulnerabilities known to be used by the Ransomware gang to attack and exploit targets. The objective of the simulation is to identify and then exploit these specific vulnerabilities on the test targets. A Ransomware attack may impact a target machine that has the MS17-010 vulnerability. In the worst case, the target machine may freeze. It is recommended to reboot the target machine after the test has completed. To mitigate operational risks, de-select the following two plugins from the Task's Plugin list:

- MS17-010 'EternalRomance/EternalSynergy/EternalChampion' SMB Remote Windows Code Execution.
- MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption And enable Windows SMB Remote Code Execution (MS17-010 and CVE-2017-0144).

In this configuration, RidgeBot can detect the MS17-010 vulnerability and report it in the Vulnerability table, but it does not perform the exploitation code in the test. Therefore, it does not report an MS17-010 Risk.

Smart Crawler + Proxy (Scraping in Proxy mode): Configuration and Procedure to Run the Task

When configuring a task, if **Proxy** is selected in **Scraping** mode, the task starts in the **Waiting** state when you click on the task's **Run** button.

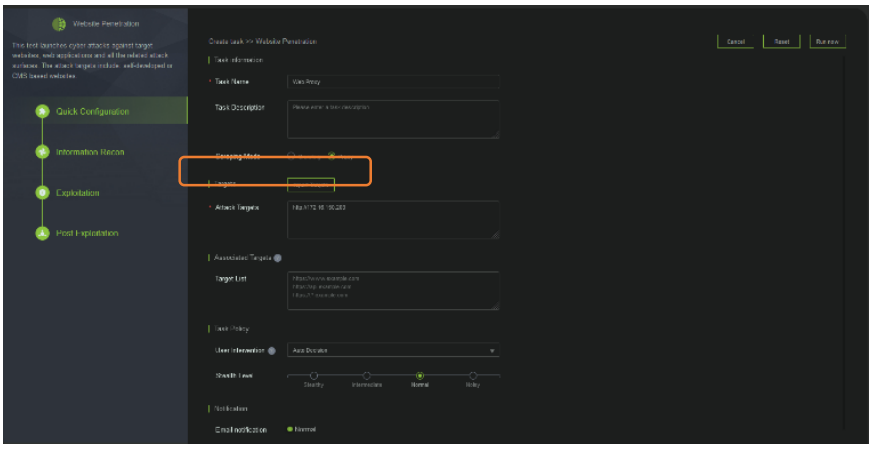


Figure 88: Proxy Option Selected in Scraping Mode

The Task Information Recon configuration allows you to input information into the form. All other parameters are not user configurable and are not shown.

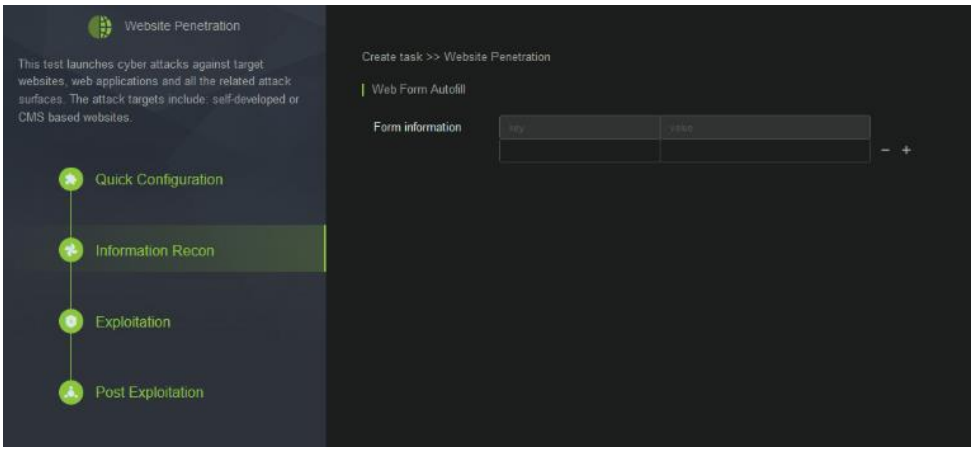


Figure 89: Task Information Recon in Crawler Proxy Option

There are additional steps to complete the configuration. You must re-open the task and select the Proxy configuration in the "Task Operation" to continue the configuration of Proxy in Scraping mode.

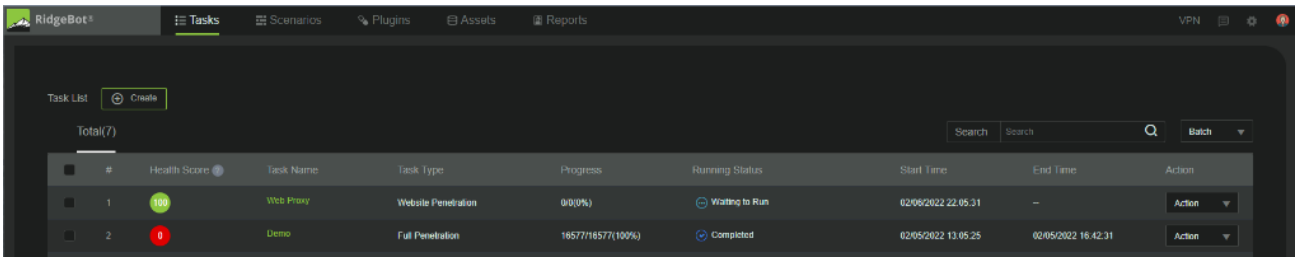


Figure 90: Web Proxy Task is in the "Waiting" State

In the Task Topology view, select Proxy in the Task Operation as shown below. A Proxy Configuration dialog box opens. Follow these steps to complete the setup.

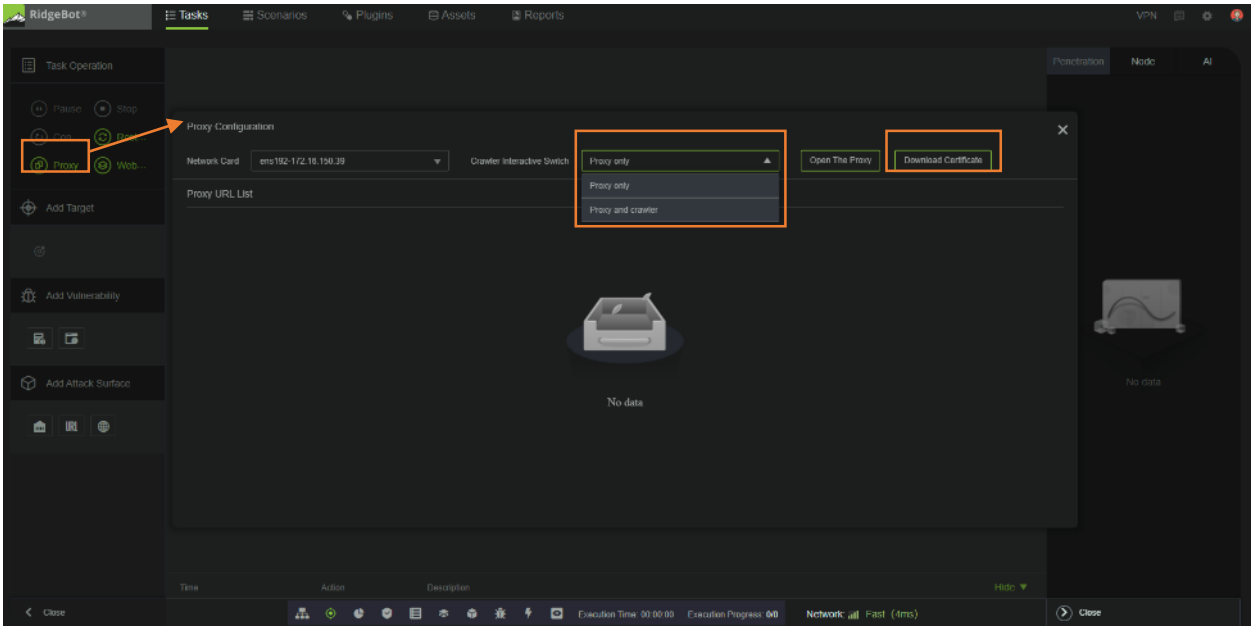


Figure 91: Proxy Configuration Dialog Box

Note: Your web browser must be able to reach the proxy server's IP address. Use the RidgeBot external mapping IP address if applicable.

1. Click on "Download certificate" to get the RidgeBot CA certificate and add this certificate to your web browser.
2. Select the Crawler Interactive Switch:
    a. **Proxy**: The proxy only mode is used for manual URL operation, and there is no crawler interaction. The recorded manual URLs are used as the attack surface.
    b. **Proxy + Crawler**: This proxy mode is a combination of the Proxy + Static and Dynamic modes.
        i. **Proxy+Static**: This mode can be used for login bypass. After the user login, a static crawler uses the cookie obtained by the login continuous crawler. The Proxy+Static crawler mode can be used for the sites like PHP, ASP, ASP.net, and WordPress.
        ii. **Proxy+Dynamic**: Similar to the Proxy+Static mode, the Proxy+Dynamic mode should be chosen for sites using HTML5, RESTAPI base SPA and mobile app.
3. Click on **Open the Proxy** to start. Copy RidgeBot's listening ID (IP address) and listening port (network port) for the web browser's proxy access setup.

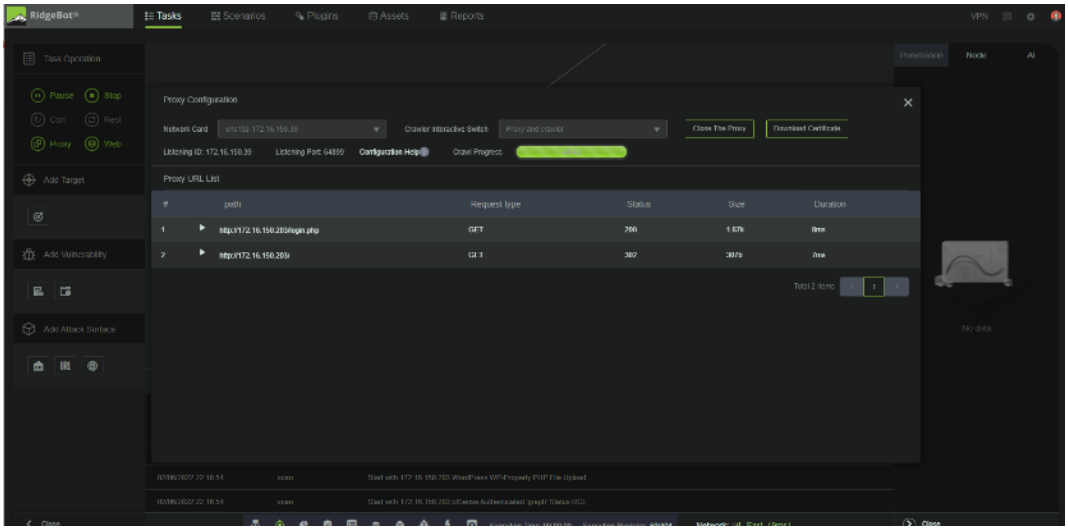


Figure 92: Open Proxy Dialog Box

4. Configure your web browser for proxy access using the information from the previous step. Using the Firefox web browser as an example, you can configure web browser proxy access to the internet using "manual proxy configuration" and select the option to use this proxy for FTP and HTTPS. The browser's HTTP Proxy is RidgeBot's Listening IP and the browser's port is RidgeBot's Listening Port. This configuration is shown below.

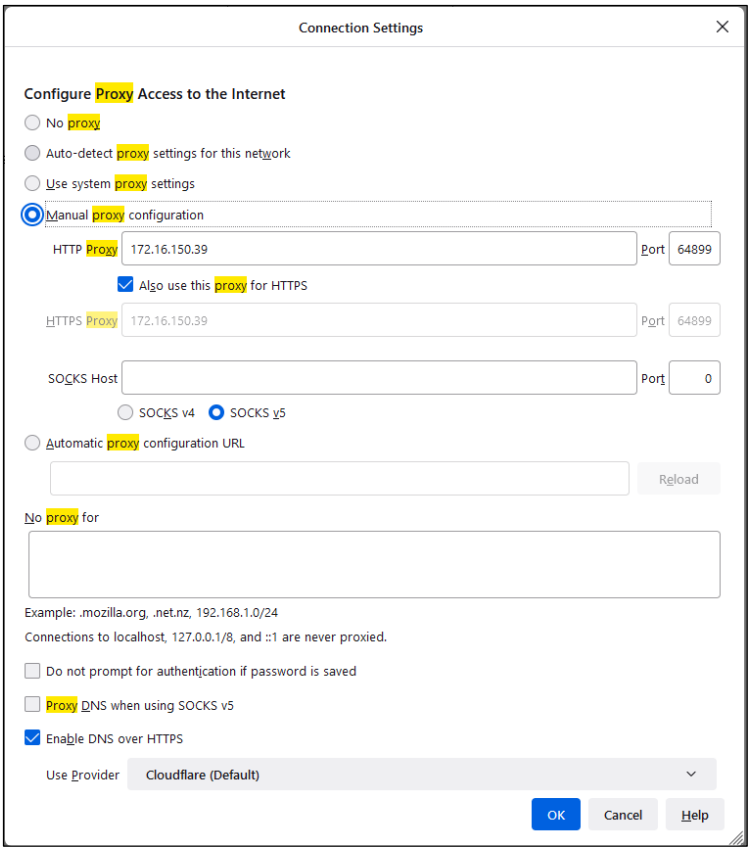


Figure 93: Example of Firefox Web Browser Proxy Configuration

5. The crawler progress bar shows activity when you interact with the target website.

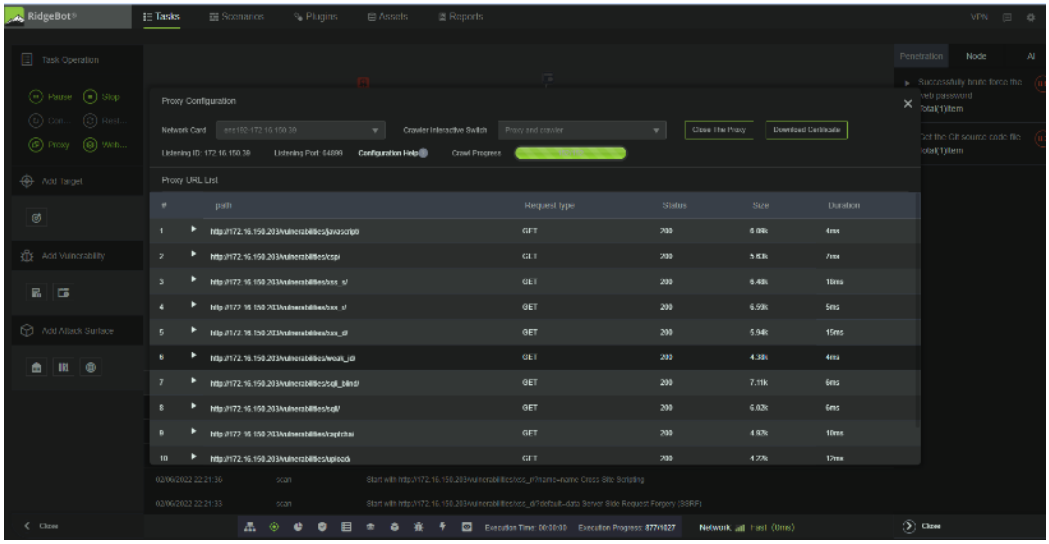


Figure 94: Proxy in Action

6. When finished, click on the "Close the Proxy" button and click OK to close the Proxy configuration dialog.

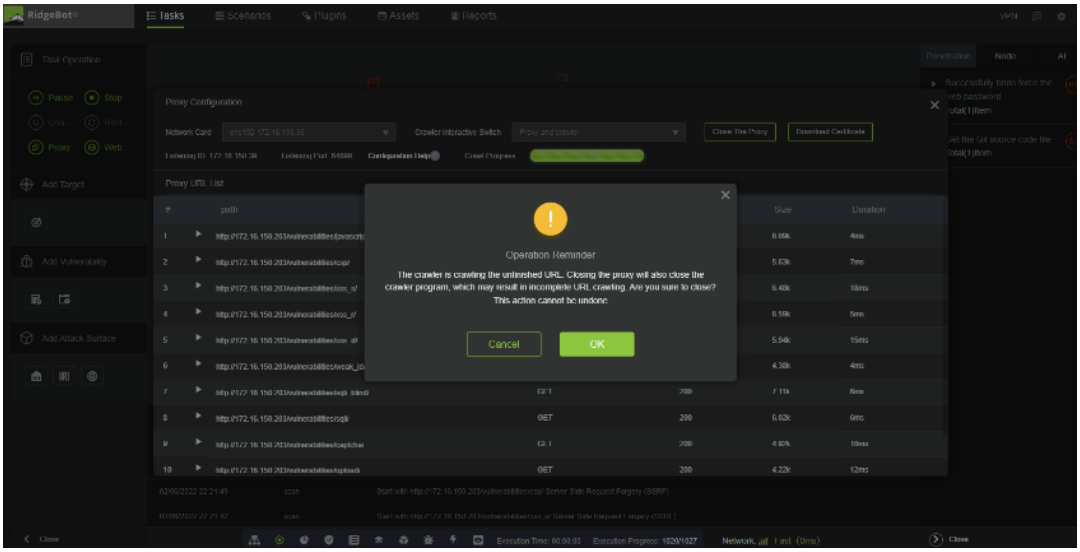


Figure 95: Close Proxy Operation Confirmation Dialog Box

7. When you close the Proxy Configuration Dialog box in the RidgeBot system and the URL recording is done, RidgeBot automatically runs the task.

Web Browser Proxy Configuration

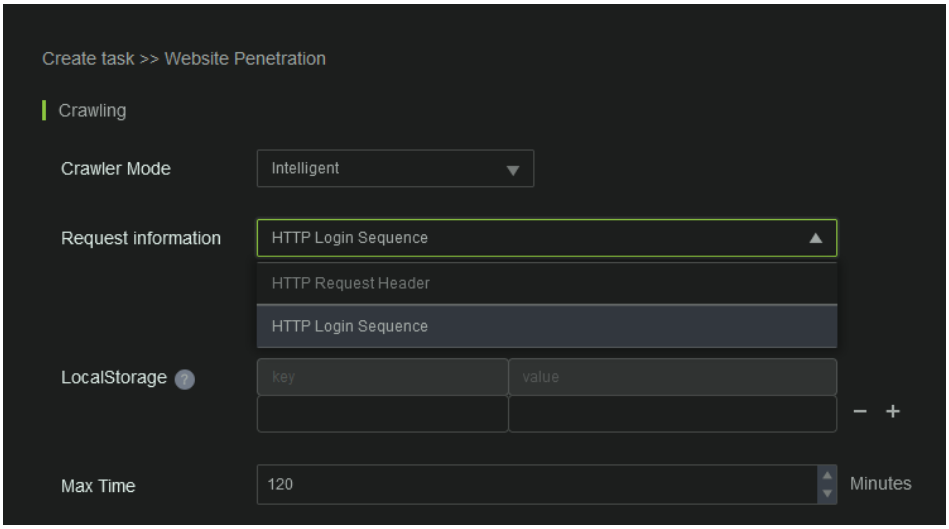
To configure proxy mode for your Web browser, follow these steps.

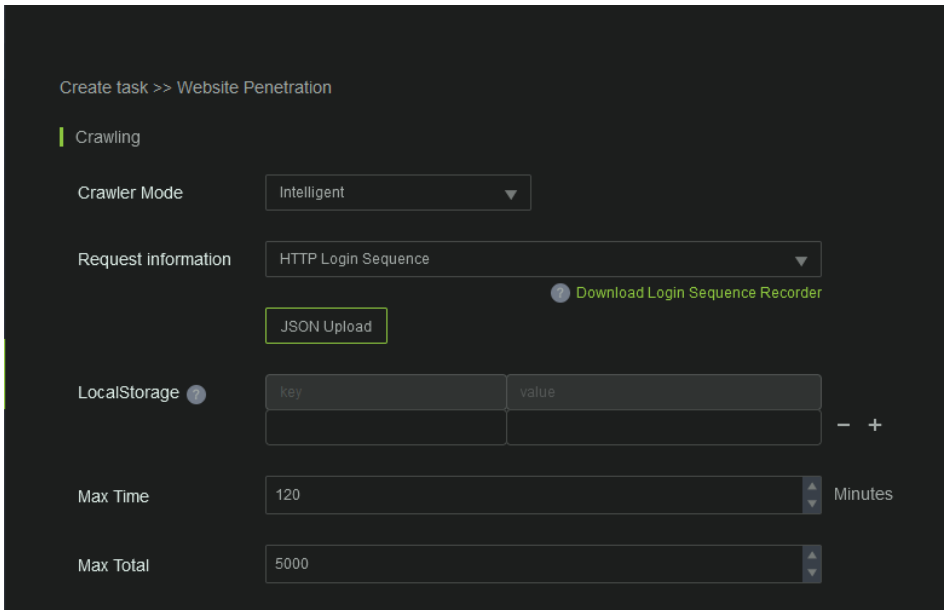
1. Open your browser (Firefox is recommended), go to the certificate settings, and import the certificate downloaded from RidgeBot.
2. Go to the **Preference > Network Configuration**, and then manually configure the Proxy Server IP and port from RidgeBot's settings.
3. Once the browser proxy is configured, open a new tab in the browser, go to the target website and click on the webpages to record the website Attack Surfaces.

Web Login Sequence Recorder

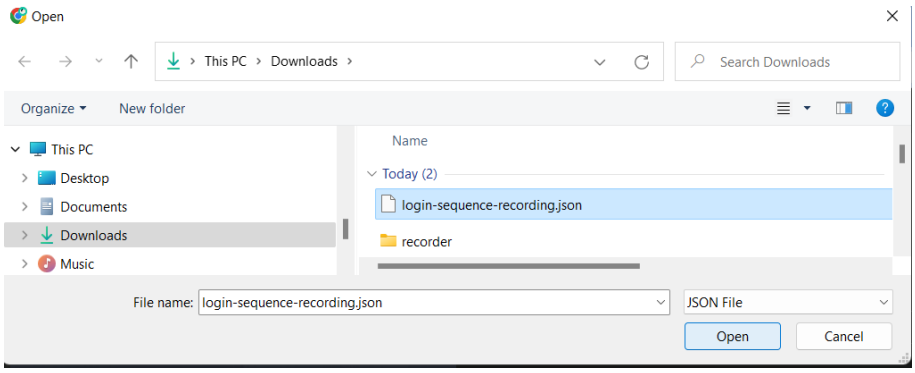
RidgeBot supports an alternative method to by-pass web login. Instead of using Smart Crawler + Proxy mode, user can use the web login sequence recorder in the **Chrome** browser to record the web login sequences and then export the output as a "JSON" file. RidgeBot can playback the recorded login sequence to access the website assuming the token or session cookie has not expired.

In a Website scenario task's Information Recon, user can select "HTTP Login Sequence" in the Request Information pull down menu. Click on the JSON Upload button to upload the JSON file.

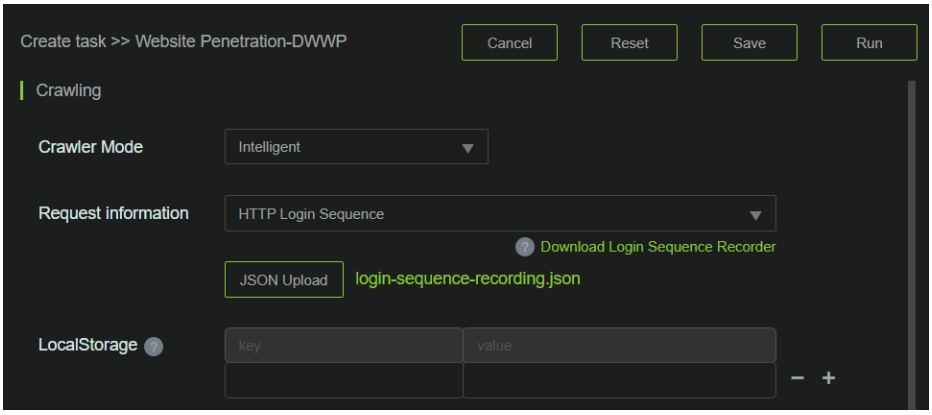




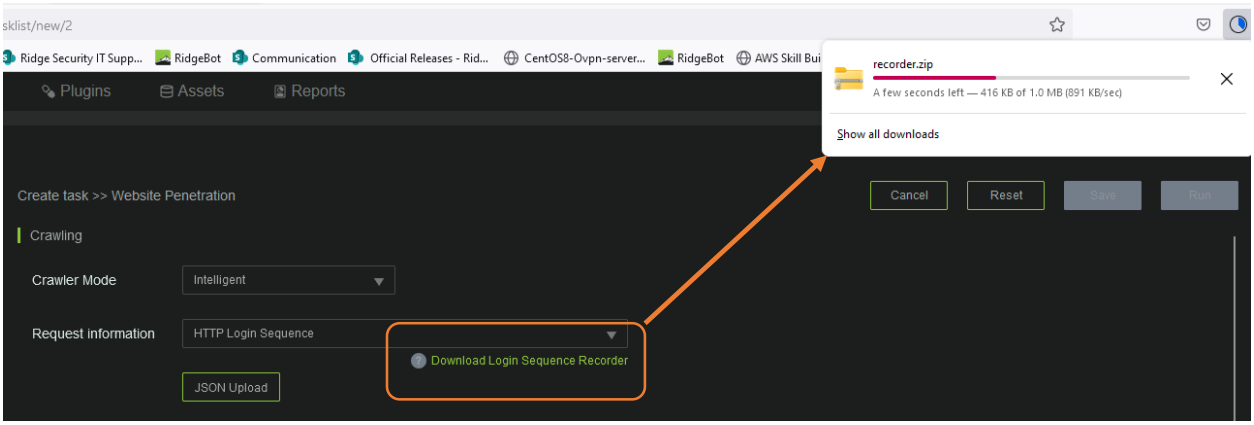
Click on the "JSON Upload" and open the "login-sequence-recording.json" file



Uploaded sequence login file as shown

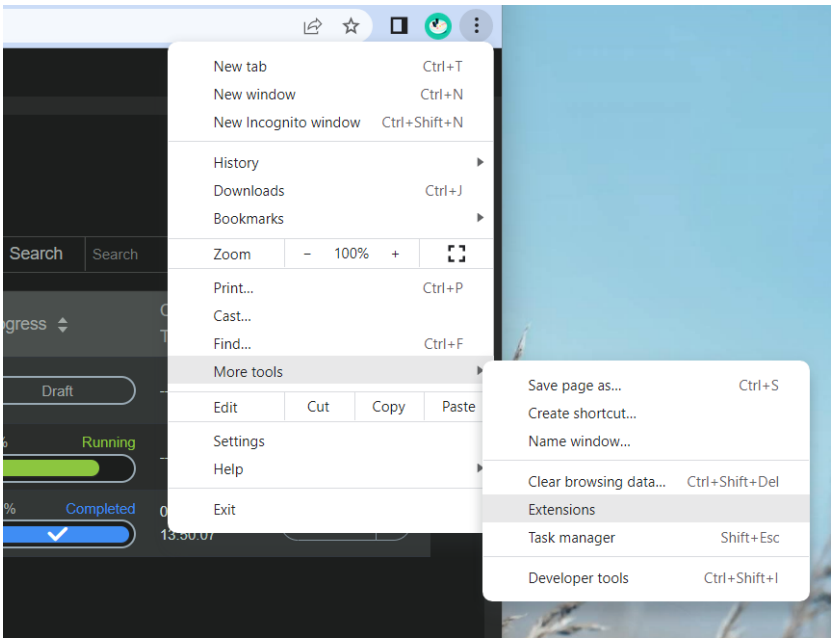


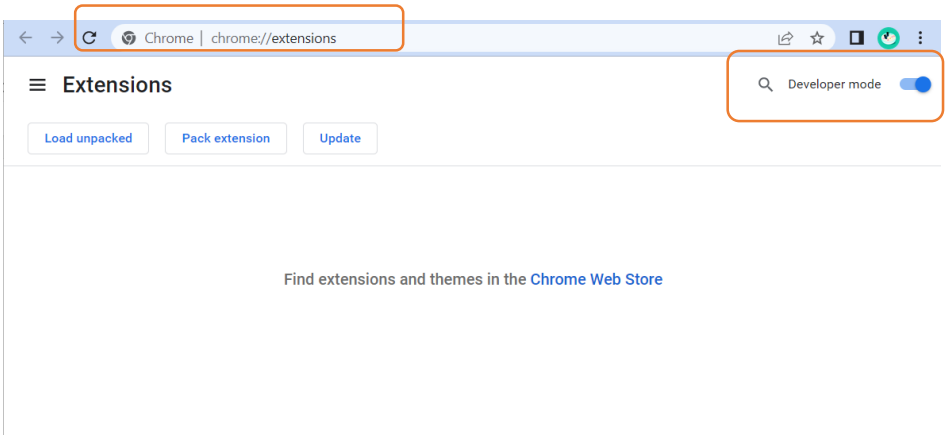
How to install and run the Login Sequence Recorder

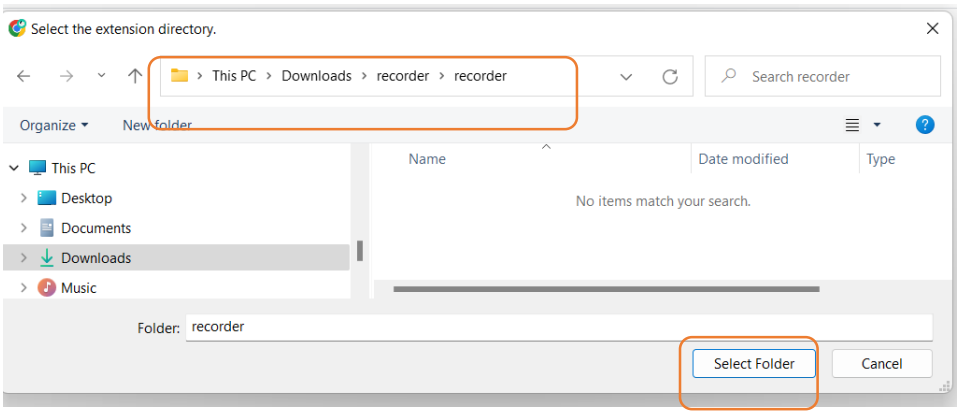


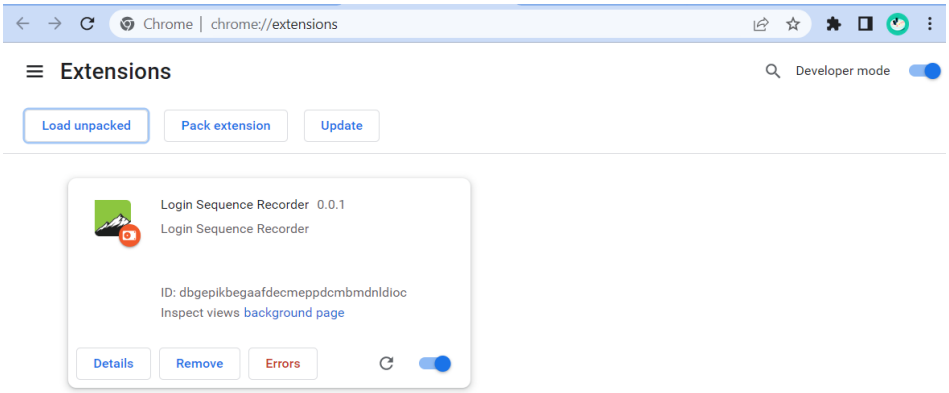
Click on the "Download Login Sequence Recorder" to add the recorder plugin

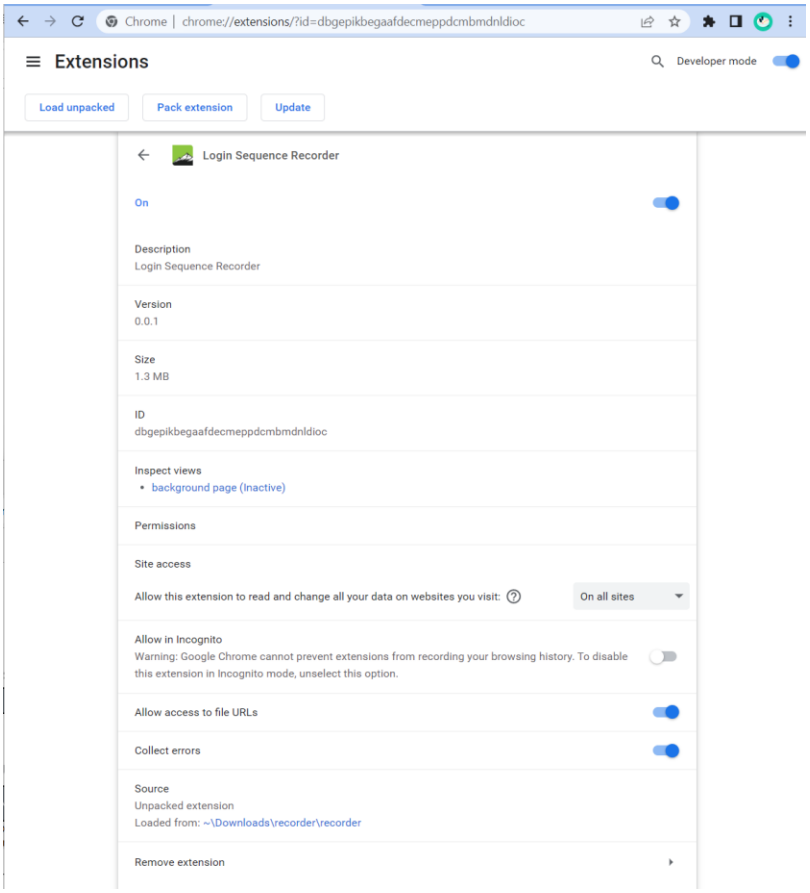
1) Unzip the recorder.zip file to extract the recorder folder
2) Open a chrome browser and go to the extension page (chrome://extensions) and enable the "Developer Mode"
3) Click on the Drag and drop the extracted folder into the page or click "Load Extracted Extensions" to add them.





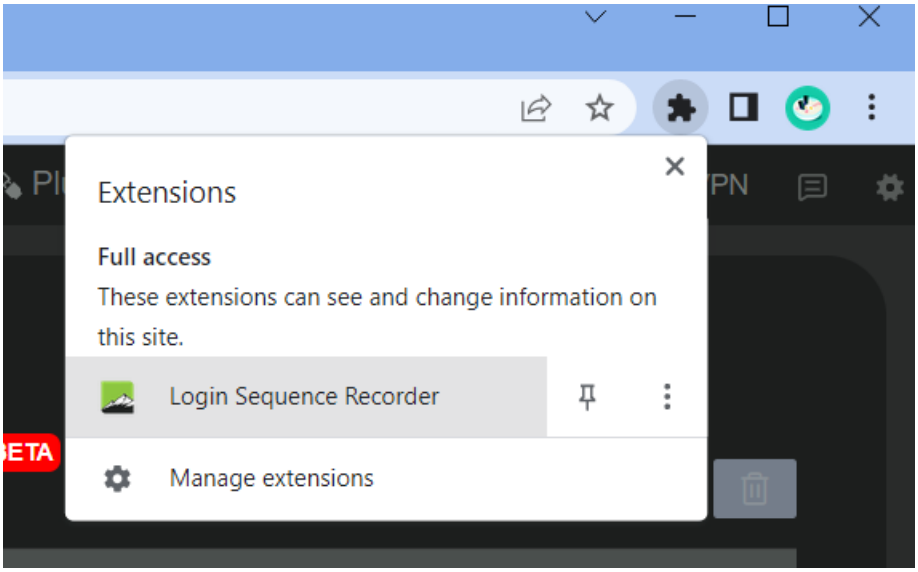

Select the extension directory.
This PC
Downloads
recorder
recorder
Search recorder
Organize
New folder
This PC
Desktop
Documents
Downloads
Music
Name
Date modified
Type
No items match your search.
Folder:
recorder
Select Folder
Cancel


Chrome | chrome://extensions
Extensions
Developer mode
Load unpacked
Pack extension
Update
Login Sequence Recorder 0.0.1
Login Sequence Recorder
ID: dbgepikbegaafdecmeppdcmbmdnldioc
Inspect views background page
Details
Remove
Errors

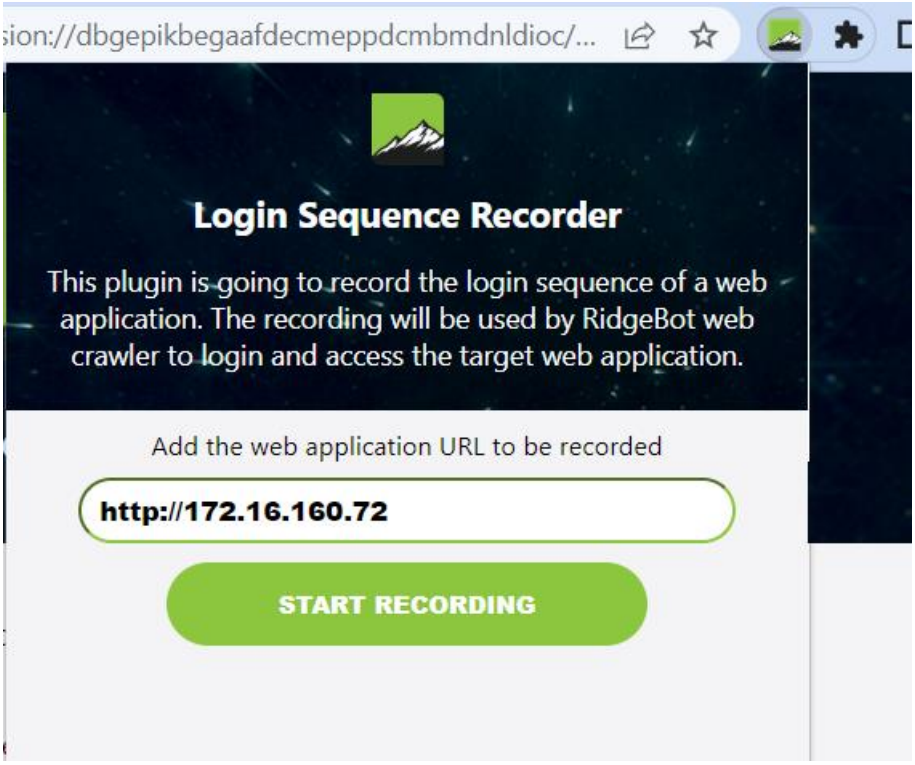


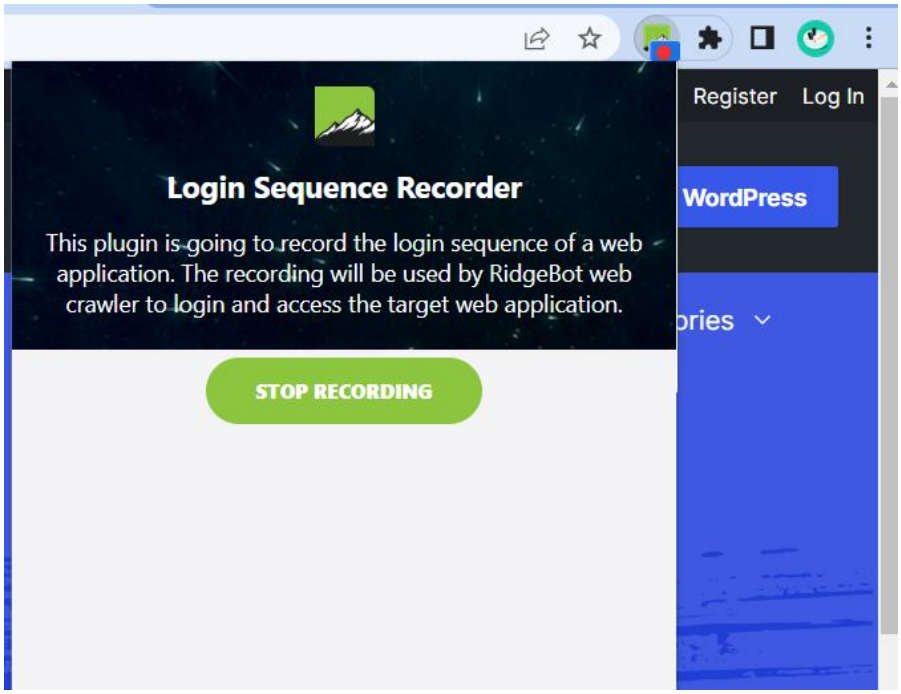
To run the recorder

Click on the extension icon on the chrome browser and select the Login Sequence Recorder

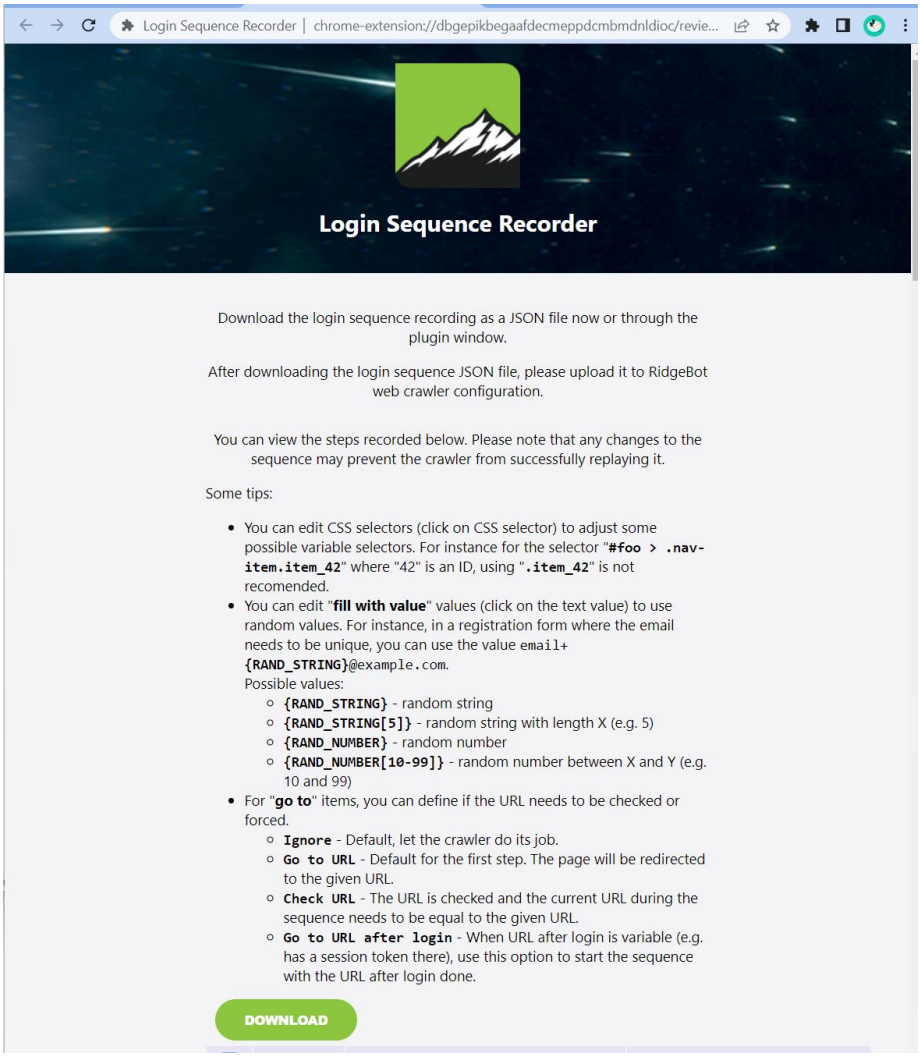


Input the URL in the Recorder and Click on "Start Recording" button. When finished, go to the Login sequence recorder and click on the "Stop Recording" button





Click on Download to download the JSON file.



3rd Party Scanning Result Validation

You can use RidgeBot to validate a scan result from 3rd party tools. As of version 4.2.2, user can import the following scan result:

- **Nessus Pro**
- **Nex**pose Pro

and have RidgeBot run a Penetration Test on the same target(s) and then show the combined results in its report. The RidgeBot report is only available in a .csv format. RidgeBot inserts two additional columns to the .csv file: **RidgeBot Discovered** and **RidgeBot Exploited**.

- **RidgeBot Discovered**: This is a new vulnerability discovered by RidgeBot.
- **RidgeBot Exploited**: This is a vulnerability exploited by RidgeBot.

To run a RidgeBot test and issue a combined report, follow these steps:

1. Generate 3rd party scan result:

- For Nessus Pro, enable the following parameters when creating a CSV Nessus report.

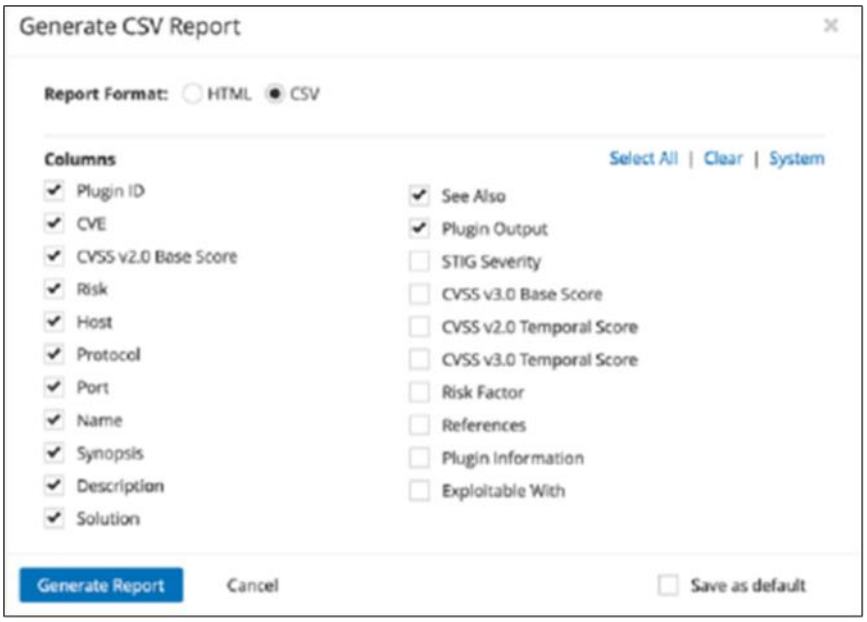
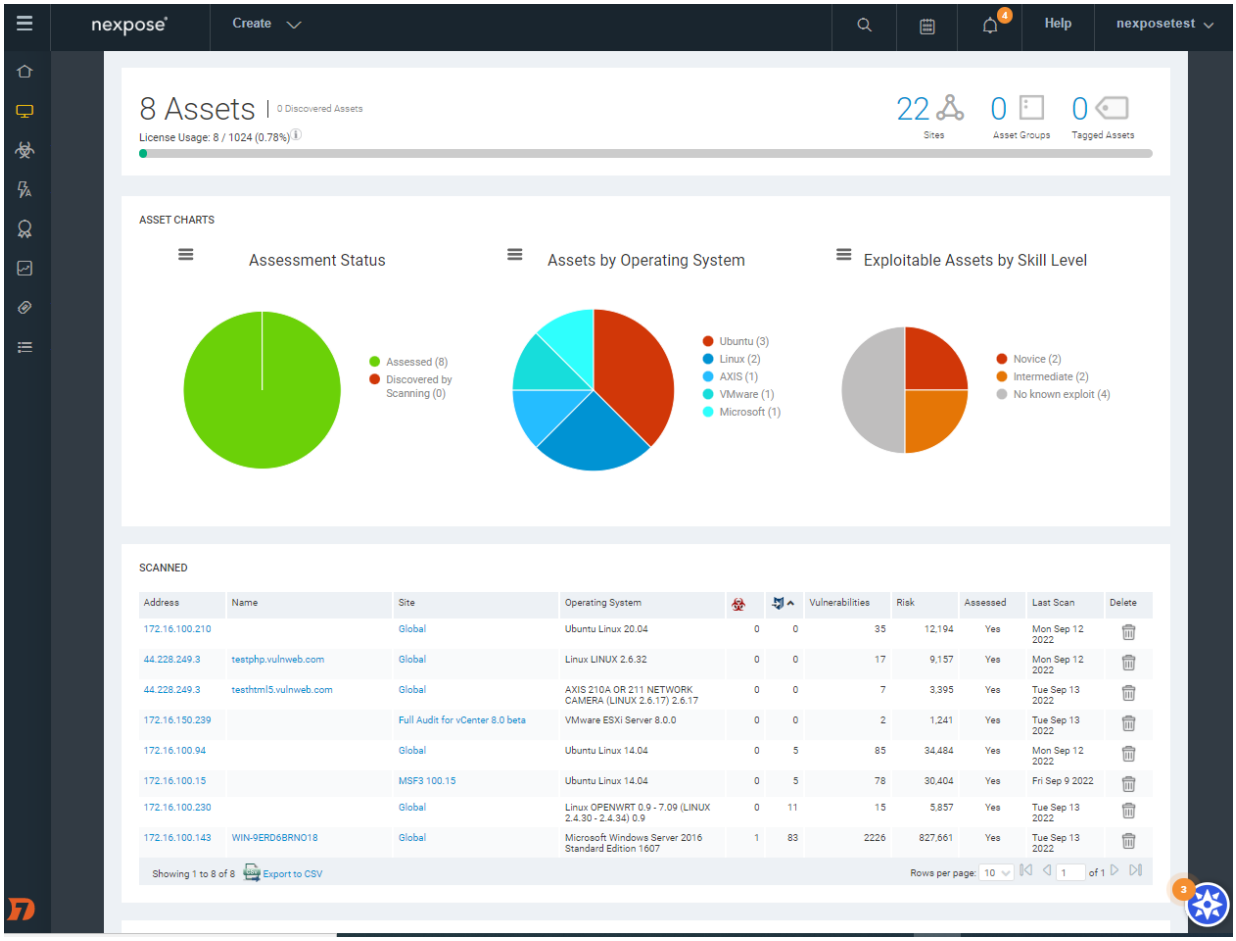
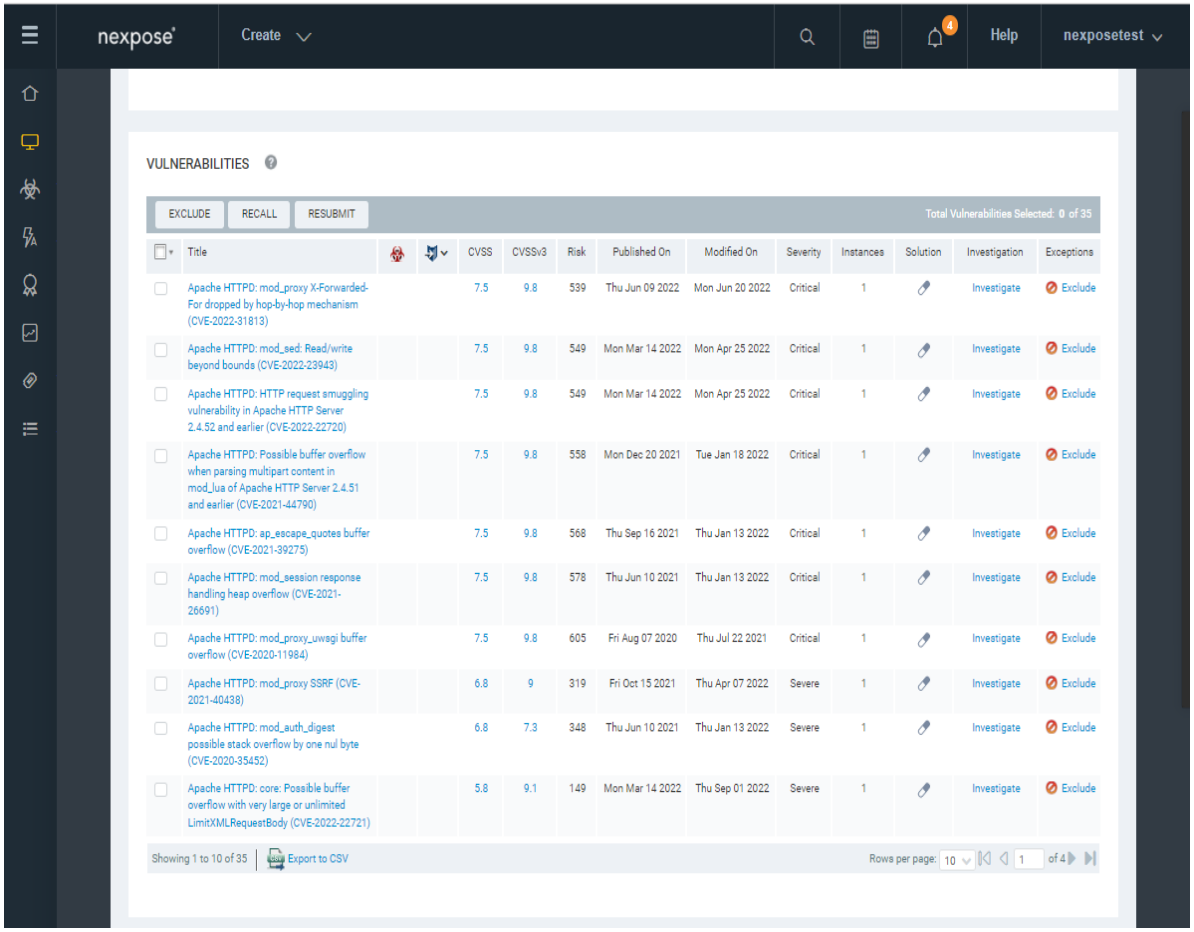


Figure 96: Generation Parameters in a Nessus CSV Report

- For Nexpose Pro, Click the "Assets" tab and browse to the "Scanned" table.



Click the IP address of the selected asset in "Scanned" table



Click the "Export to CSV" to download the Vulnerability List in CSV format.

2. Create a RidgeBot task to do a 3rd party scan result validation scenario.
3. In the "Quick Configuration", import the report into RidgeBot by selecting "Nessus" or "Nexpose", then click "Import Nessus(or Nexpose) Report". RidgeBot automatically uses the targets from the report as the Attack Targets. For Nexpose user needs to configure the target(host) IP manually as Nexpose's "Asset Vulnerability List Export" report doesn't include target IP address information,

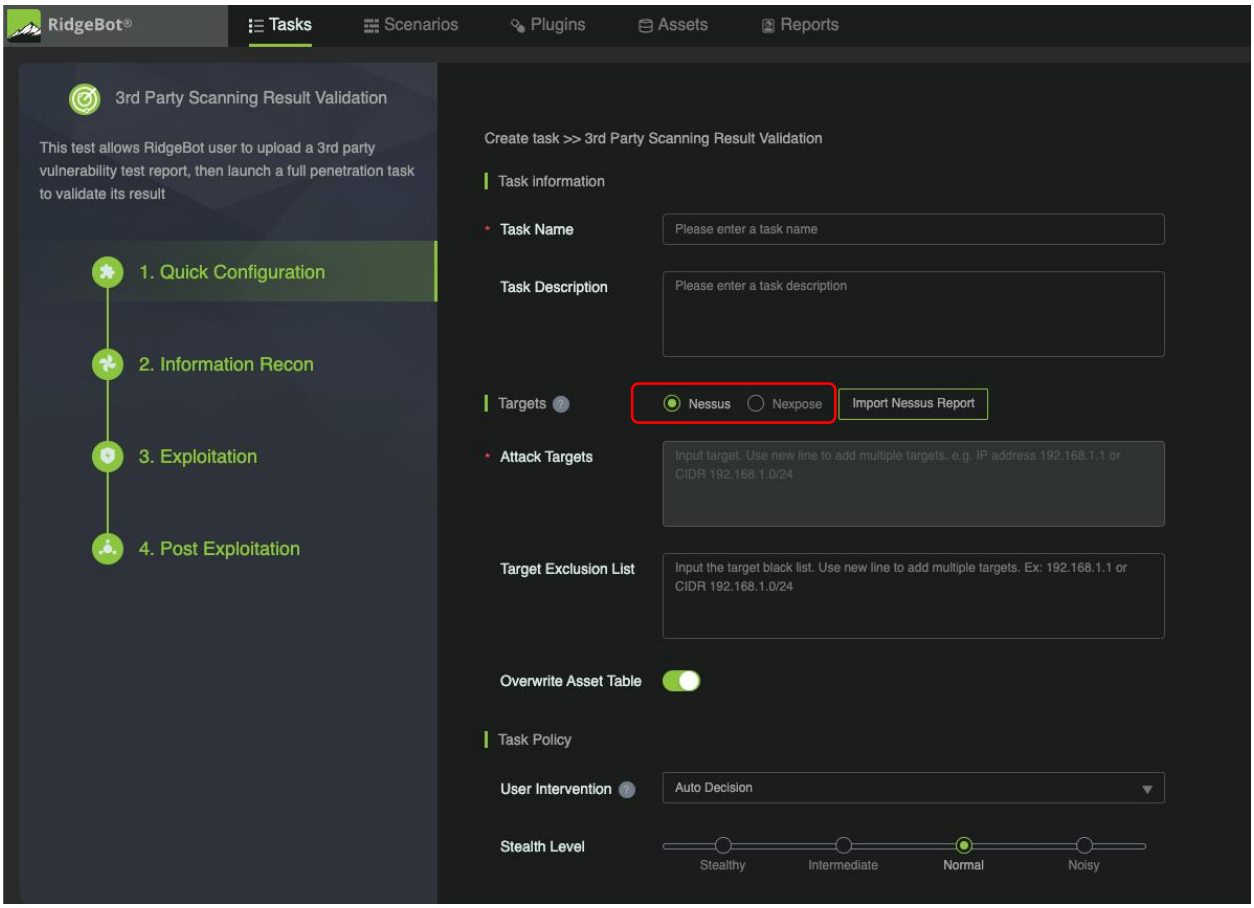


Figure 97: Import 3rd Party Report to Define RidgeBot Task Targets

4. Run the RidgeBot task.

ACE: Data Exfiltration

An ACE data exfiltration scenario simulates an unauthorized data transfer by the Botlet from the host target. When you create a task, it must upload a sensitive data file as part of the task configuration to the targets (as defined in the Assets host list).

You must define a sensitive data file to be uploaded for each data type using any of these formats: .csv, .txt, .pdf, .docx or .xlsx. RidgeBot does not require the data type to be in any specific format. The Botlet tries different tactics and techniques to send the uploaded "sensitive data file(s)" to RidgeBot.

If RidgeBot is able to match the file received to the sensitive data file using a particular script, then it reports the script in the "un-blocked" category.

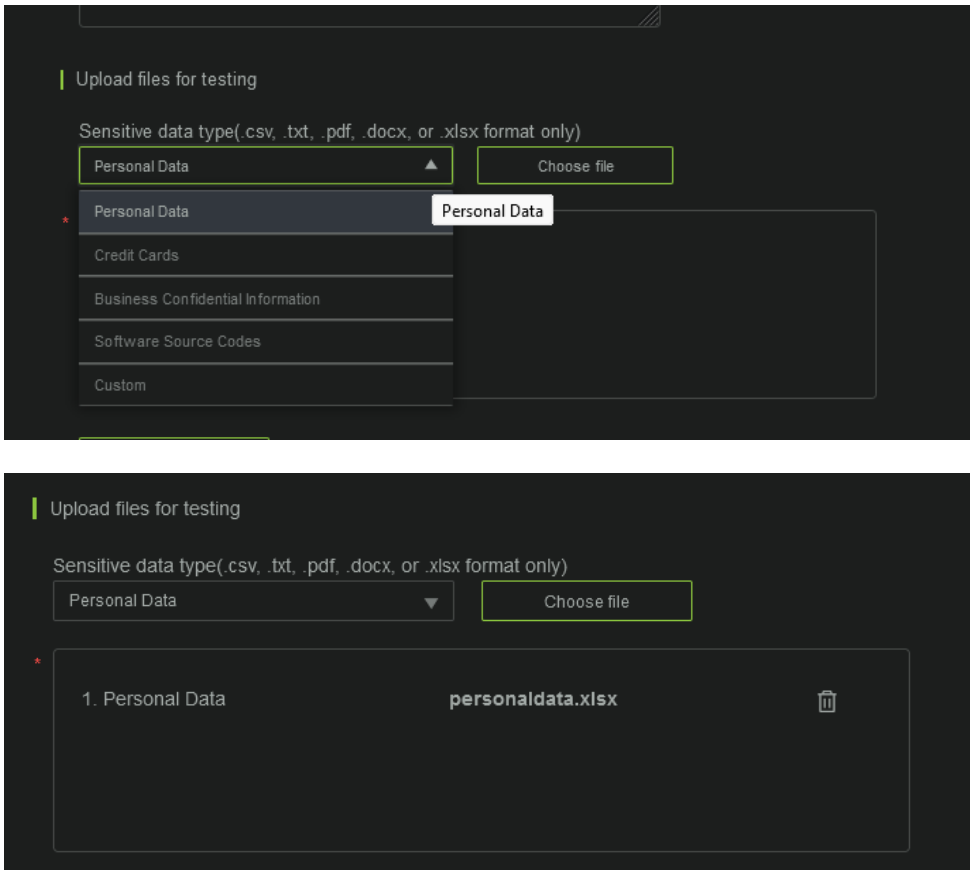


Figure 98: Upload Sensitive Data File(s) for RidgeBot Test

An example of a credit card .xlsx sensitive data file format is shown below.

	A	B	C	D	E
1	SSN	First	Last	Credit Card	Code
2	123-45-6789	aa	bbbb	1234567890121230	123
3					

Figure 99: Example of a Sensitive Data File for Upload

Chapter 9 Message Center

The **Message Center** shows messages from the RidgeBot system. System messages inform you of changes in the system. This chapter discusses **Message Center** operations.

This chapter has the following sections:

Entering the Message Center

On the righthand side of the **Navigation Bar**, mouse over the message icon  , and then click **Read More** to enter the Message Center.

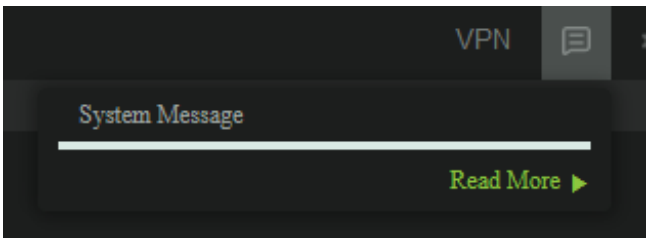


Figure 100: Message Center Pop-up Dialog Box

Operating on Messages

The **Message Center** displays messages in tables.

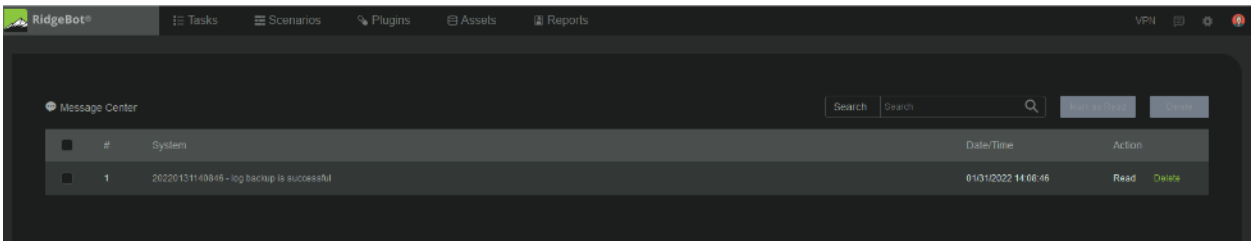


Figure 101: Message Center

To search for a certain message, enter a keyword in the search text box and then click the search icon.

To mark one message as read, click **Read** in the **Action** column of the message.

To delete a message, click **Delete** in the **Action** column of the message.

To mark multiple messages as read, select the checkboxes of the messages in the message table, and then click the **Mark as Read** button at the top right of the screen.

To delete multiple messages, select the checkboxes of the messages in the message table, and then click the **Delete** button at the top right of the screen.

Warning message

Botvassd process is down. When this warning message is shown in the message center, user can take action to recover the botvassd service using the recover-service command in RidgeBot management console

Chapter 10 System Settings

RidgeBot System Settings are accessed by mousing over, or clicking, the gear wheel at the top right of the **Navigation Bar** and then selecting an item from the drop-down box. Each option is discussed in this chapter.

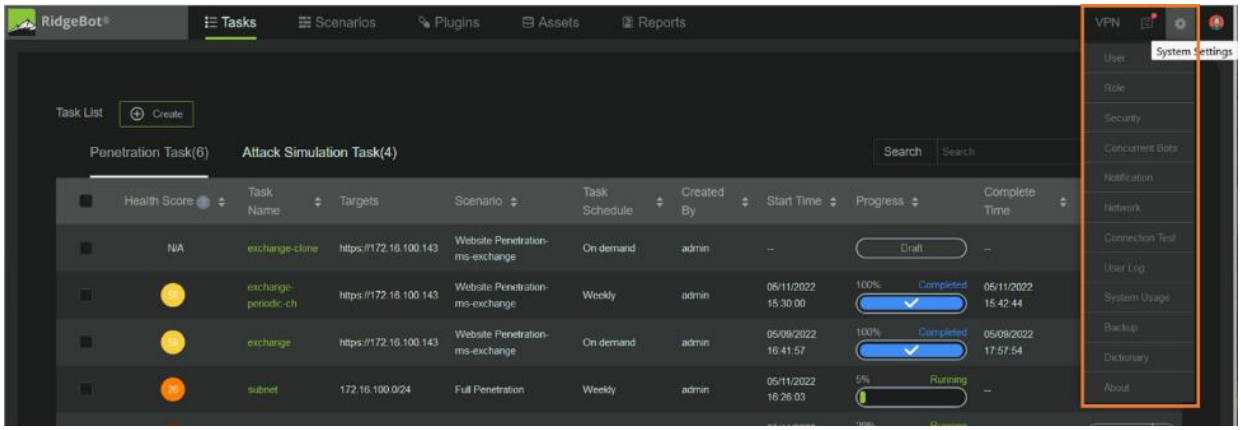


Figure 102: Navigation Bar Access to System Settings

This chapter has the following sections:

- About: Managing Your License
- About Information
- Software and Plugin Library Upgrades

Users

A user has an account and logs into the RidgeBot system. The user will have access to various feature based on the account role. User privileges—pages that the user can see and manage—are granted by assigning a role to the user. An **admin** user has full system access and can create, edit, delete, or search user account credentials (admin or user).

To add a user, follow these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **User** from the drop-down menu. The System Settings page is displayed.
2. Click the **Add user** button to display the **Add user** dialog box.
3. Enter values for the options on the page.

Notes:

- The password specified for the user must comply with the password strength rules. For more information about the password strength configuration, see Chapter 9 Security Settings.
- The **Role** option lists all the roles that have been created in the system for you to choose from.

4. Click **Save**. The specified user is created and listed in the user list.

To modify a user, select the checkbox next to the user you want to modify, then click **Modify** in the **Action** column. Change the desired values, and then click **Save**.

To delete a user, select the checkbox next to the user you want to delete, then click **Delete** in the **Action** column.

To delete multiple users, select the checkboxes next to all the users you want to delete, then click the delete button.

To search for a certain user, enter a keyword into the **Search** text box at the upper right corner of the page, 

and then click the search button.

Roles

When you create a user, it must be assigned a role. A role defines which pages a user can see and manage. RidgeBot supports three pre-defined roles, System administrator, Log auditor and Security guard. You can also create your own roles.

To add a role, follow these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **Role** from the drop-down menu. The System Settings page is displayed.
2. Click the **Add role** button to display the **Add role** dialog box.
3. Enter a name for the role in the **Role Name** box.
4. Select the **view** or **manage** checkboxes of the pages this user may access. Choose **Select All** to select/deselect all options.
5. Click **Save**. The specified role is created and listed in the role list.

To change the pages authorized for a role, select the checkbox next to the role you want to modify, click **Authorization** in the **Action** column, then change the values, and click **Save**.

To delete a role, select the checkbox next to the role you want to delete, then click **Delete** in the **Action** column.

To delete multiple roles, select the checkboxes next to all the roles you want to delete, then click the delete button.

To search for a certain role, enter a keyword into the **Search** text box at the upper right corner of the page, 

and then click the search button.

Roles and Hierarchy

Admin user – this is a super user that has full access privileged with visibility to every task in the system

Administrator – full access privileged, but can only see self-created tasks and other tasks created by non-administrators i.e. Security guard or other user defined role.

Security guard and other user created roles – feature access as defined by the role. User only has accessed to the self-created tasks.

Security Settings

The System Security settings refer to the password strength and other login account related configuration.

By default, the password strength configuration is disabled, and you can specify the password for system users to suit your needs. To increase the security of the system, you can specify password strength rules. To configure password strength, follow these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **Security** from the drop-down menu. The System Settings page is displayed.
2. Under the **Password Security** tab, enable the settings by opening the switch and then specifying values for each option.
3. Click **Save**.

To modify account login-related configurations, click the **Account Security** tab, then specify values for the options:

- **Timeout**: If the currently logged-in user has been inactive for the duration of time specified here, the user is automatically logged off from the system.
- **Number of Attempts**: The maximum number of unsuccessful user login attempts. If the number of attempts specified by this parameter is exceeded, the user is locked out for the duration of time defined by the **Lockout Duration** option.
- **Lockout Duration**: The duration of time that a user—who has tried to login unsuccessfully more than the number of times specified by the **Number of Attempts** option—is locked out from accessing the system.

You can restrict the RidgeBot GUI to be accessed from only a specific list of IP addresses. To build a whitelist of allowed IP address entries, click the **IP Whitelist** tab, then click the **Add** button to display the **Add Authorized IP** dialog box. Enter the whitelisted IP addresses into the text box, one address per line, then click **Save.**

Concurrent Bots: Configuring System Work Capacity

You can limit the maximum number of processes and the maximum number of concurrent threads of each process in the system. The maximum number of tasks the system can run simultaneously is set in the Concurrent Bots setting page.

To configure the system work capacity, follow these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **Concurrent Bots** from the drop-down menu. The Concurrent Bots setting page is displayed.
2. Enter a number into the field or click the up/down arrows buttons to adjust the numbers. The default value is 100.
3. Click the **Save** button.
4. Restart the system.

A larger number of Concurrent Bots shortens the duration of a task's execution. The maximum of concurrent bots is correlated to the allocated vCPU cores.

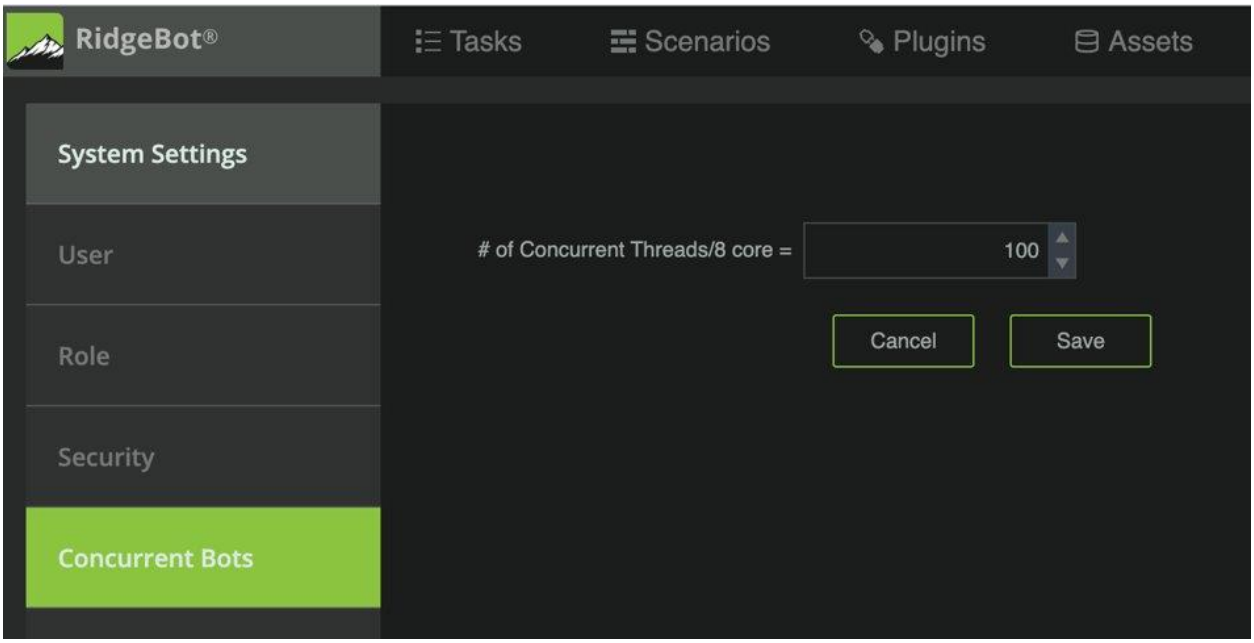


Figure 103: Concurrent Bot Configuration

Notes:

- Ensure that there is no task actively running when you modify the number of Concurrent Bots.

- Each thread may consume approximate 62MB of memory. Make sure the total memory consumption do not exceeds the number of memory available.

Notification: Email and Syslog

Email

You can configure RidgeBot to send email notifications to a set of email addresses by following these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **Notification** from the drop-down menu, and then select the **Email** tab.
2. Enter the values of each parameter according to your own email server settings.
3. Click **Save**.

After the configuration is saved, you can test the configuration by clicking on **Test** and looking for a **Success** pop-up confirmation. A confirmation email with a "This is a test message" is sent to each of the receivers listed in the configuration.

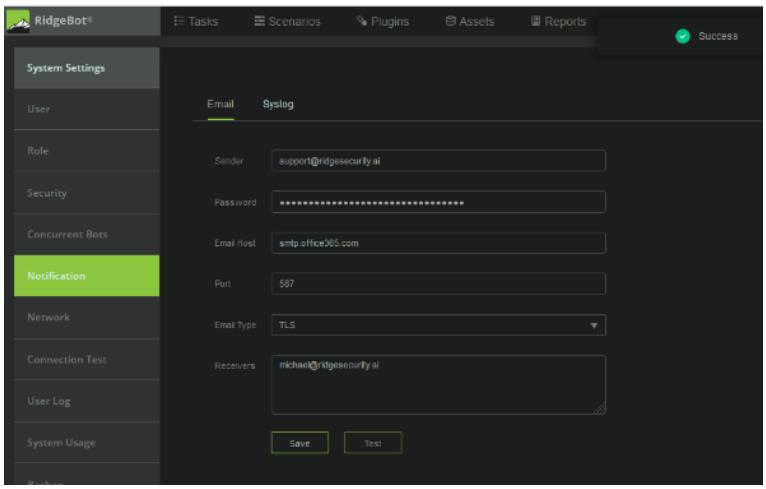


Figure 104: Example Email Configuration with a Success Acknowledgement

Note: RidgeBot only supports the Outlook and Office365 SMTP email hosts. The Yahoo and Google email hosts, as well as mail hosts with 2FA authentication are not supported

Depending on your account configuration, Microsoft may block the account if there are too many messages sent by RidgeBot

Syslog

RidgeBot supports Syslog version 3.3 and later. RidgeBot syslog messages comply with the Common Event Format (CEF) specifications and can be used for SIEM or other SOC integration.

RidgeBot supports the following syslog messages:

1. Audit Log
    - User Login/Logout, User Login Failed, Add/Update Users, System Settings Changed, System Shutdown, and System Backup Complete.
2. System Health Log
    - Resource limit exceeded, Service unavailable, License expiry (future), License has expired, and Quota exceeds limit.
3. Task Information and Status Log
    - Task name, target IP
    - Task starts running, Task is completed, Task is paused, and Task is restarted.
4. Risk and Vulnerability

Syslog message format:

- Header: timestamp host (host is the message source IP address)
- Message: CEF: 0|RidgeSecurity|RidgeBot|ver|ID|Name|Severity|Extension

To configure Syslog options, select the **Syslog** tab and enter values for the syslog server parameters and click the **Enable** button. Then click **Save**.

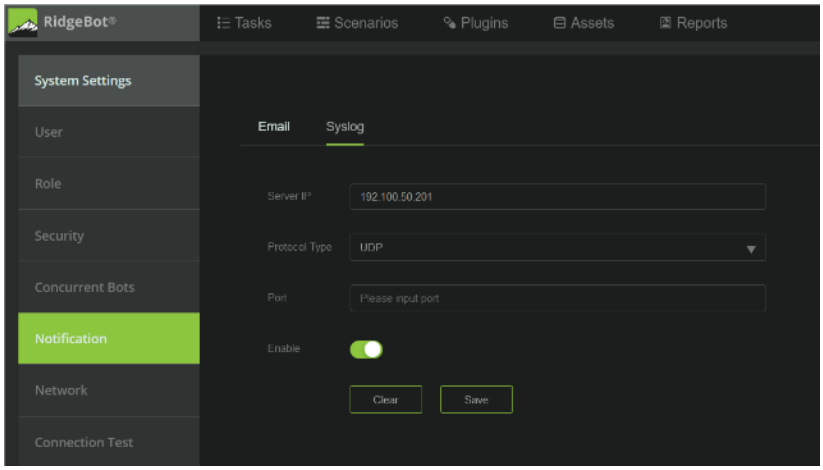


Figure 105: Configuring Syslog Settings

Example of syslog messages in /var/log from a Linux rsyslog server is shown below.

```
Jul 22 00:30:33 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|1004|system settings change|3|act=admin System Settings Have Changed: update syslog suser=admin
Jul 22 00:35:46 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|3003|Task is paused|3|taskName=test AS
Jul 22 00:35:55 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|3001|Task starts running|3|taskName=test AS
Jul 22 00:36:34 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|3005|Task is stopped|4|taskName=test AS
Jul 22 00:37:13 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|3004|Task is restarted|3|taskName=msf-75
Jul 22 00:37:13 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|3007|Task report is generated|3|reportName=test AS_2022-07-22-00:36:59
Jul 22 00:44:20 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|4011|High severity vulnerability is detected|8|pt_test=Task=msf-75 NodeIP=172.16.160.75 Target=http://172.16.160.75/phpmyadmin/
Jul 22 00:44:21 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|4001|Critical business risk is exploited|9|pt_test=Task=msf-75 NodeIP=172.16.160.75 RiskType=Credential Disclosure RiskName=Backend Weak Password Target=http://172.16.160.
Jul 22 00:44:57 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|4031|Low severity vulnerability is detected|6|pt_test=Task=msf-75 NodeIP=172.16.160.75 Target=http://172.16.160.75/
Jul 22 00:47:12 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|4041|Informational severity vulnerability is detected|5|pt_test=Task=msf-75 NodeIP=172.16.160.75 Target=http://172.16.160.75/5VpgSrEjnp.aspx
Jul 22 00:52:01 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|4011|High severity vulnerability is detected|8|pt_test=Task=msf-75 NodeIP=172.16.160.75 Target=172.16.160.75
Jul 22 00:52:13 172.16.160.45 CEF: 0|RidgeSecurity|RidgeBot|4.0.1|5301|ACE Botlet is online|3|ace_blocked=172.16.160.75 agent is online
```

Figure 106: Example of CEF Syslog Messages

Note: configure the Syslog Server IP, Port and Protocol per your Syslog server setup

Network

Configure RidgeBot's network settings to fit into your network environment.

Configuring Reverse Shell

The reverse shell configuration can be referenced by a task. For more detailed information about the reverse shell configuration, click the **Configuration Help** button.

The Reverse Shell IP should be on the same subnet as the targets. Use the pull-down menu to select the correct interfaces if RidgeBot is set up with multiple network interfaces. Click **Test** to confirm and then **Save**.

Configuring the Network Interfaces

To configure network interfaces, follow these steps:

1. In the **Navigation Bar**, mouse over the **System Settings** icon, and select **Network** from the drop-down menu. The network configuration page appears.
2. Under the **Network Interfaces** tab, specify values for the options to be in line with your network.
3. Click **Save**.

Configuring Routes

To configure the network routes for the RidgeBot system, follow these steps:

1. In the **Navigation Bar**, mouse over the **System Settings** icon, and select **Network** from the drop-down menu, then select **Route** tab.
2. Click the **Add** button to display the **Add Route** dialog box.
3. Specify values for the options to complete the configuration of a route.
4. Click **Save**.

To delete a route, click the **Delete** button in the **Action** column.

As of Version 3.4, the priority of a network route can be changed by selecting the **Up** or **Down** buttons in the Priority column.

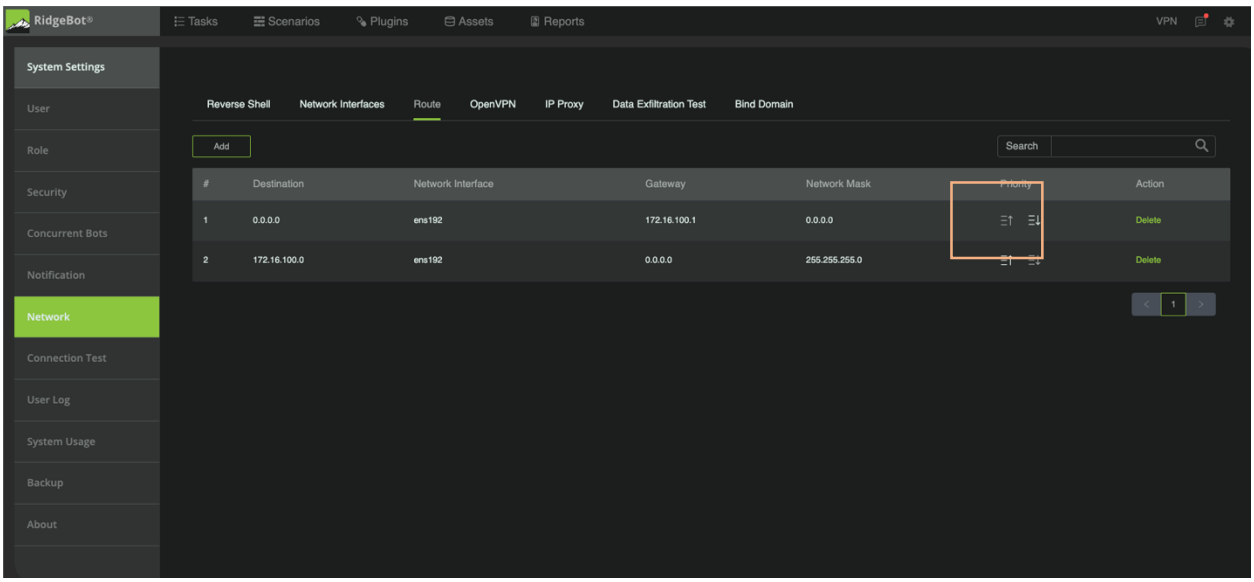


Figure 107: Network Route Configuration Page

Note: RidgeBot management traffic uses the default route. If the priority of the default is changed, your web browser must update its URL to re-establish connection with the RidgeBot GUI.

Configuring a VPN

Use a VPN if RidgeBot is deployed outside the target network. RidgeBot has a built-in OpenVPN client and only supports OpenVPN with a domain name or an IP address with username and no password as options.

To install the OpenVPN configuration, follow these steps:

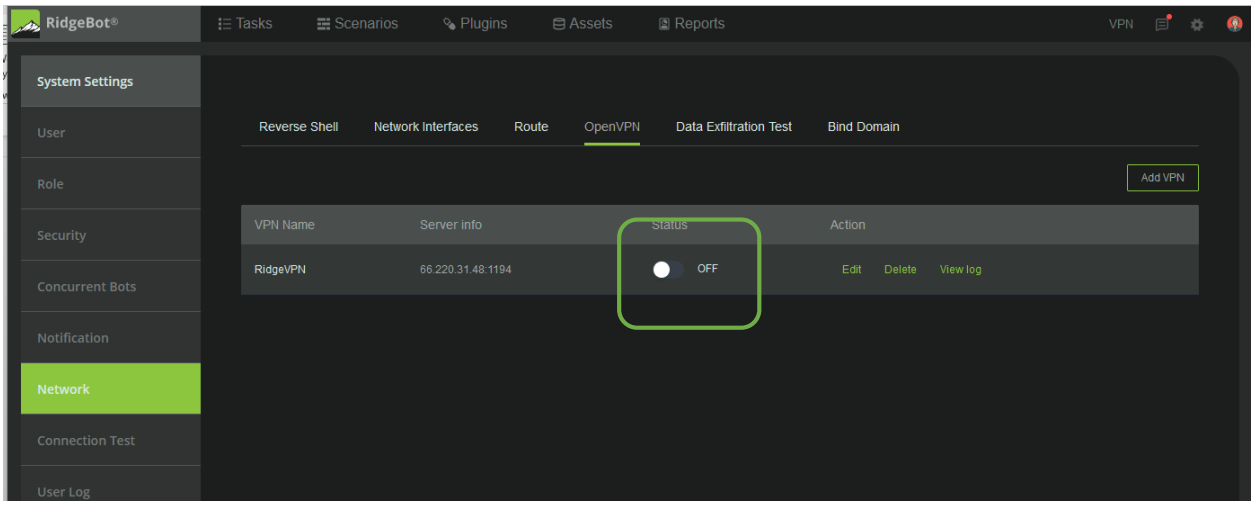
1. On the **Navigation Bar**, select **VPN**. The network configuration page is displayed.
2. Click the **OpenVPN** tab.
3. Click the **Add VPN** button to display the **Add VPN** dialog box.
4. Enter a name in the **VPN Name** text box.
5. Click the **Import** link and find the appropriate .ovpn file to upload.
6. If you want to keep your tasks executing while the VPN is disconnected, enable the option **When VPN connection is down, the task is continued**.
7. Click **Save**.

To manage a VPN profile

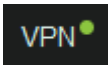
1) Click on **Edit** under Action to edit the select VPN profile
2) Click on **Delete** under Action to remove the select VPN profile

To initiate a OpenVPN connection to the open server

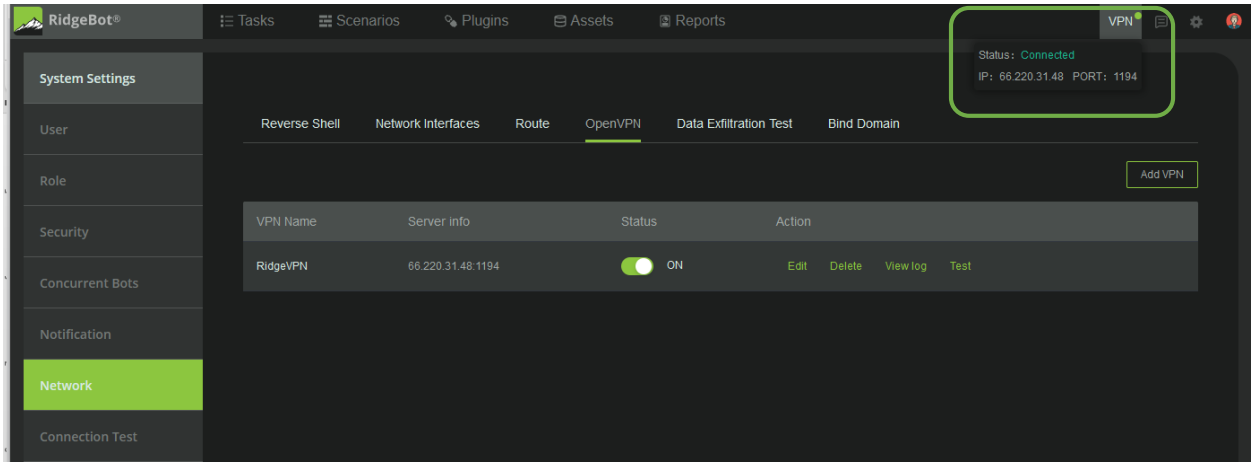
1) Select the VPN name, click on the "**off**" switch on the VPN Status to start the VPN process



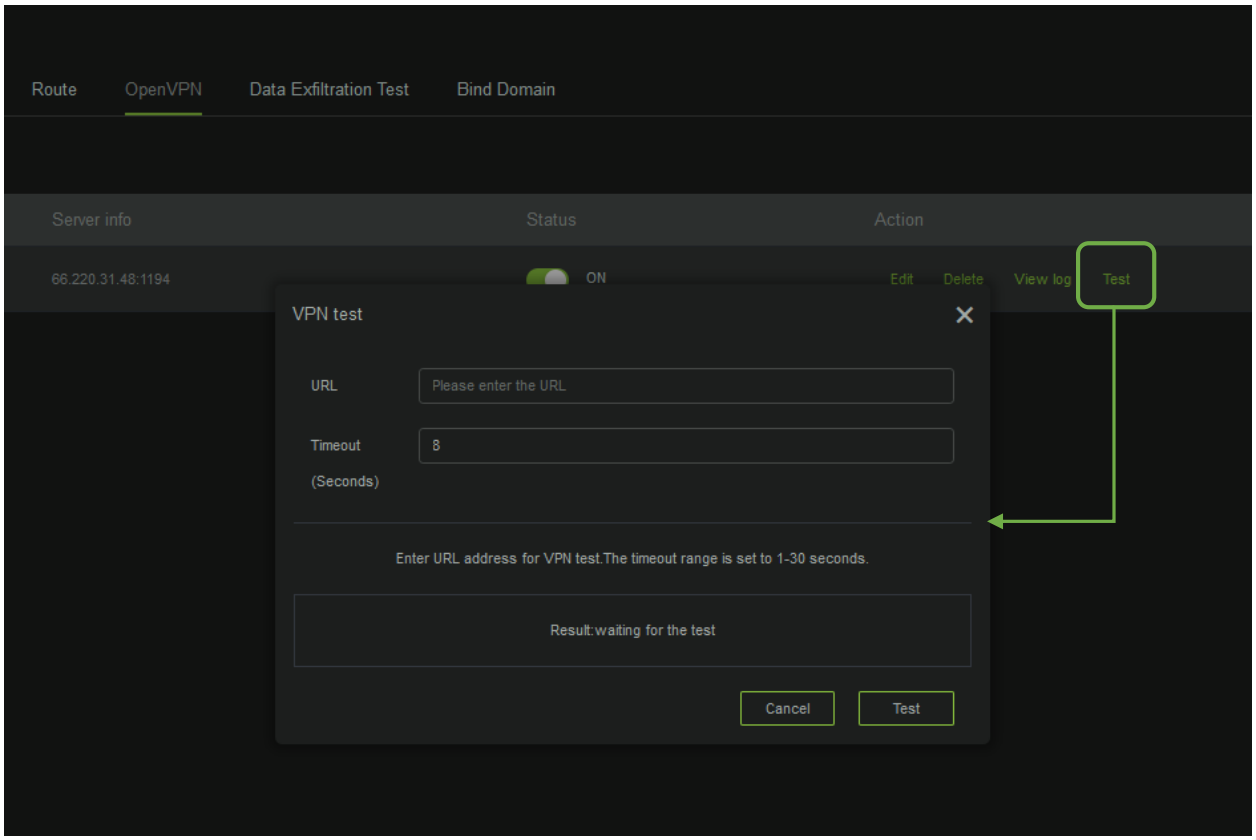
2) VPN switch is ON with the GREEN background when the VPN session is established successfully.

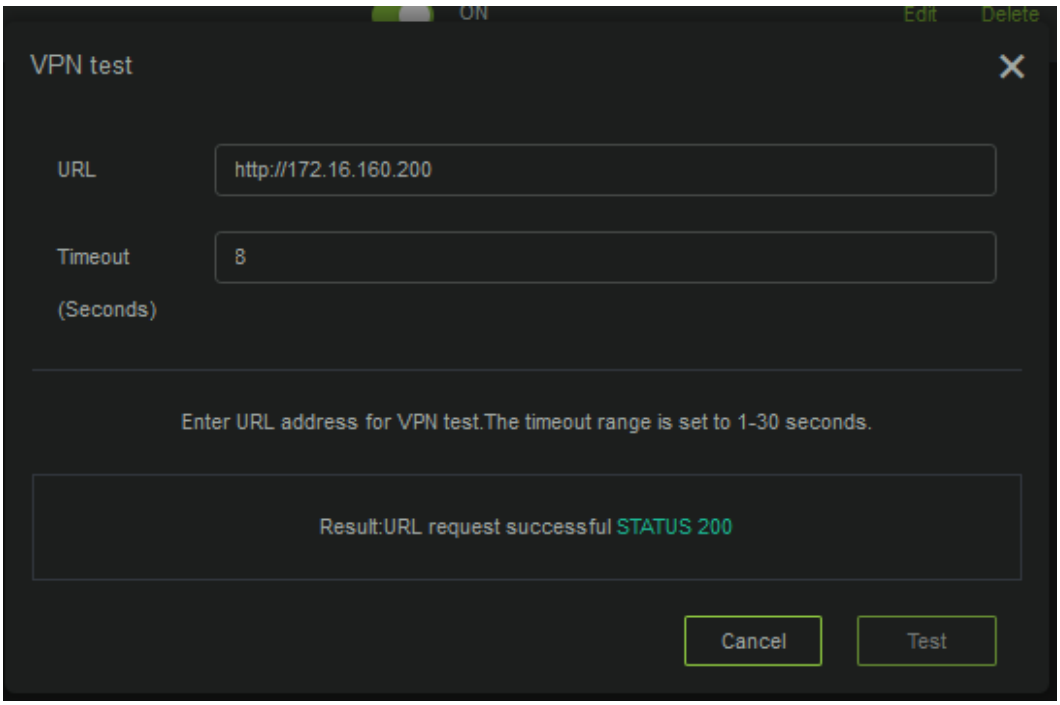
Note: when click on the VPN icon 

in the GUI upper right corner to show the VPN status, IP address and Port

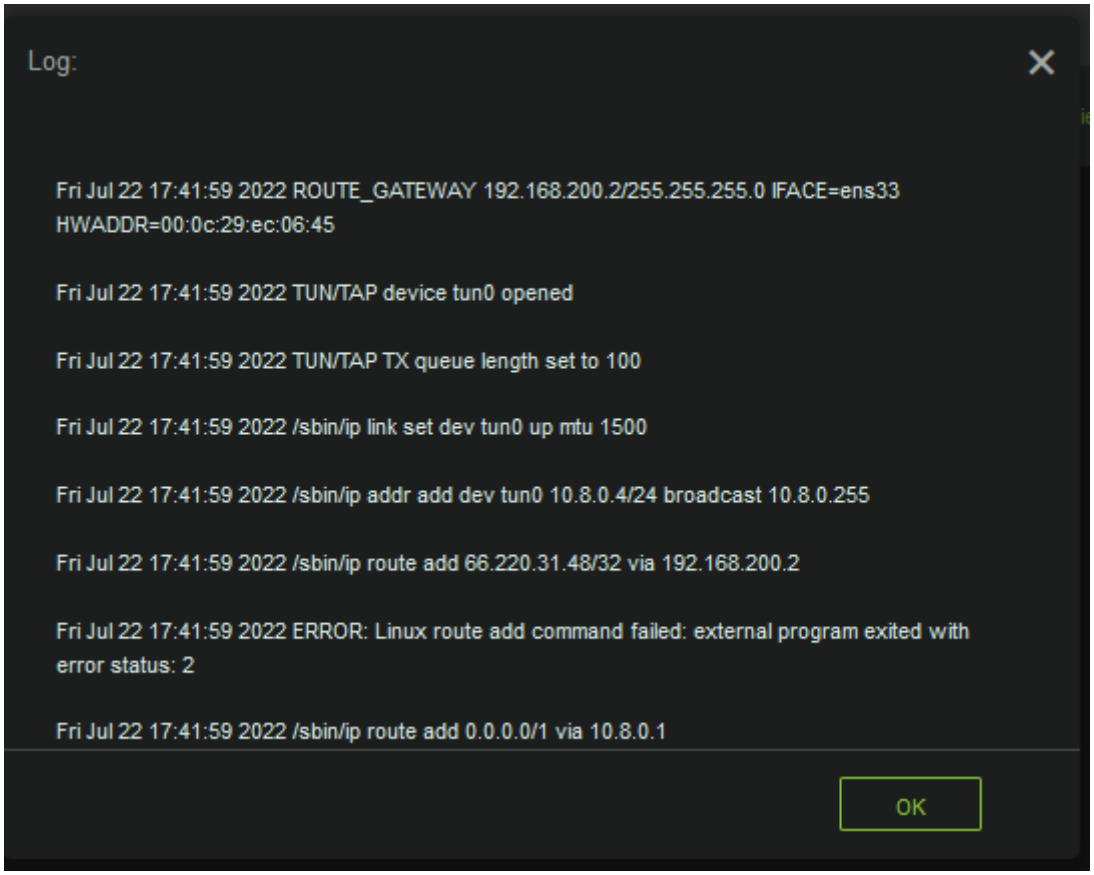


3) To check connectivity of a server behind the OpenVPN server, click on Test in the Action to get a VPN Test pop up dialog box





4) Troubleshooting: click on the View Log in the Action to see the session log



Configure IP Proxy

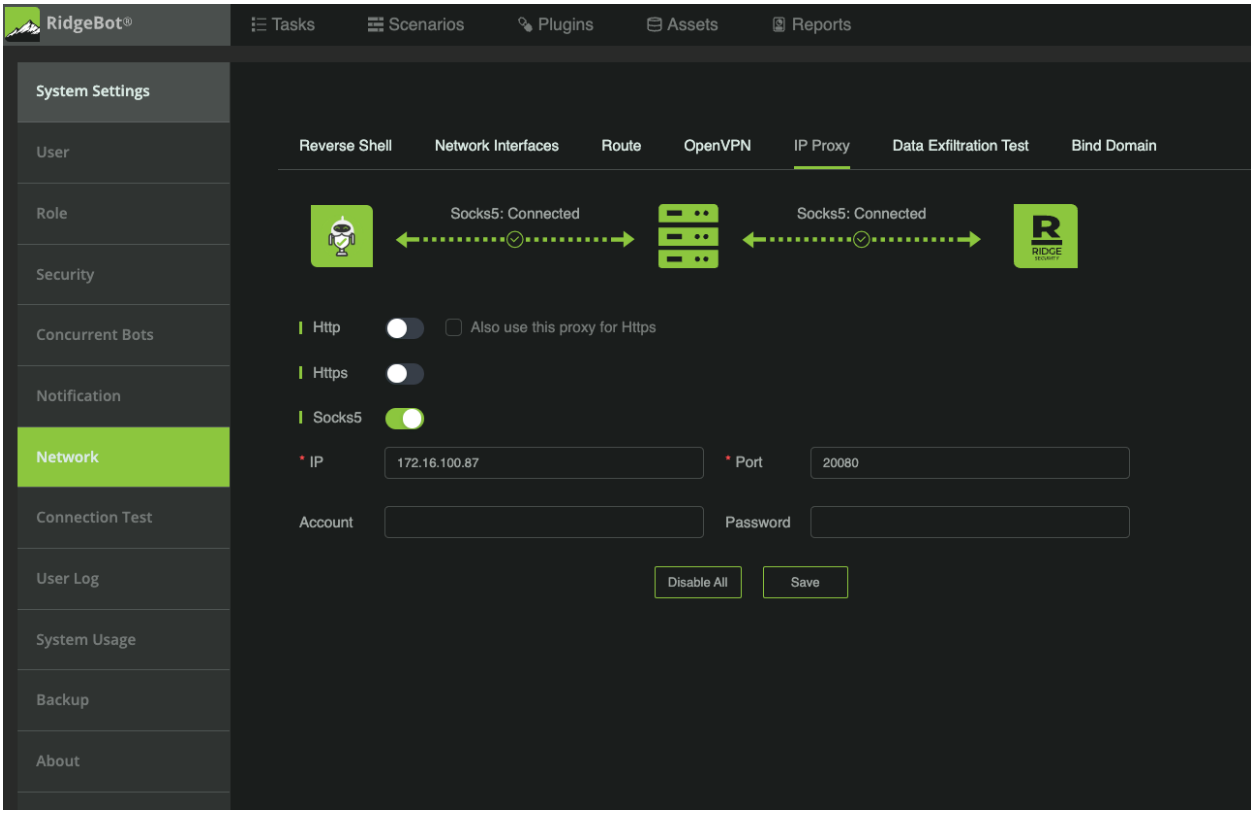
If the RidgeBot is installed inside the company firewall, the user need to setup a proxy for RidgeBot to communicate license server, upgrade server, and integrated services, such as JIRA Cloud and GitLab.

By clicking the IP Proxy tab in Network, user can see the current proxy setup and change the proxy setting. It also shows the connection status of the RidgeBot through the proxy.

The RidgeBot support HTTP, HTTPS, and Socket 5 proxies. The figure below shows the Socket 5 proxy has been setup (was done in management console). User can enable other proxies by slide the switch buttons and input the IP addresses and port numbers of the proxy servers, similar to the ones in the Socket 5 information fields.

HTTP and HTTPS proxy is prioritized over Socket 5 proxy if multiple proxies are enabled and configured.

Click save to save the proxy configuration.



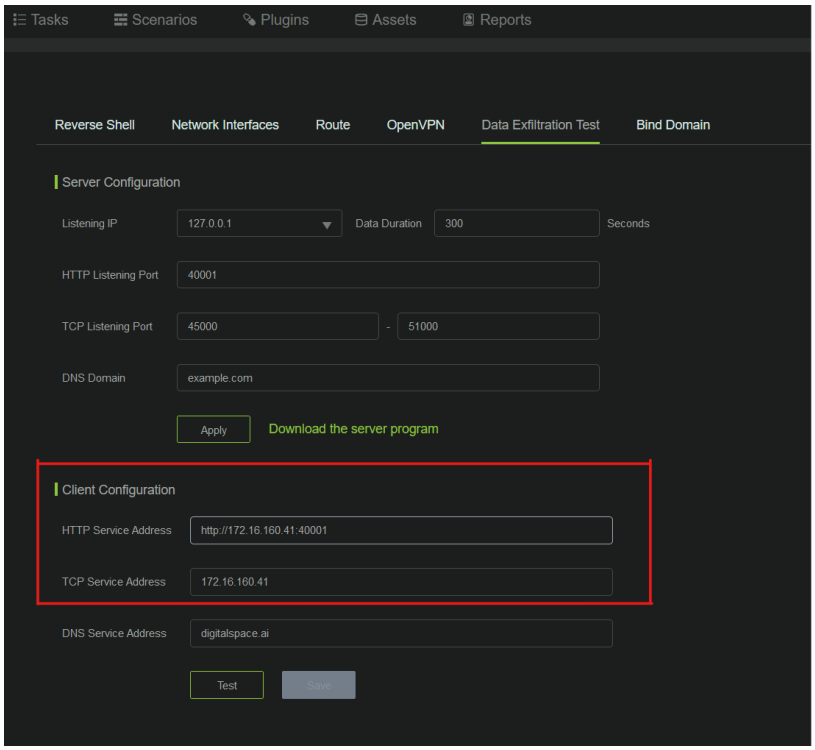
Configuring a Data Exfiltration Test

Data Exfiltration happens when data is extracted from the target machine and moved to another system. In a Data Exfiltration Test RidgeBot uses the exploited target machine to send a specific payload to a data exfiltration server in a default location, or to a specific location set up by you.

The Data Exfiltration Test set up is configured at the system level. In the **System Setting > Network > Data Exfiltration Test** tab, the Server and Client Configurations are shown. By default, RidgeBot uses the HTTP server hosted by the Ridge Security Data Center located in the United States. Starting in RidgeBot 4.2.1, RidgeBot supports an internal blind monitor.

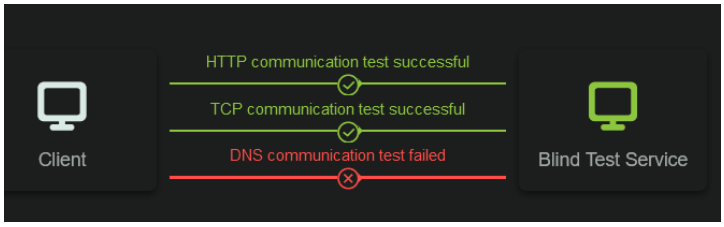
If a RidgeBot deployment does not have internet access or you choose to host your own server, user can choose to use RidgeBot internal blind monitor (Data Exfiltration server); otherwise, to set up your own server.

To use RidgeBot internal blind monitor, configure the Client Configuration HTTP Service Address and TCP Service Address using RidgeBot IP address and the HTTP Listening Port. See example.



Click "Test" to confirm the HTTP and TCP communication test are successful. Note the DNS communication test is failed as a known issue.

Then Click "Save"



To setup your own blind monitor server, first download the BlindMonitor server program by clicking the "**Download the server program**", then install the program. When done, specify values for the server in the RidgeBot configuration.

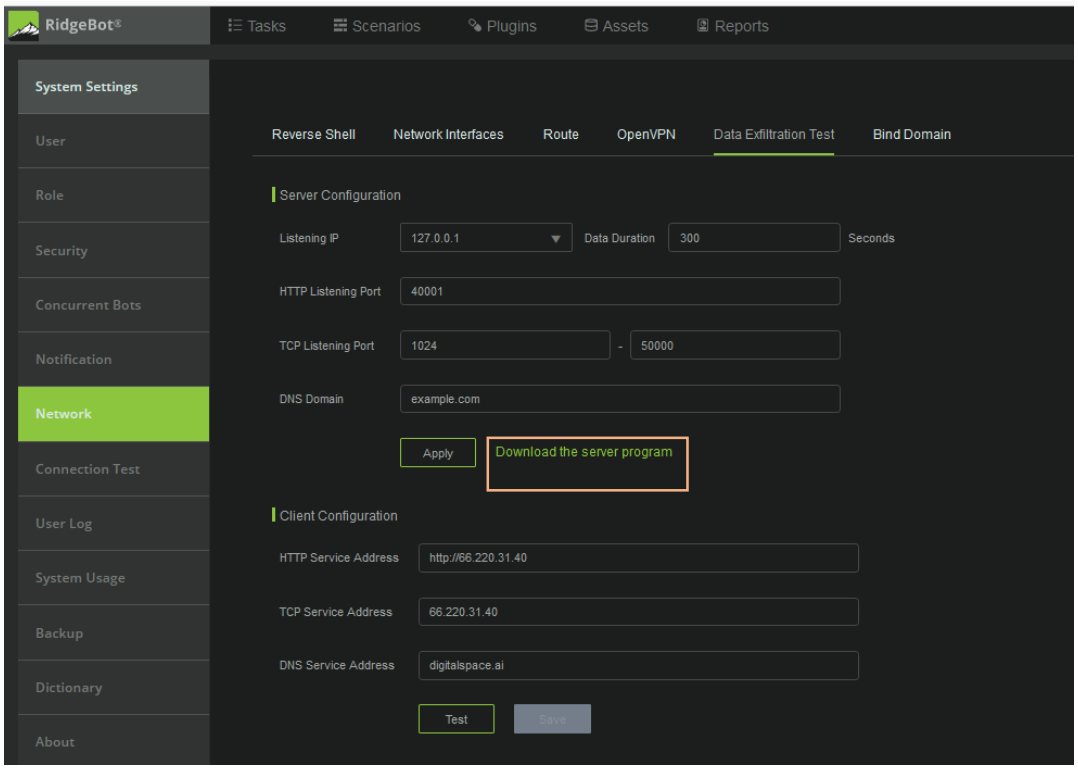


Figure 108: Data Exfiltration Test Configuration

Configure the server with the same information as in the BlindMonitor configuration and click "**Apply**" to save the parameters. Update the HTTP Service Address and TCP Service Address in RidgeBot's Client Configuration.

Select **Test** to verify communication between the client and the BlindTest Service. The communication test passes if the configuration is set up correctly. Click "**Save"**.

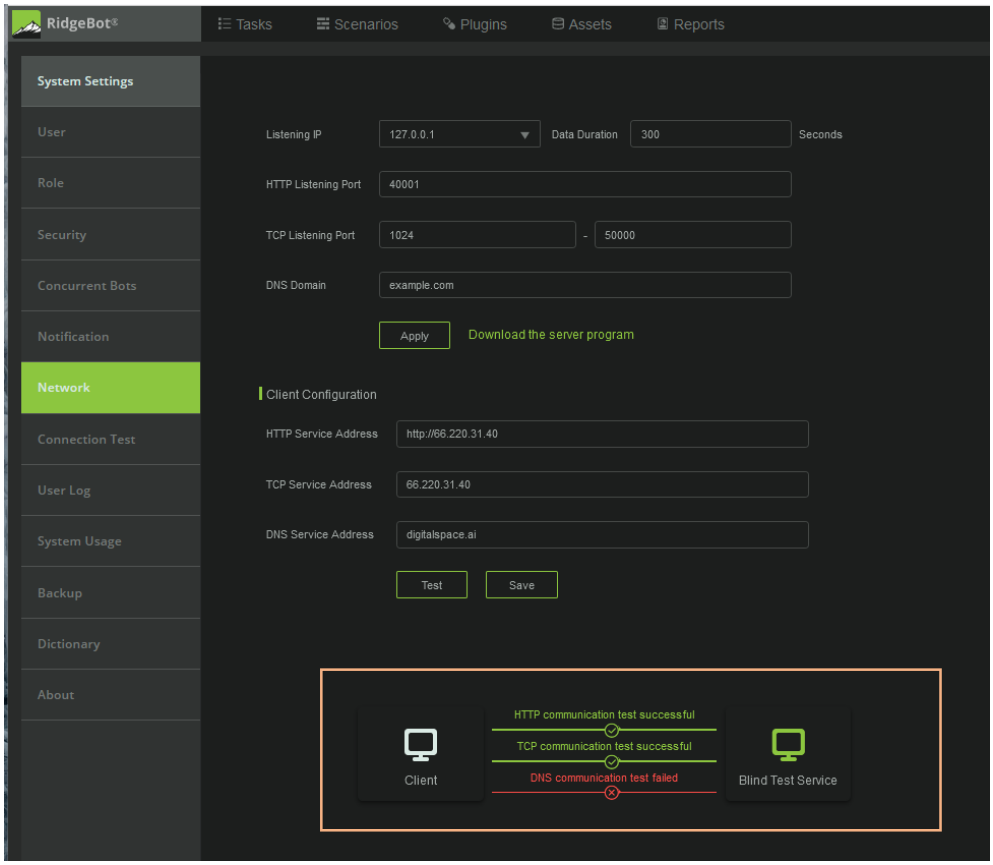
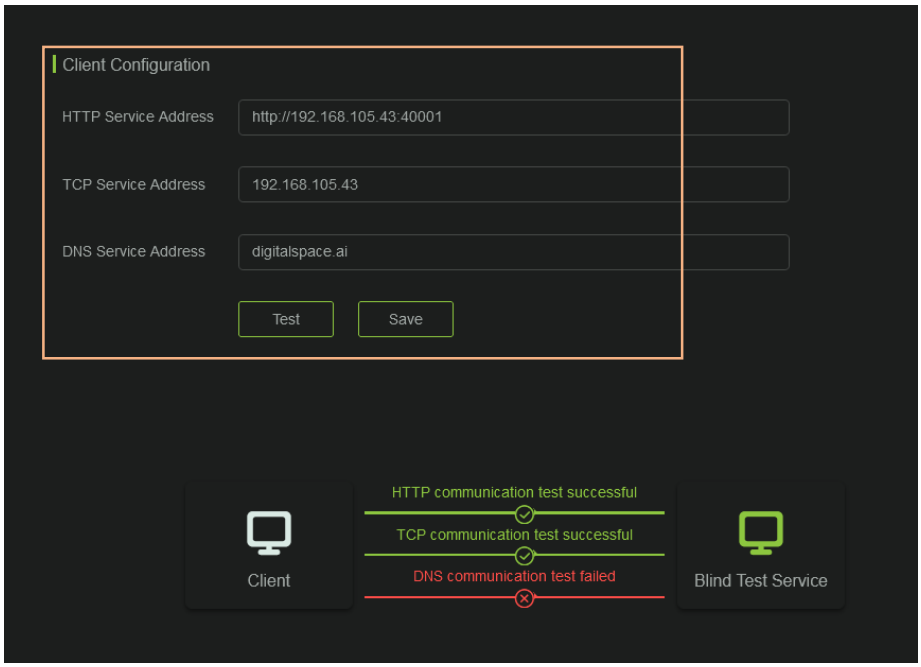


Figure 109: Data Exfiltration Client Configuration Test

Note:

- Ridge security provides a BlindMonitor server at 66.220.31.40. RidgeBot will use this server to validate data exfiltration from the target during exploitation.
- Only the Blind Monitor HTTP server program provided as a download from the RidgeBot GUI is compatible with RidgeBot.

Starting in version 4.2, RidgeBot has a built-in blind monitor using port 40001. The internal blind monitor does not support DNS lookup.



Configuring the Bind Domain

The Bind Domain is used as RidgeBot's internal DNS service. To assign an IP address to a host name, select the Domain Name and enter the information in the dialog box.

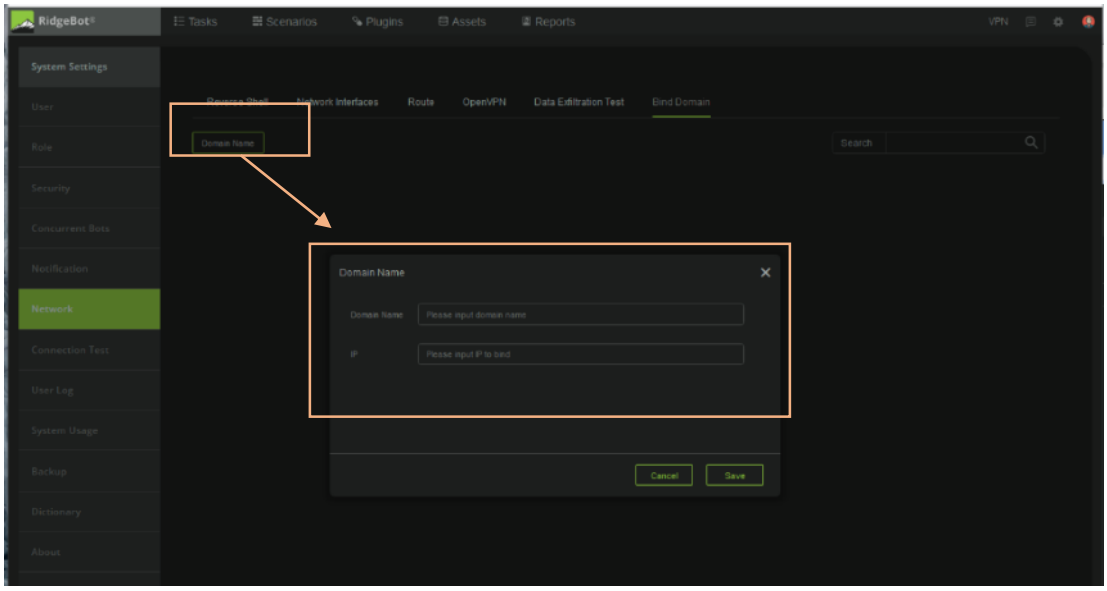


Figure 110: Bind Domain Configuration

Connection Test

RidgeBot provides Ping and Traceroute tools to diagnose network problems. To use the tools, follow these steps:

1. In the **Navigation Bar**, mouse over the **System Settings** icon, and select **Connection Test** from the drop-down menu.
2. Under the **Ping** tab, enter an IP address to ping the target, and under the **Traceroute** tab, enter values for the parameters to trace a route to a target.
3. Tip: Use traceroute to test if a target network port is open. For example, use traceroute to check if RidgeBot can reach the license server on port 8001.

User Log

The User Log contains a history of the activities performed by RidgeBot admin users, such as actions taken, configuration operations, and task operations.

To view the User Log, follow these steps:

- In the **Navigation Bar**, mouse over the **System Settings** icon, and select **User Log** from the drop-down menu.
- The User Log entries are displayed on the page. To search for specific log entries, enter a keyword into the search text box and then search.

System Usage

RidgeBot system information is collected and shown in the System Log dashboard, including CPU, memory, disk and network traffic information.

To view the system information, on the **Navigation Bar**, mouse over the **System Settings** icon, and select **System Usage** from the drop-down menu. All system information is shown in graphical format.

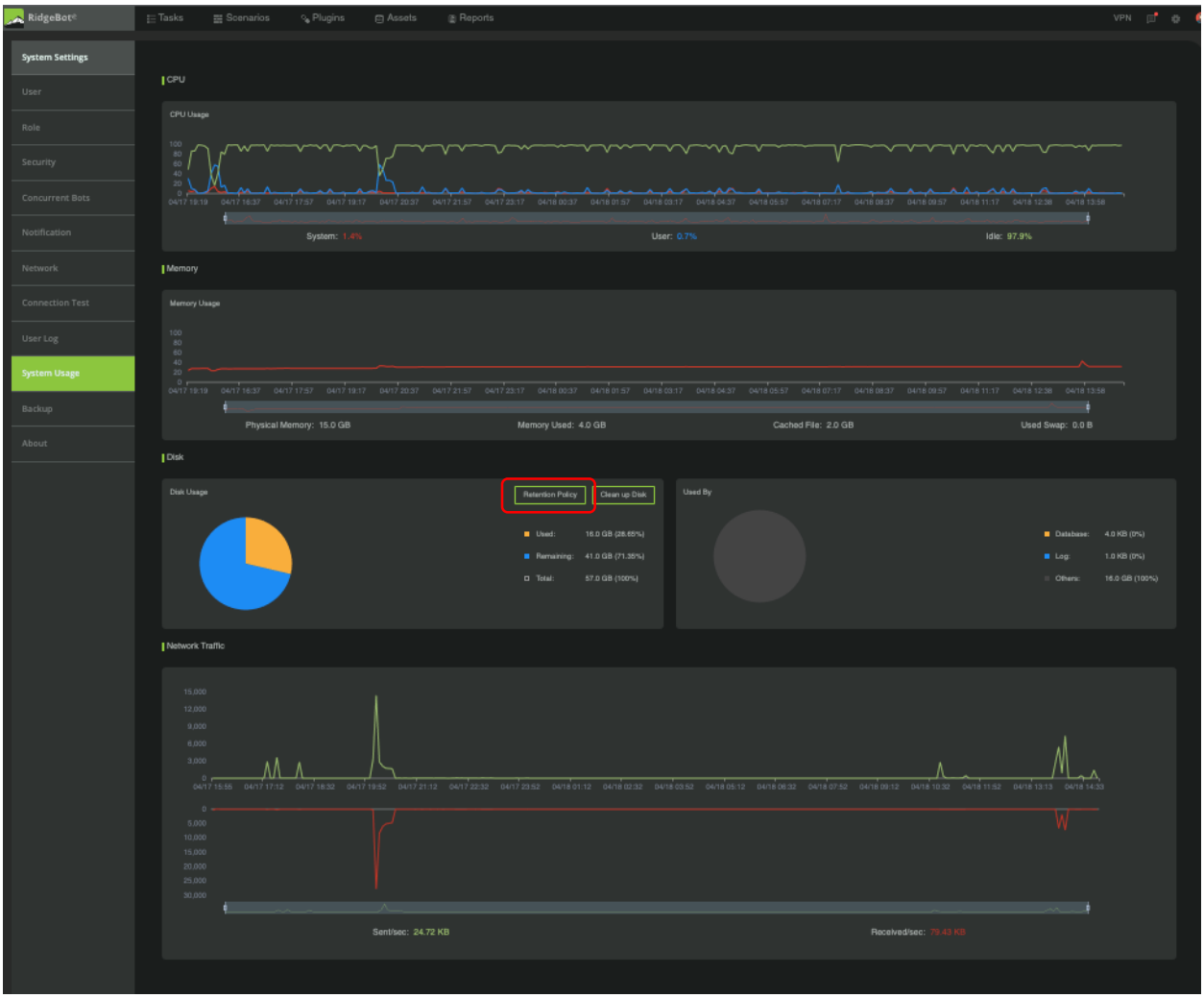


Figure 111: System Usage Graphical Display

Disk space is managed by user by click on the "Clean up Disk" button. This action will delete the internal log and backup files. In addition, the user can delete a task or the Backup configuration and Log zip files in the System Settings -> Backup. When a task or a backup file is deleted, RidgeBot cleans up the data and frees up the associated disk space.

In 4.2.2, User can configure the retention period for RidgeBot logs. Default setting is 180-day

RidgeBot Disk Usage:

- System: 14GB
- Task: Approximately 250MB. Actual disk usage depends on the number of targets and the results of the task.

Backing Up Configurations and Logs

RidgeBot's configuration backup allow user to create a restore point of RidgeBot settings and task information. When user creates a restore point, RidgeBot will back up all the settings, scenarios, tasks, assets, and reports into a configuration backup file. User can restore the RidgeBot back to the same restore point as needed. Here are some rules governing the back configuration feature:

1. The backup and restore configuration file can only be applied to the same RidgeBot. User can delete, restore and download the configuration file.
2. The restore configuration should be applied to RidgeBot that has the same software version as the backup configuration (Note: to find the configuration file software version, check the configuration file date and Update History)
3. If RidgeBot has been upgraded to a newer software version, it is **not** advised to restore RidgeBot using configuration backup from an older version.

RidgeBot backup log is a snapshot of RidgeBot system logs. This log does not contain the target test data, only its IP address as an exception. This log is useful to assist Ridge Security engineer to do troubleshooting.

RidgeBot's configurations and backup logs can be backed up periodically. You can download or delete past backups.

On the **Navigation Bar**, mouse over the **System Settings** icon, and select **Backup** from the drop-down menu.

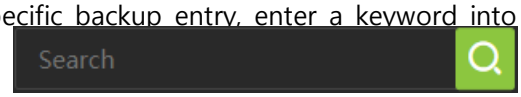
To back up a configuration immediately, click the **Backup Now** button. When it has completed, a backup entry is added to the backup list.

To schedule automatic backups, click on the **Automatic Backup** option to select **Weekly** or **Monthly**. The backup is performed at the specified time and completed backup entries are displayed in the backup list on the page.

To download a backed-up configuration, click **Download** in the **Action** column.

To restore the system to a backed-up configuration, click **Restore** in the **Action** column.

To delete multiple backup entries, select the checkboxes of the entries to be deleted in the backup list, and then click the delete button  in the upper right corner.

To search for a specific backup entry, enter a keyword into the **Search** text box at the upper right corner of the page, 

and then click the search button.

You can use similar steps in the **Log Backup** section of the same page to back up, download or delete user logs.

About Information

On the **Navigation Bar**, mouse over the **System Settings** icon, and select **About** from the drop-down menu. The display shows RidgeBot product, module and quota information, and allows you to do an offline upgrade as well as adding a license file.

About: Managing Your License

A license is required to use RidgeBot. This section discusses how to manage the license files and the license server.

Importing a License File

Use one of the following methods to import a license file into the system:

1) At the bottom of the **About** page, drag the license file into the authentication file area.
2) At the bottom of the **About** page, click to choose an authentication file.

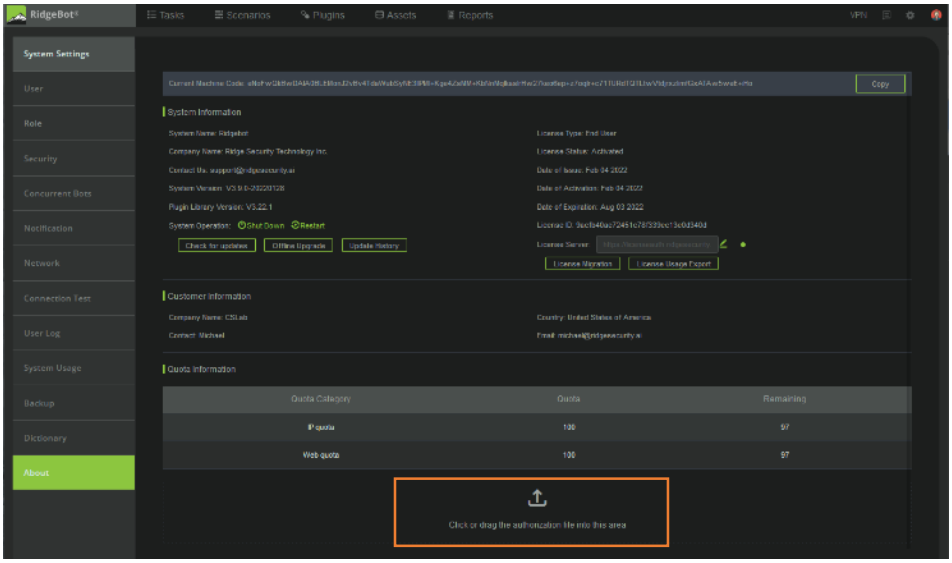


Figure 113: Importing a License File

Changing the IP address of the License Server

To change the IP of the license server, follow these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **About** from the drop-down menu.
2. If you click the **Edit** icon of the **License Server**, the text box becomes editable.

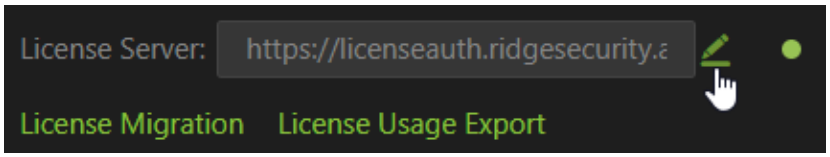


Figure 114: Changing the License Server

3. Enter the new IP address or URL in the text box.

> **Caution**: You should not change the license server URL. Port 8001 on the License Server is required to be opened. RidgeBot cannot run a new task if it is unable to communicate with the License Server on port 8001, except when it is deployed in the appliance **offline** mode.

The little dot to the right of the **Edit** icon shows the connection status of the License Server:

- Green: Connect to the license server
- Red: Disconnect from the license server

> **Note**: User can verify the license server communication in RidgeBot management console using the "check-license" command. See the latest version of RidgeBot Deployment Quick Start Guide for more detail.

Migrating a License

License migration is used to transfer a license from one RidgeBot to another RidgeBot. User can request a license migration from one RidgeBot to another RidgeBot via the online RidgeBot license request in the Partner Portal.

License migration policy will be shown in the License migration policy section.

To migrate a license, follow these steps:

1. On the **Navigation Bar**, mouse over the **System Settings** icon, and select **About** from the drop-down menu.
2. Click the **License Migration** link License Migration to export the current license file.

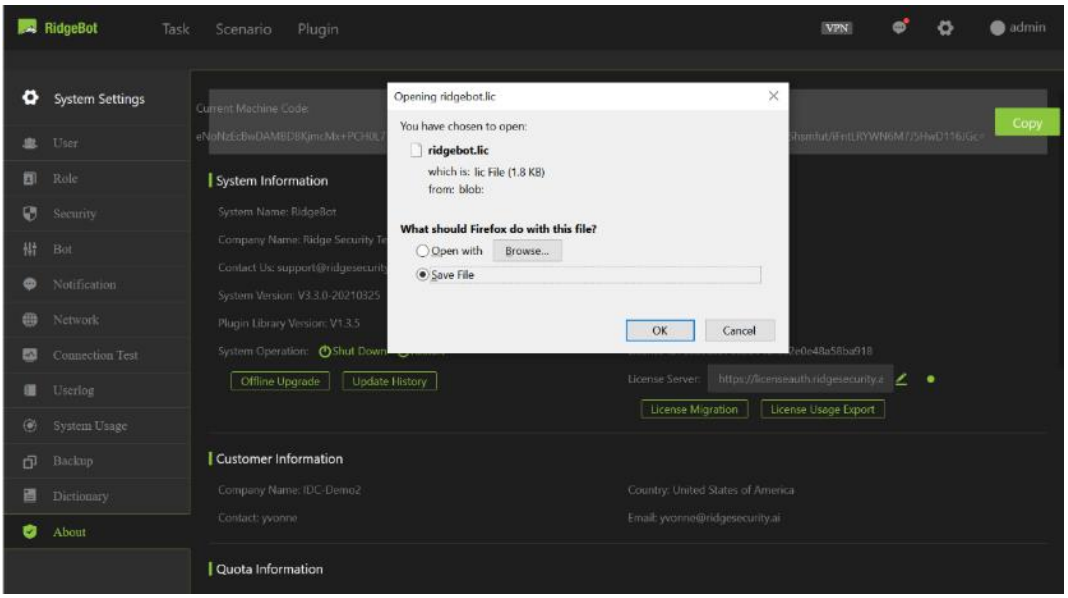


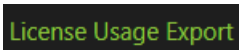
Figure 115: Export the License File for License Migration

3. Send the exported license file (ridgebot.lic) to the Ridge Security Support team for them to generate a new license file that includes the remaining quota from your exported license.
4. Import the new license file into the system.

Note: The system is disabled after you export the license. You can access any existing task data but cannot create a new task. The system is re-enabled after a new license file is imported.

Exporting License Usage Information

The license usage function exports a report on your current license quota usage, including the time, as well as IP address or URL that was executed.

To export license usage information, click the **License Usage Export** link 

on the **About** page. A **usage_info.csv** file is downloaded to your desktop.

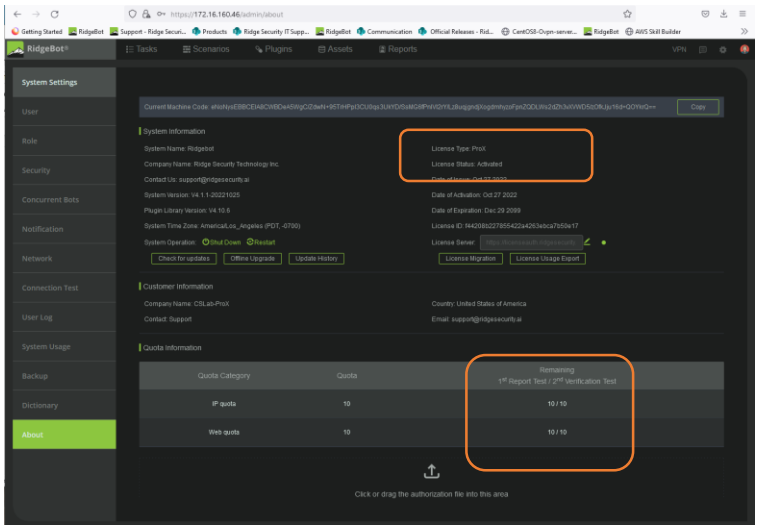
The usage info file includes the following information:

- **id**: The identifier.
- **timestamp**: The timestamp in Unix format with a link to the conversion tool: https://www.epochconverter.com/
- **target**: The target, in either IP or FQDN format.
- **target_type**: In IP or Web format.
- **task name**: The task's name.
- **status**: 1 or -1:
    a. 1 indicates this target is valid and does not require additional license quota if the task is restarted. This is subject to the restriction of the Pro-X license or End-User Annual Subscription License.
    b. -1 indicates this target is now invalid and requires a new license quota if the task is restarted.

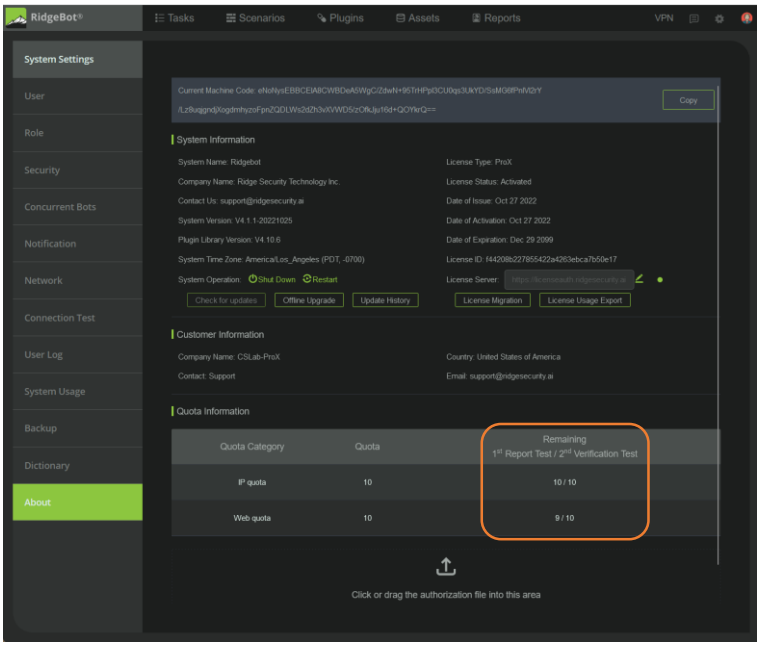
License Type

RidgeBot supports three different license types:

1) MSV – This license is a single use for MSSP. The license is a one-time used. It is consumed once the task is completed and does not have a 14-days grace period . This MSV license type has a one-year expiration date for the unused license.
2) ProX – This license is a single use for MSSP that has two 14-days test windows and a time limit consumption model. A task will trigger the ProX license first test window and this test window will expire in 14 days as the license "first use". This license will be consumed after the completion of the task using the same IP or URL in the 2nd test window within 6 months or the license will expire in 6 months after the "first use". The unused ProX license does not have an expiration date.



Example of the ProX license and the quota in RidgeBot "about" page



Example of a task that uses the web license on the 1st test window

3) End User Annual subscription – This license is an annual subscription for End User only. This license allows unlimited testing on the same IP or URL within the subscription period.

Note: MSSP is Managed Security Service Provider

License Migration policy

ProX Ridgebot license migration policy

1) ProX license can be transferred from the original RidgeBot to another RidgeBot per user request. The license issue to the new RidgeBot will be referred to as migrated license. Since ProX license is based on usage or count, the migrated license will have the original license term and condition and only has the remaining or unused license quota from the original RidgeBot. License count that has been used are not transferred. The original license will be invalidated
2) ProX license does not apply to de-commissioned asset.

MSV Ridgebot license migration policy

1) MSV license can be transferred from the original RidgeBot to another RidgeBot per user request. The license issue to the new RidgeBot will be referred to as migrated license. Since MSV license is based on usage or count, the migrated license will have the original license term and condition and only has the remaining or unused license quota from the original RidgeBot with the same expiration date. License count that has been used are not transferred. The original license will be invalidated

2) ProX license does not apply to de-commissioned asset.

End User Annual subscription (EUAS) license migration policy

1) EUAS license transfers from the original RidgeBot to a new RidgeBot. End User annual subscription will be allowed end user to transfer a license in the following condition:
   a) End-User will request the reseller to request a License migration from Ridge Security Partner Portal
   b) The request will be reviewed and approved by Ridge Security at its sole discretion
   c) If the request is approved, Ridge Security will be invalidated the original license and issue a migrated license.
   d) The migrated license will have the same original license term and condition. The migrated license start date is the date when the migrated license is issue, and the license expiration date is the same date as the original license.
   e) The RidgeBot license migration only transfers the license quota to the new RidgeBot. The configuration and data of the original RidgeBot are not transferred.

2) End User Annual subscription license transfers for de-commissioned asset in the same RidgeBot – End User annual subscription will be allowed end user to transfer a license from a decommissioned asset in the same RidgeBot in the following condition:
   a) The de-commission asset can only be transferred after the asset is not active for 90 days or more
   b) End-User will request the reseller to request a License migration from Ridge Security Partner Portal
   c) Ridge Security will review the request and may approved the request at its sole discretion
   d) Once the license request is approved, Ridge Security will credit end user the same number and type of license from the de-commission assets. The original license will be invalidated.
   e) The new license will have the same original license term and condition. The new license start date is the date when the new license is issue, and the license expiration date is the same date as the original license.

License Requirement Exception

RidgeBot needs to be activated to run, but there are one scenario and beta features that do not require license as listed below:

- PT scenario: Attack Surface Identification
- ACE Scenario: Scenario marked with Beta*
- Targets defined in the Ranger of Lateral Movement of the Task Post Exploitation configuration*

Note *: license will be required to use these features in the future version of the software.

Software and Plugin Library Upgrades

Software Upgrade Package

The software upgrade package is to upgrade the RidgeBot software to the latest software version. The software package can be download online (starting in version 4.2) or offline.

IMPORTANT:

1. License file for version 4.2 is not compatible with the license file from version 4.1.1 or earlier.

1. RidgeBot software version 3.9 cannot be upgraded from the previous releases.

Plugin Library Upgrade Package

- The plugin library upgrade package is to add new plugins including plugin bug fix to the current ridgebot.
- The RidgeBot Plugin Library package is to add new plugins or update the plugins in the RidgeBot. The Plugin Library is available in the same software folder as the RidgeBot system software.
- The RidgeBot Plugin Library can be upgraded directly to the latest version. Intermediate versions of the Plugin Library can be skipped during an update. For example: RidgeBot v3.6 is bundled with Plugin Library version 2.7.2. During an update, you can skip Plugin Library version 2.9.2 and update directly to RidgeBot Plugin Library version 2.10.1.
- The RidgeBot software upgrade package filename is in the format CUP-version-EN-date.bin, where the "date" is the release date. For example, the upgrade package name to update the RidgeBot Plugin Library is CUP-V2.10.1-EN-20211013.bin.

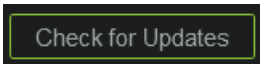
Note: As of version 3.7, the Plugin Library upgrade package extension has changed from .zip to .bin.

Software Upgrade and Plugin Library Process

Starting in software version 4.2, RidgeBot supports upgrade online and upgrade the software or plugin library in the offline mode. click on the appropriate upgrade button and follow the instruction of the pop-up dialog box.

Software Upgrade Process

Software Online Upgrade Process

- Make all the tasks are completed or stopped before starting the online upgrade process
- In the About page, the 

button is now enabled. When user clicks on the button, RidgeBot will access the upgrade server for update. A pop-up dialog box shows a message if RidgeBot current software version is up to date or there is a newer software version available to be upgraded.

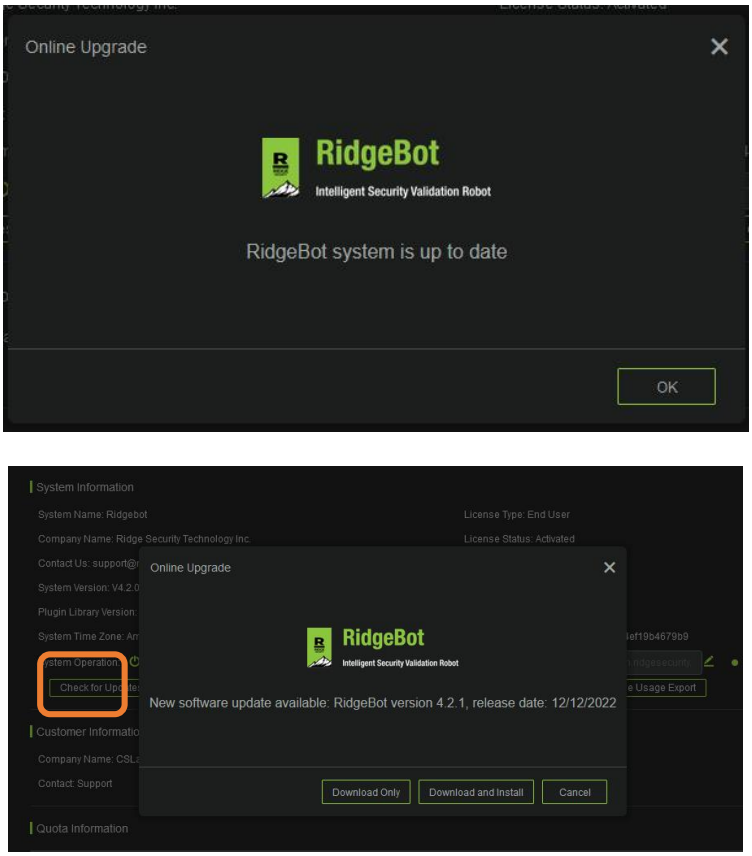
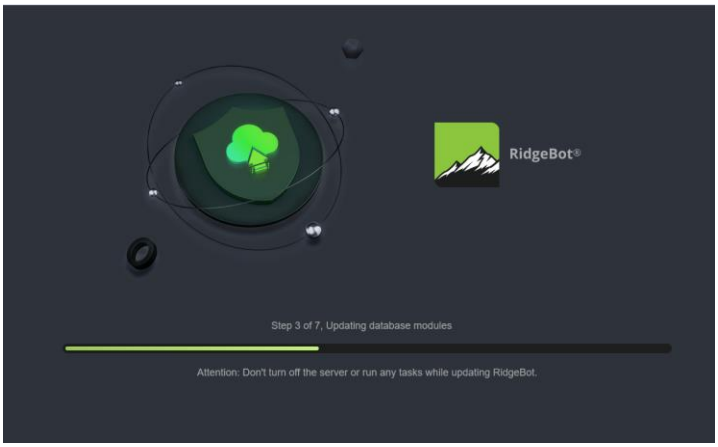


Figure 116: Online Upgrade pop-up dialog box

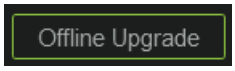
- User can select to download the package and Click on "Install" or click on "download and Install" to start the upgrade process.
- RidgeBot will download the package and start the installation (sample upgrade installation screenshot)



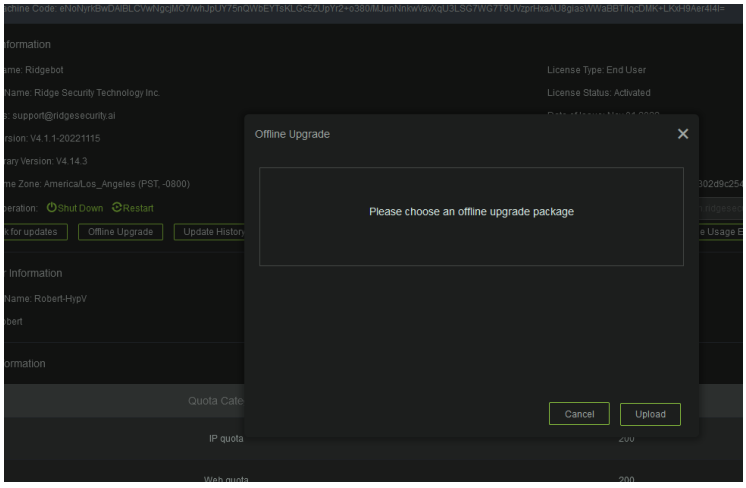
- When finished, it will show the status as "Update Successful" or "Update fail". This process may take approximately 30 minutes. Click on the Login to return to the Login GUI.

Software Offline Upgrade Process

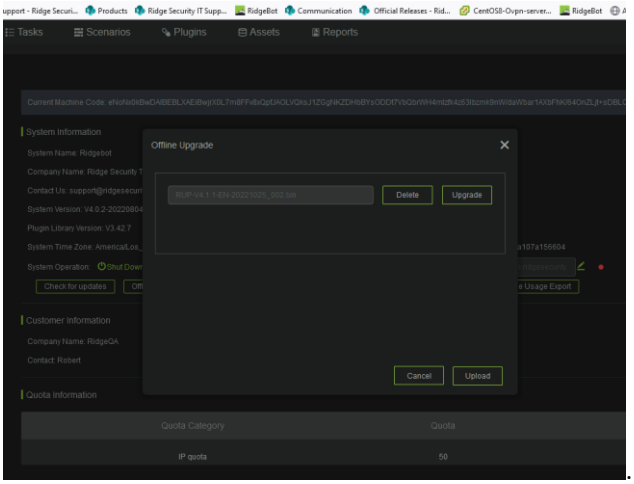
To use the offline procedure to upgrade the RidgeBot software, follow these steps:

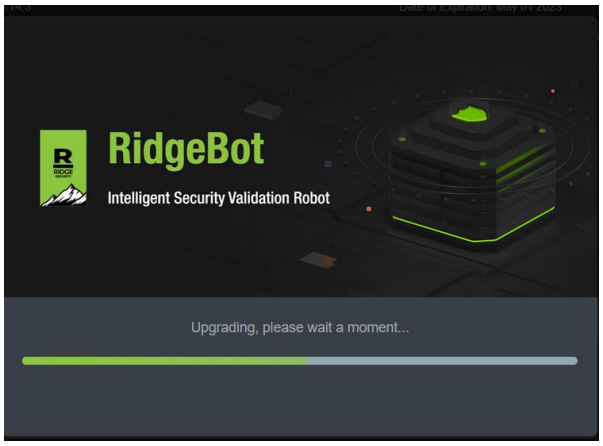
1. Download the "RUP_XXXX" upgrade package from the software download folder.
2. Make all the tasks are completed or stopped before starting the online upgrade process.
3. In the system setting -> about page, click the 

button.
4. In the pop-up dialog, click the **Upload** button to select the RidgeBot Software patch as a .bin file (note: the software patch file is shown in the dialog box—if it is the incorrect file, you must click the delete button and upload the correct file).
5. In the pop-up dialog box (as shown below), click on Upload and select the "RUP_XXXX" upgrade package.

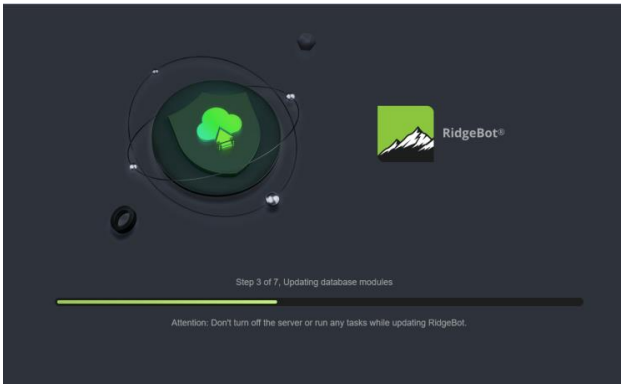


6. After the file upload to RidgeBot then click on “Upgrade” to start the upgrade installation





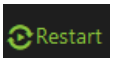
Upgrading dialog box from 4.1.x



Upgrading dialog box from 4.2.x

7. Once the upgrade is completed, The “Update Successful” message is shown. Click on the “Login” to return to the login screen or “Experience Now” (for RidgeBot version 4.1.1 or earlier)

Upgrade completion dialog box From 4.1.x

8. Click the 

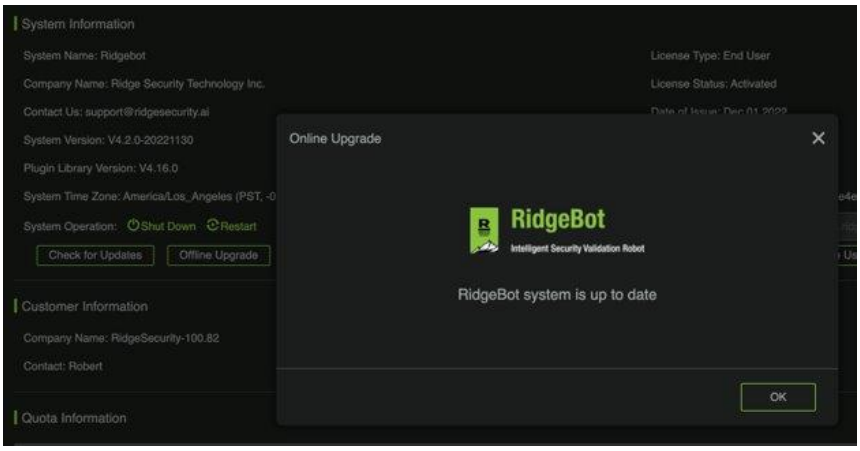
button in the About page -> System Information or run the “restart-service” from the management console. (this step is only required as stated in the README First instruction).

Note: It is important to read the “**README First**” file in the software download directory. This “**README first**” file contains specific upgrade procedures for each version.

Plugin Library Upgrade Process

Online Update Process:

- Make all the tasks are completed or stopped before starting the online upgrade process
- In the About page, the “Check for updates” button is now enabled. When user clicks on the button, a pop-up dialog box shows a message if current version is up to date or there is a new version available to upgrade.



- If an upgrade is available, user can select to download the package and Click on "Install" to start the upgrade process. When finished, it will show the status as "Upgrade success" or "upgrade fail" as in the software upgrade process.

Offline Update Process:

The Plugin Library information is listed on the **About** page. You can upgrade the Plugin Library by importing a new plugin package. The latest Plugin Library and RidgeBot software are available on the Partner Portal.

To use the offline procedure to upgrade the Plugin Library, follow these steps:

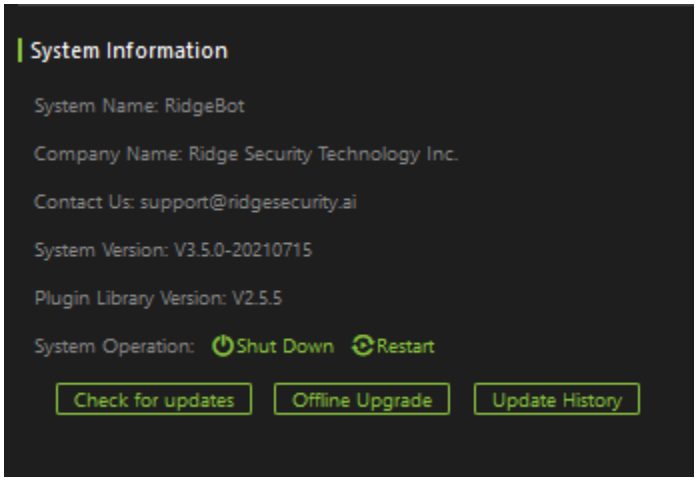


Figure 117: Offline Plugin Library Upgrade

1. Request a software download: You need the ISO Installation package on the Partner Portal to get access to the Plugin Library.
2. Download the Plugin Library to your PC.

3. In the **System Information** section, click the 

button.
4. In the pop-up dialog, click the **Upload** button to select the plugin package (CUP-Vxxx.bin file) from your PC.
5. Click the **Upgrade** button to start the Plugin Library upgrade process (note: the plugin file is shown in the dialog box—if it is the incorrect file, you must click the delete button to remove the file before you can upload the correct file).
6. Click the **Update History** button to see the update history.

Chapter 11 Management API

As of version 3.5, RidgeBot provides an API to integrate with 3rd party tools to manage user tasks and reports. For each new software version, RidgeBot may include a new version of API which may be compatible with the previous version.

Note:

- The RidgeBot API documentation and user guide are available on Partner Portal for download.
- The RidgeBot API documentation can be accessed from RidgeBot at https://your_RidgeBot_IP/public/api/

This chapter has the following sections:

API Compatibility

The current API version is V4

Identity Token

Each user has an Identity Token used to manage the user's task. Follow these steps to get an Identity Token to be used as the API access key:

1. Click on the **Username** in the GUI's upper right corner to access the User Center.
2. Select **Identity Token** on the lefthand workflow.
3. Click on **Generate** or **Regenerate** to create a Token.
4. Once the Token is generated, the Action options are to **Copy** the Token or **Delete** the Token (deleting the Token disables access to this user's tasks).

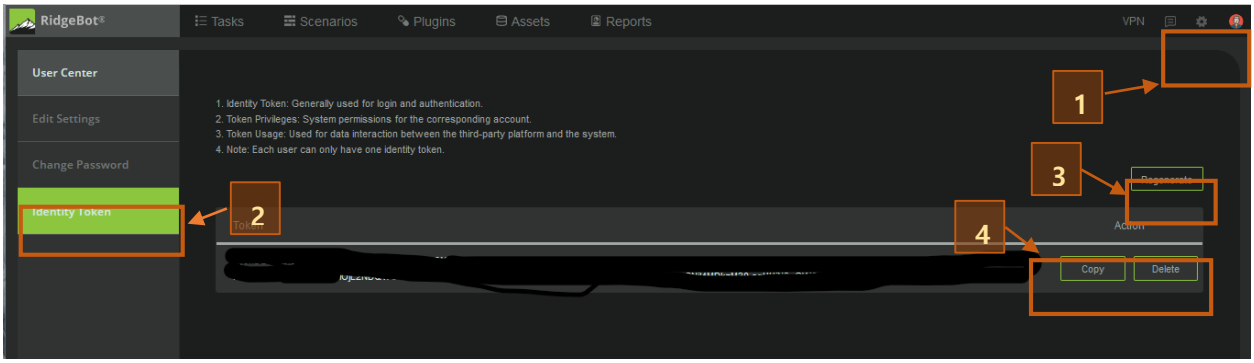


Figure 118: User Center

Supported API Functions

As of version 4.1.1, the following actions can be invoked from the API:

- **Assets:** To get, add, delete, or input a host, site or user.
- **Task Management**: To manage a list of user tasks.
- **Task Data**: To retrieve an ACE summary and trend information.
- **Scenario Management**: To access the scenario list and information about scenarios.
- **Report**: To access the list of reports, or to generate, delete or download a report.
- **ErrorCode**: To retrieve the list of error code
- **Test**: To use an API call to RidgeBot to check connection and to valid the API token

To access RidgeBot API JSON file, type in the below URL in the web browser:

https://RidgeBot_IPADDR/public/api

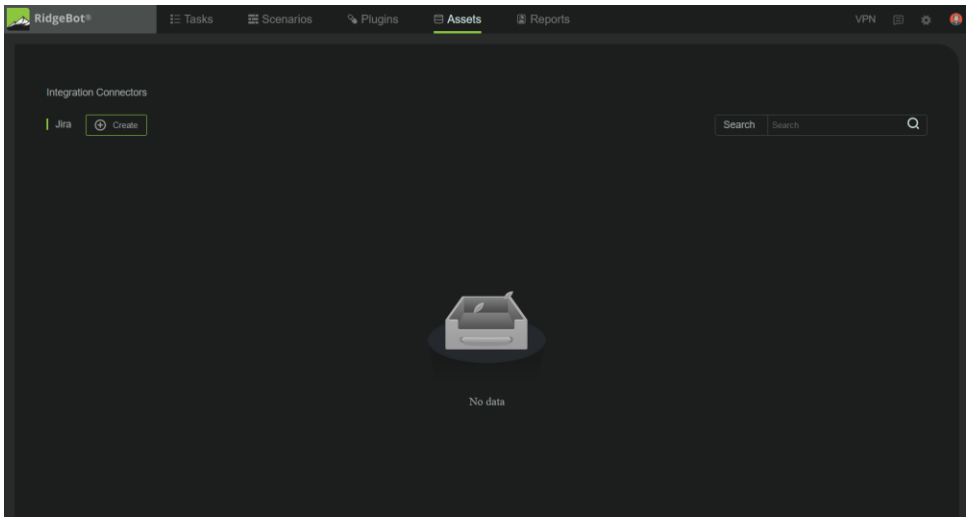
Chapter 12 – Integration

RidgeBot supports the integration with JIRA (on-prem), Jira Cloud and GitLab (OnPrem and Cloud). User can define multiple JIRA or GitLAB servers and projects to be used in a task. User can configure RidgeBot to automatically open a JIRA or GitLAB case during a task creation. User can also manually open a JIRA or GitLAB case by selecting the vulnerabilities from the task vulnerability table.

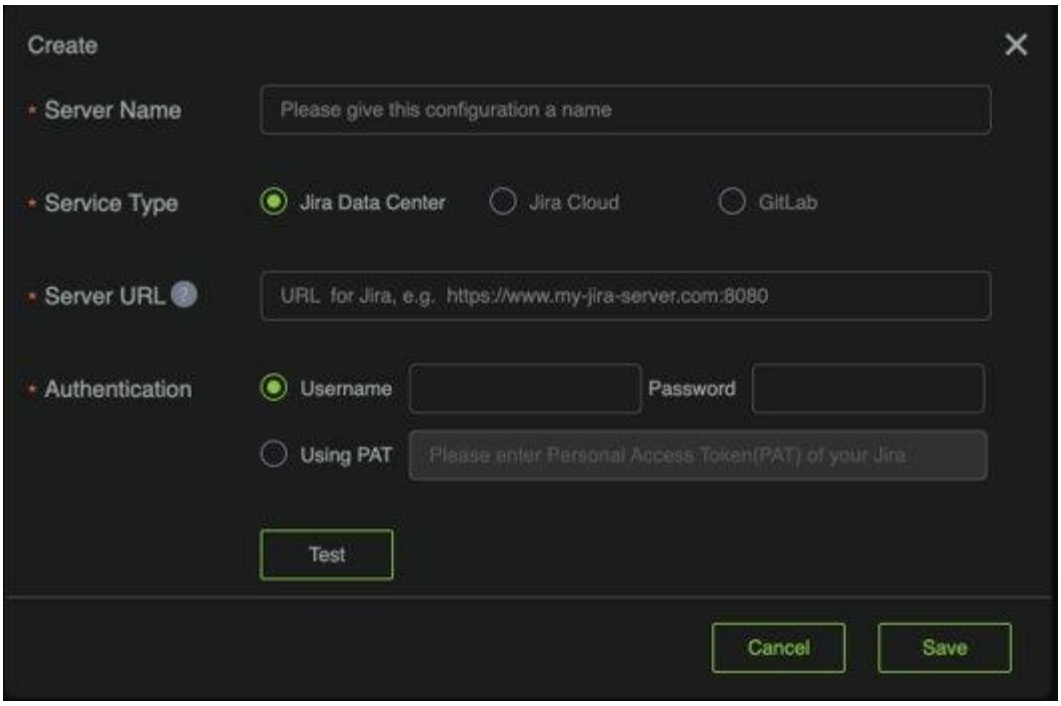
JIRA Integration

Connect to a JIRA server

To setup JIRA integration (On Prem only), go to the Asset tab and select "Integration Connectors"

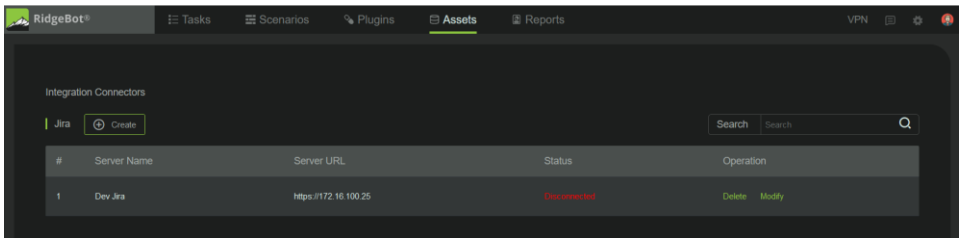


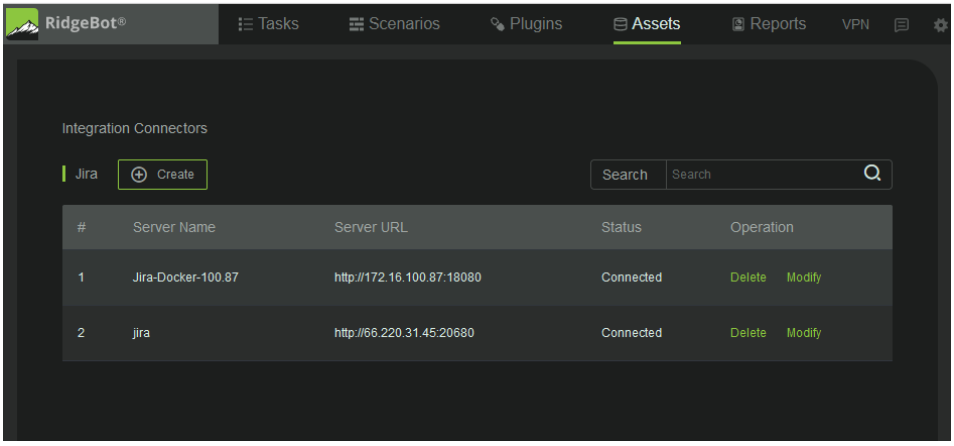
Click on Create to create a JIRA connection



After the required information is input, click on "Test" to verify and "Save" to create the Jira connector

The Integration Connectors will list the Jira connector for each server with the connector status. User can modify or delete the connector from the option in Operation.

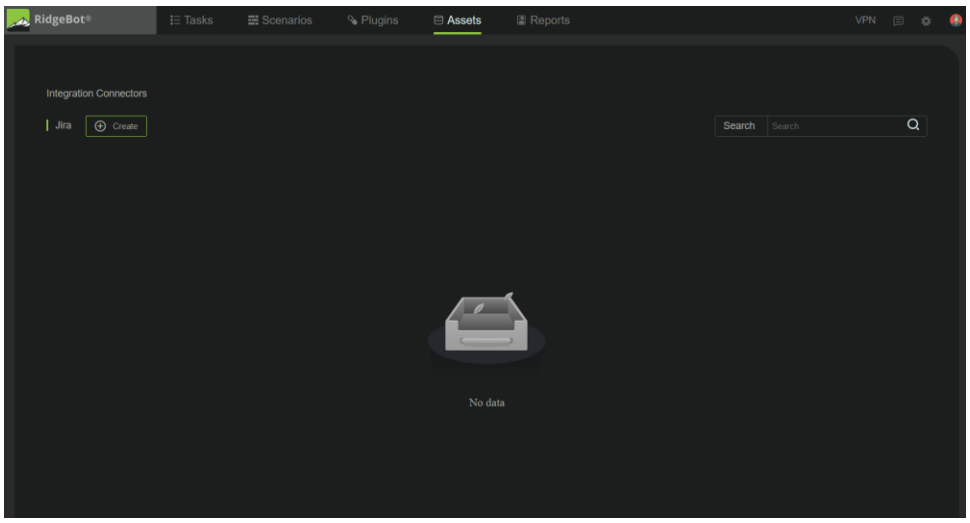




Example of Jira servers and status

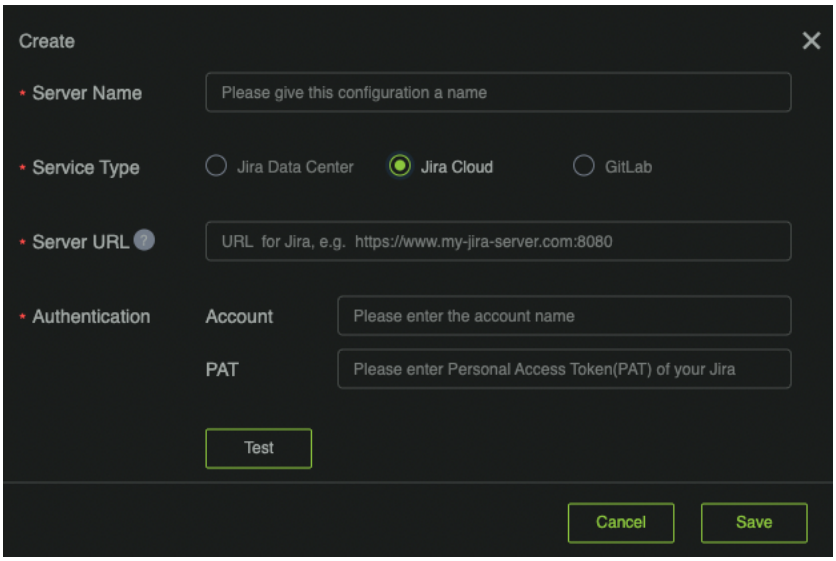
Connect to JIRA Cloud

To setup JIRA Cloud integration with your active Jira Cloud account, go to the Asset tab and select "Integration Connectors".



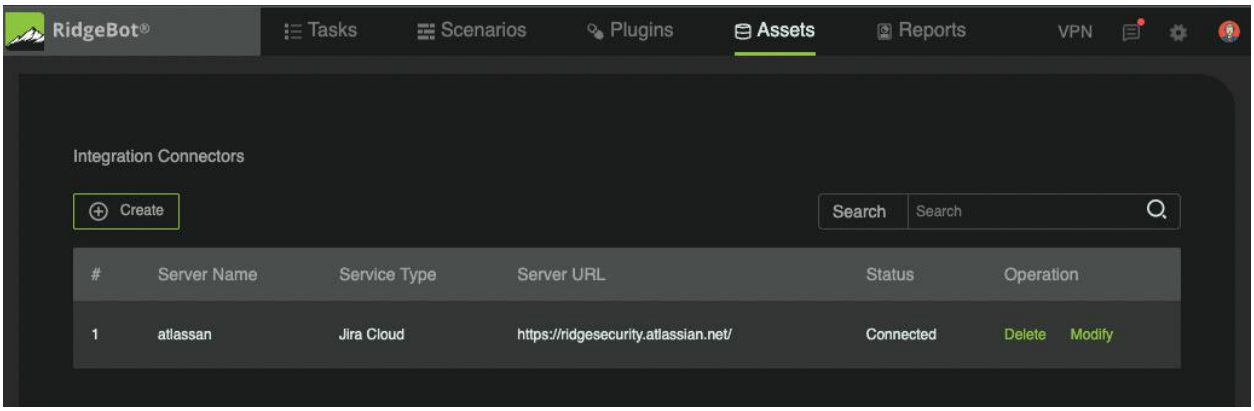
Please make sure to generate a personal access token (PAT) in Jira Cloud before the next step. See Jira Cloud documents for how to generate PAT.

Click on Create to create a connection, select "Jira Cloud".



After the required information is input, click on "Test" to verify and "Save" to create the Jira connector

The Integration Connectors will list the Jira connector for each server with the connector status. User can modify or delete the connector from the option in Operation.

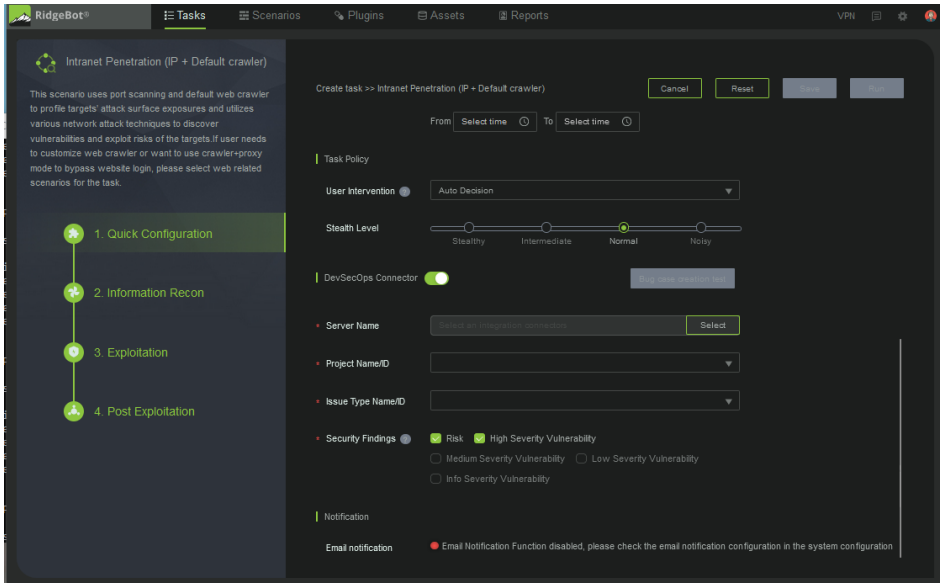


Example of Jira servers and status

Open Jira case from a Task

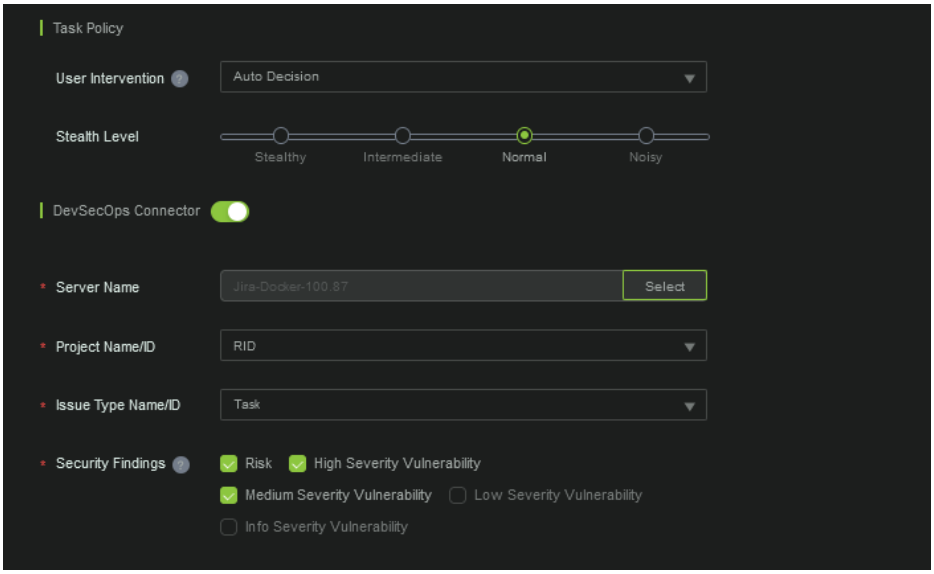
The following procedure is the same for both Jira Server and Jira Cloud.

- Enable DevSecOps in the Task Quick Configuration



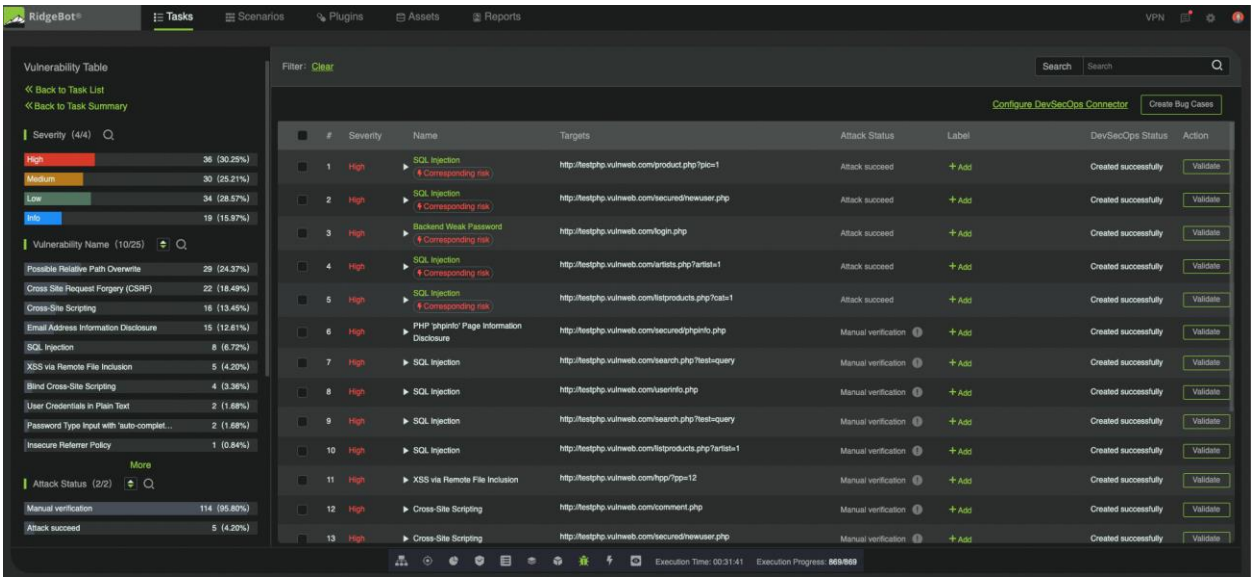
- Select a Jira server and its project

1. Select a Server from the Integration Connectors list – Click "Select" in the Server Name
2. Select Project Name and Issue Type. This is the project folder where RidgeBot will put newly created case with the selected issue type. The Project Name/ID and Issue Type Name/ID are the categories created by user in the selected Jira Server.
3. Security findings selection allows the user to select a category that will automatically generate a Jira case.

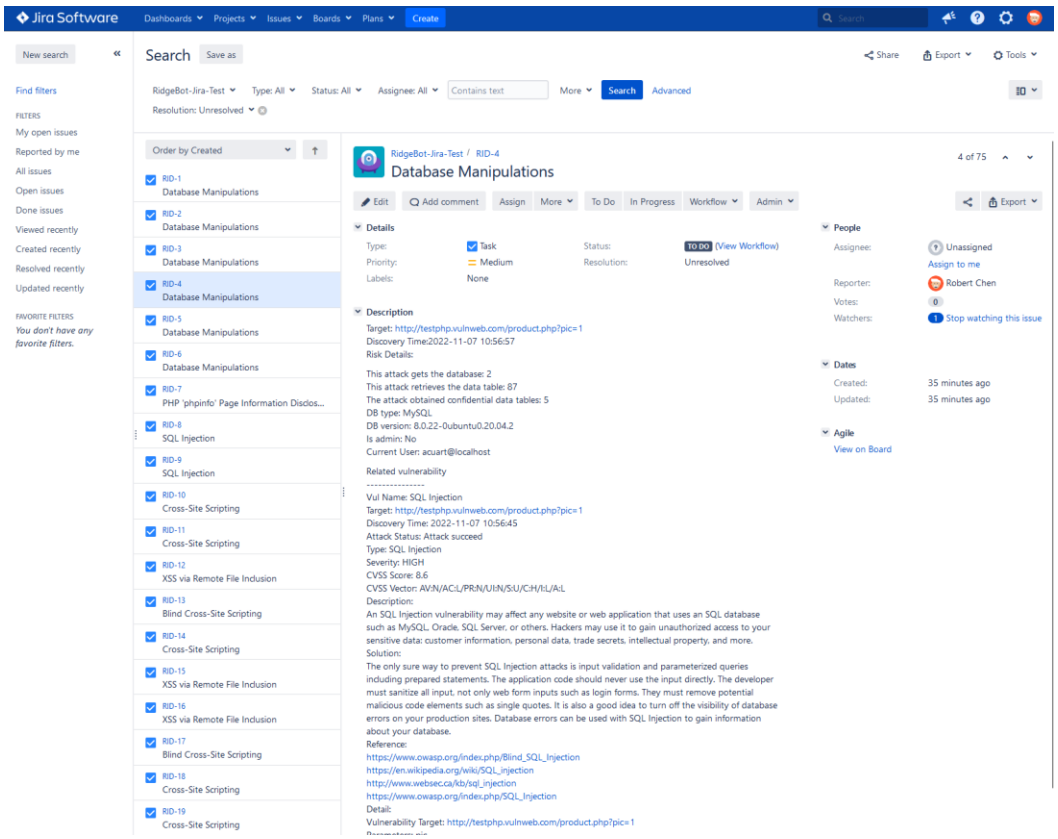


Example of a server configuration in a task

- After the task is finished, check the vulnerabilities list to see if the cases have been created in the "DevSecOps Status" column.



- Example of a Jira case opened by RidgeBot. In Jira Server – user needs to review and updates the Jira cases accordingly.

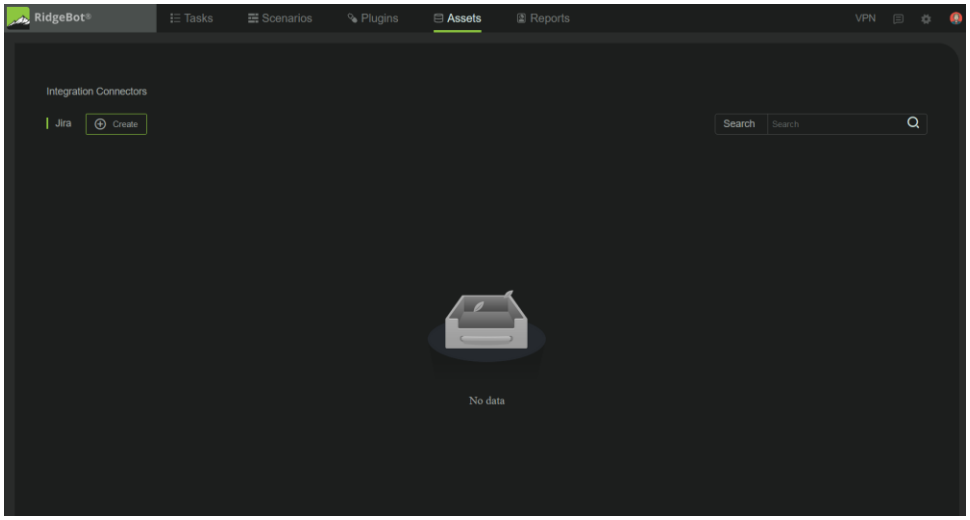


GitLab Integration

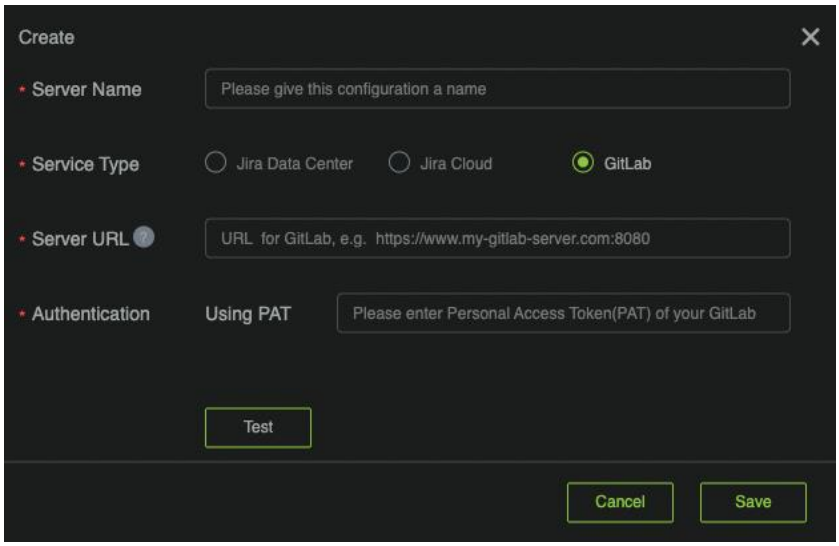
Connect to a GitLab

Please make sure to generate a personal access token (PAT) in GitLab before the next step. See GitLAB documents for how to generate PAT.

To setup GitLab integration (On Prem or Cloud), go to the Asset tab and select "Integration Connectors".



Select "GitLab"

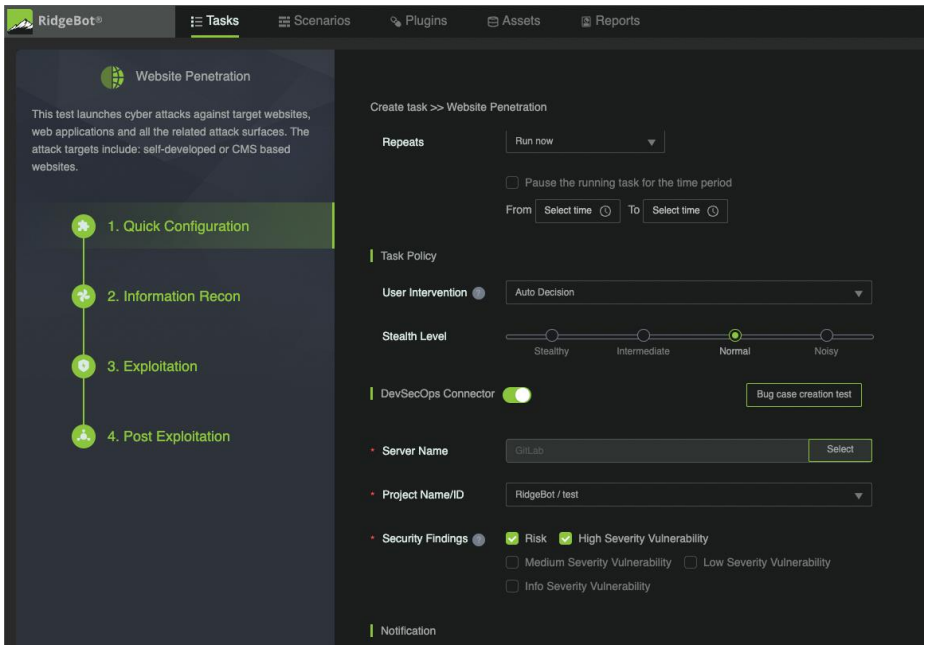


After the required information is input, click on "Test" to verify and "Save" to create the GitLab connector

The Integration Connectors will list the GitLab connector for each server with the connector status. User can modify or delete the connector from the option in Operation.

Open GitLab case from a Task

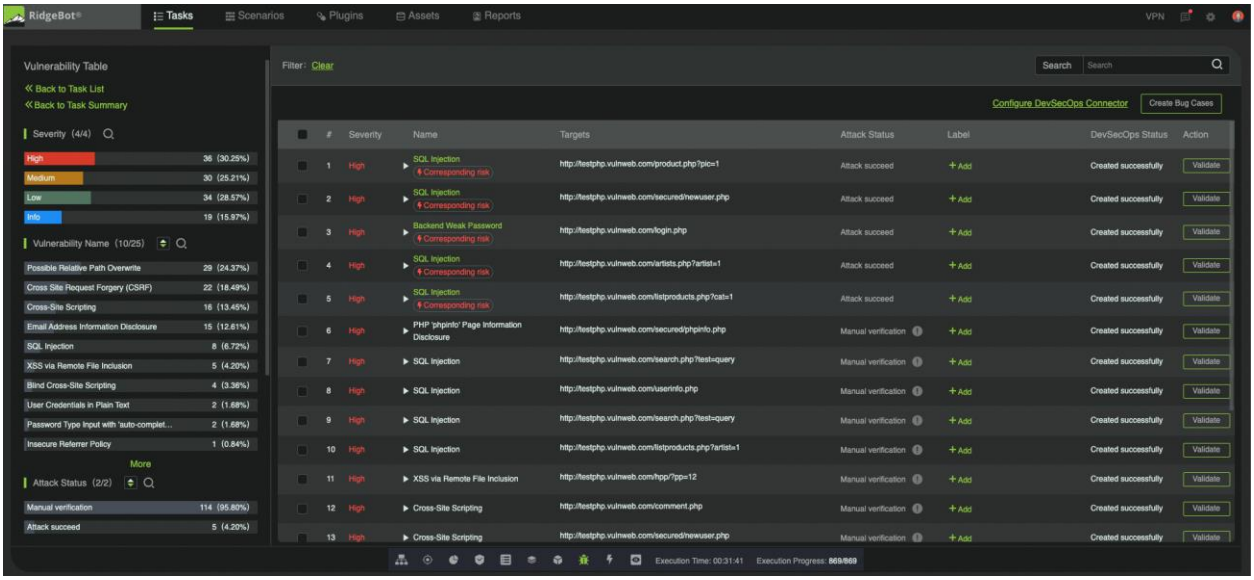
- Enable DevSecOps in the Task Quick Configuration



- Select a GitLab connector and its project

1. Select a Server from the Integration Connectors list – Click "Select" in the Server Name
2. Select Project Name and Issue Type. This is the project folder where RidgeBot will put newly created case with the selected issue type. The Project Name/ID and Issue Type Name/ID are the categories created by user in the selected GitLab.
3. Security findings selection allows the user to select a category that will automatically generate a GitLab case.

- After the task is finished, check the vulnerabilities list to see if the cases have been created in the "DevSecOps Status" column.

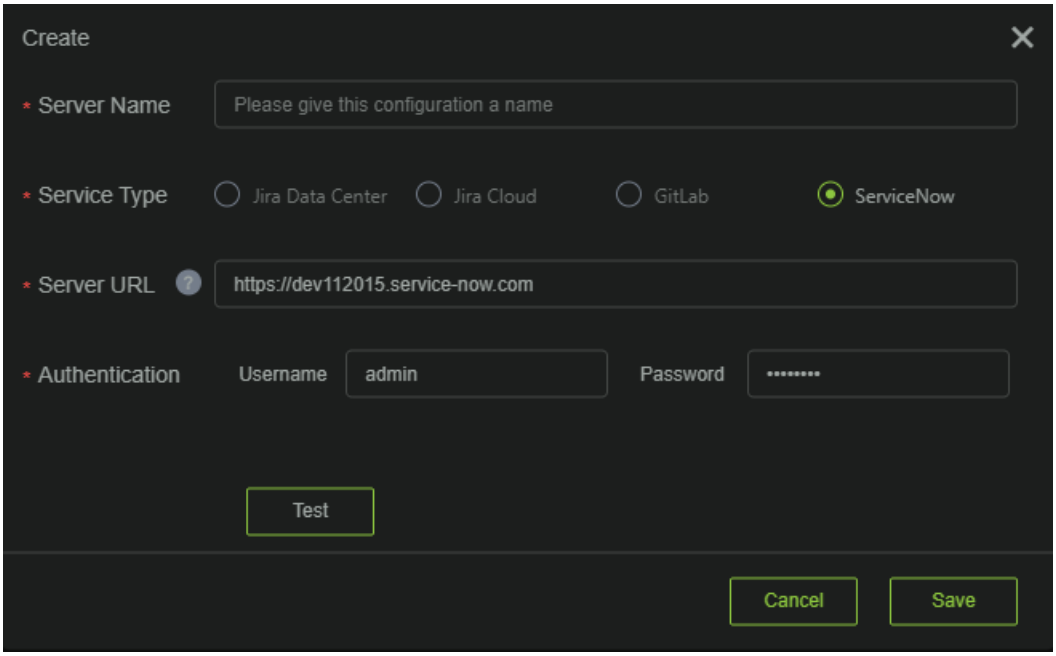


ServiceNow Integration

Connect to ServiceNow

Please make sure you have the admin account and password for the development portal.

To setup ServiceNow, go to the "Assets" tab and select "Integration Connectors", then click "Create", a dialog box will open up.

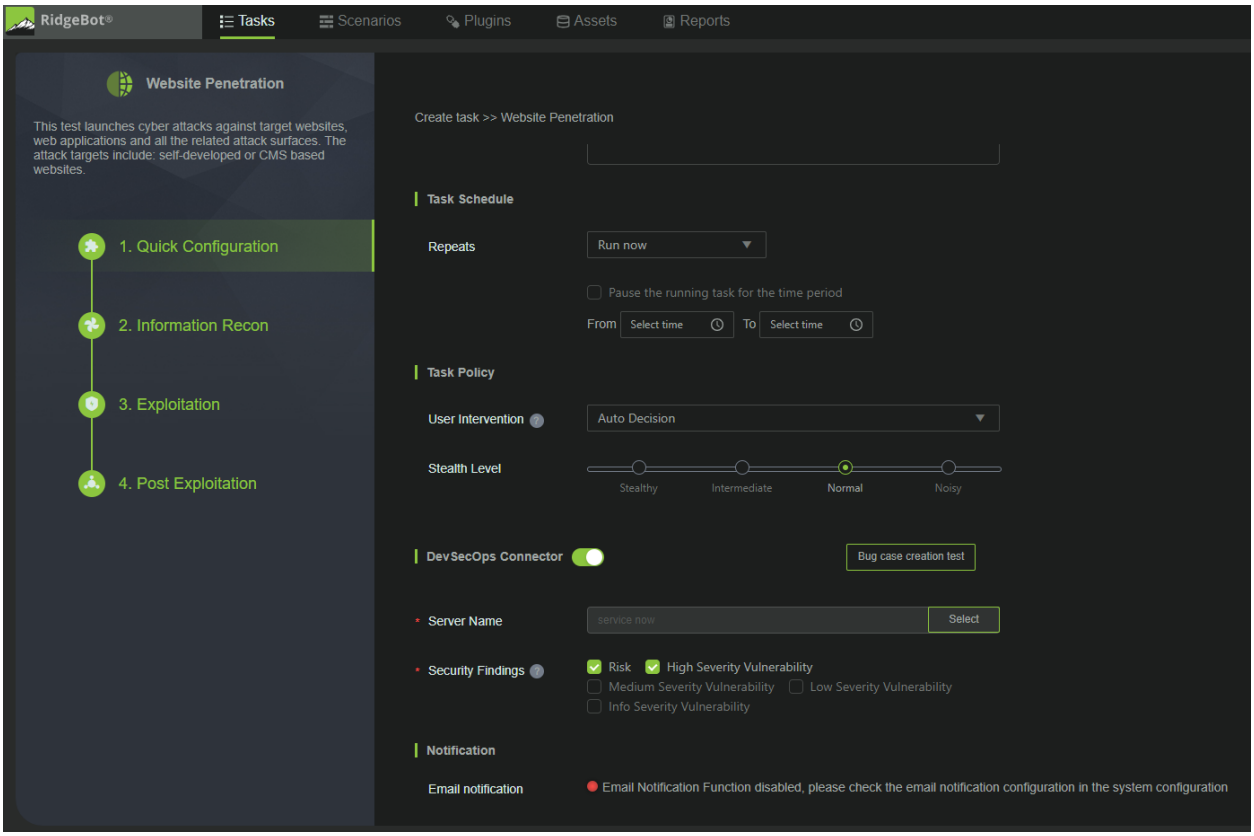


Select "ServiceNow" and input all required information. Then click test. Please NOTE that your instance in ServiceNow need to be active in order for this test to be successful. Otherwise, the connection will fail. If the test is successful, click "Save" to save the connector.

The Integration Connectors will list the ServiceNow connector for each server with the connector status. User can modify or delete the connector from the option in Operation.

Create instances in ServiceNow

Enable DevSecOps in the Task Quick Configuration



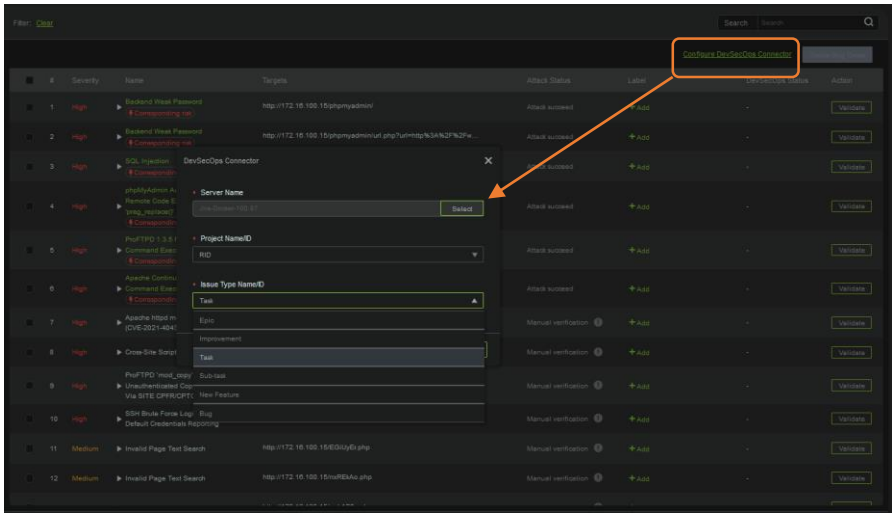
Select a ServiceNow connector.

Security findings selection allows the user to select a category that will automatically generate a ServiceNow case.

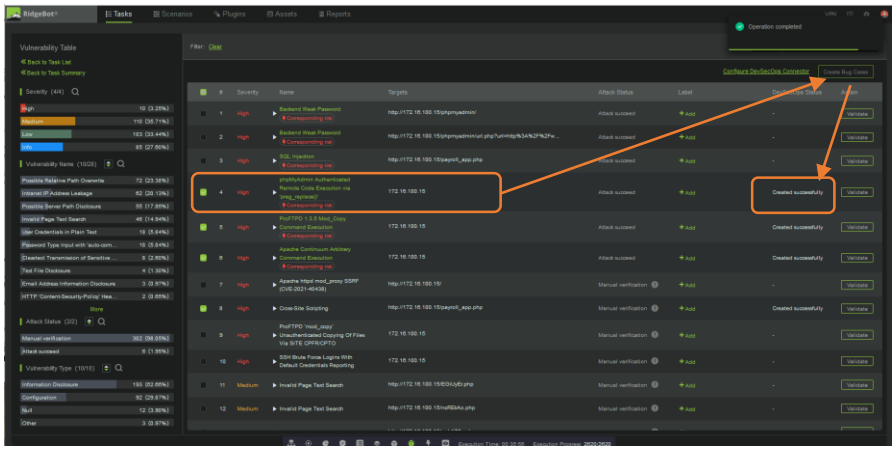
After the task is finished, check the vulnerabilities list to see if the cases have been created in the "DevSecOps Status" column.

Open a Jira, GitLab or ServiceNow case manually

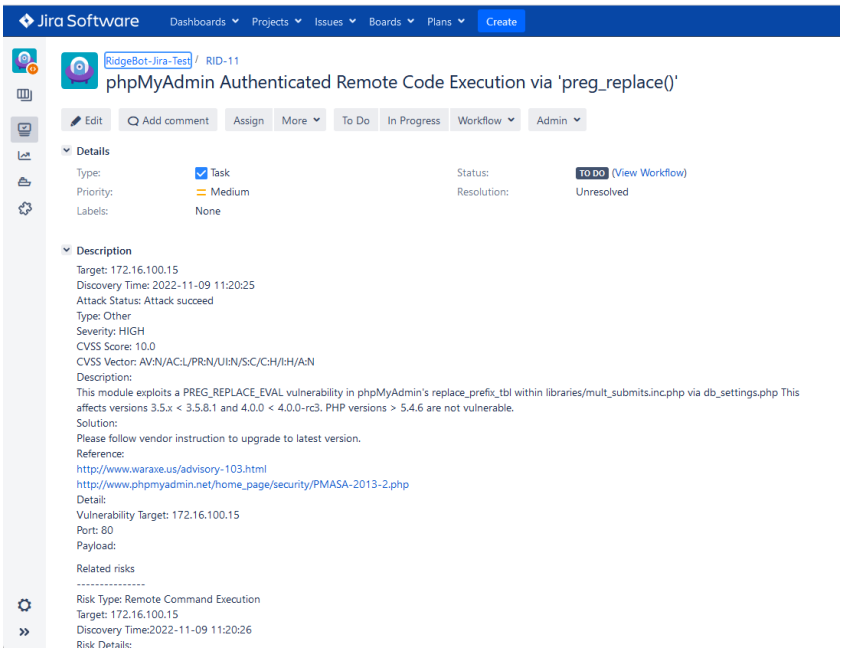
- This operation can only be done after the task is completely finished.
- Open task's vulnerability table. Click on the "ConfigureDevSecOps Connector" and Select a Jira server, a GitLab server, or a ServiceNow server and its project from a task vulnerability table



- Select the desired vulnerabilities and then click the "create bug cases" button. The DevSecOps Status shows "Created successfully" in the status column.



- Example of a Jira case opened by RidgeBot. In Jira Server – user needs to review and updates the Jira cases accordingly.


Jira Software
Dashboards
Projects
Issues
Boards
Plans
Create
RidgeBot-Jira-Test / RID-11
phpMyAdmin Authenticated Remote Code Execution via 'preg_replace()'
Edit
Add comment
Assign
More
To Do
In Progress
Workflow
Admin
Details
Type: Task
Priority: Medium
Labels: None
Status: TO DO (View Workflow)
Resolution: Unresolved
Description
Target: 172.16.100.15
Discovery Time: 2022-11-09 11:20:25
Attack Status: Attack succeed
Type: Other
Severity: HIGH
CVSS Score: 10.0
CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N
Description:
This module exploits a PREG_REPLACE_EVAL vulnerability in phpMyAdmin's replace_prefix_tbl within libraries/mult_submits.inc.php via db_settings.php This affects versions 3.5.x < 3.5.8.1 and 4.0.0 < 4.0.0-rc3. PHP versions > 5.4.6 are not vulnerable.
Solution:
Please follow vendor instruction to upgrade to latest version.
Reference:
http://www.waraxe.us/advisory-103.html
http://www.phpmyadmin.net/home_page/security/PMASA-2013-2.php
Detail:
Vulnerability Target: 172.16.100.15
Port: 80
Payload:
Related risks

Risk Type: Remote Command Execution
Target: 172.16.100.15
Discovery Time:2022-11-09 11:20:26
Risk Details:

Appendices

Reference Documents

- RidgeBot™ Deployment QuickStart Guide
- RidgeBot™ Release Notes
- RidgeBot™ API user Guide
- RidgeBot™ API Reference
- RidgeBot™ POC Best Practice Guideline

Q&A

Q: Where can I find the RidgeBot documents?

A: RidgeBot documents are available in the Ridge Security Partner Portal.

Q: During initial installation, I get a License Validation File error when upload the license file.

A: Please check the following:

- Refresh your web browser and upload the license file again.
- In the RidgeBot management console, run "service-restart" and then refresh your web browser and upload the license file again.
- Check that the machine code is correct.
- Click Close on the License dialog box, login as admin and then upload the license file from the RidgeBot System->About page.
- If the above steps are unable to resolve license file validation, you need to re-install the RidgeBot software.

Q: Using offline upgrade to update the software or plugin library, why does the System Information still show the previous version of the software or plugin library?

A: Please check the following:

- Refresh your web browser.
- Before uploading the upgrade file, make sure the previous version has been removed (if there is a filename in the dialog box, click delete to remove it before uploading the latest version of the software).

Q: Why can't I access the RidgeBot System?

A: Please check your environment for the following:

- Whether the HTTPS protocol is used, and whether HTTPS is the right protocol.
- Whether the IP address, DNS and gateway are configured properly.
- Whether the network connection is correct.

Q: What type of user can do a license authentication?

A: Users with a system administrator role can import the license file from the About page. One exception is that the installer can upload the license file during the first login onto Ridgebot during installation.

Q: Why don't I receive a task report when the task completes, even though email notification is configured for the task?

A: No email is sent when a report generation fails.

Q: What do I do if a report generation fails?

A: Click retry to regenerate the report.

Q: Why does a task is finish without test results?

A: Check whether the target is reachable.

Q: Why is a specific target not shown in the topology map?

A: RidgeBot does not display an un-detected object in the topology map.

Q: Does RidgeBot interfere with targets' execution due to its large number of threads?

A: The PT operation is safe if the target is used as a common server. There are general guidelines to reduce the risks on the target during Penetration testing.

Q: When a user launches multiple tasks in RidgeBot, why is a task Progress is in "Queuing"?

A: RidgeBot has reached the concurrent task limit. Any task above this limit will be in a Queue. When a task is completed, RidgeBot will automatically start another task in the Queuing state.

Q: When a user launches multiple tasks in RidgeBot, one of the tasks sometimes does not make any progress?

A: The RidgeBot web crawler is assigned to one task at a time. If multiple tasks require the web crawler, the remaining tasks wait until web crawler becomes available.

Q: Why I can not install Botlet in Windows 10/11 or Windows Server 2016 or later?

A: In Release 4.0.x, the Botlet does not have the digital certificate. Therefore, it can not be installed in Windows with the Microsoft Defender or antivirus. This is a known issue that will be addressed in future release.