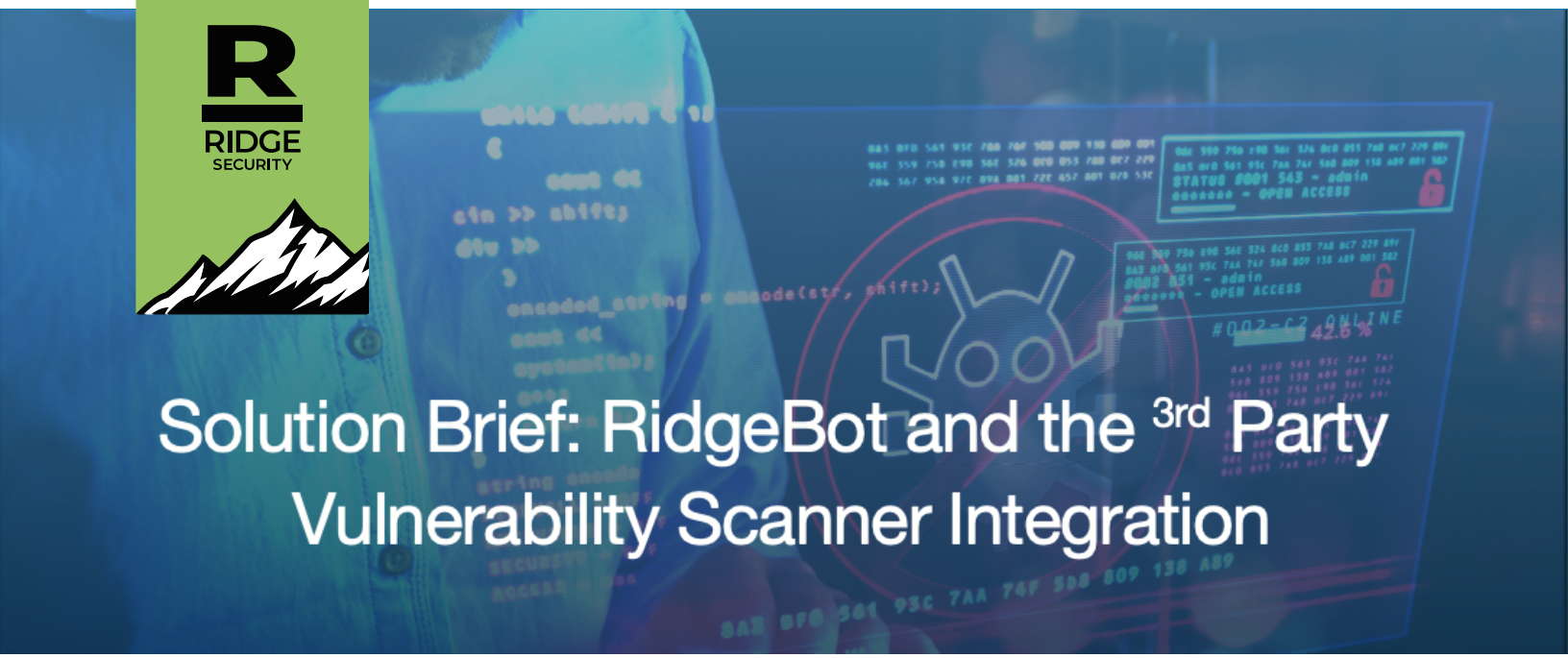

The integrated solution of RidgeBot and the 3rd party vulnerability scanner offers customers an efficient and risk-based vulnerability management approach. This solution combines the capabilities of two powerful tools - Nessus and Nexpose - with RidgeBot's advanced vulnerability exploitation and validation technology.

Nessus and Nexpose are popular third-party vulnerability scanners that provide customers with comprehensive vulnerability management capabilities. They scan systems for vulnerabilities, prioritize them based on risk, and provide reports that help customers understand their security posture.

RidgeBot is an AI-powered penetration testing tool that can exploit and validate vulnerabilities to determine whether they pose a real threat to the customer's environment. By leveraging RidgeBot's advanced capabilities, customers can prioritize their vulnerability remediation efforts based on the actual risk of exploitation.

Using the pre-built scenario called "3rd Party Scanning Result Validation," users can easily import Nessus vulnerability tables into RidgeBot for further validation. RidgeBot will exploit and validate these vulnerabilities to determine whether they can be successfully exploited in the customer's environment. Any vulnerabilities that are successfully exploited are deemed as risks and become the highest priority for customers to fix.

This integrated solution offers a risk-based approach to vulnerability management for existing Tenable and Rapid 7 customers. By prioritizing the highest risk vulnerabilities, customers can effectively allocate resources to fix critical vulnerabilities and reduce the overall risk in their environment.

Overall, the integrated solution of RidgeBot and the 3rd party vulnerability scanner provides customers with an efficient and effective way to manage vulnerabilities and prioritize their remediation efforts based on the actual risk of exploitation.

Figure 1: The pre-built 3rd party scanning result validation scenario

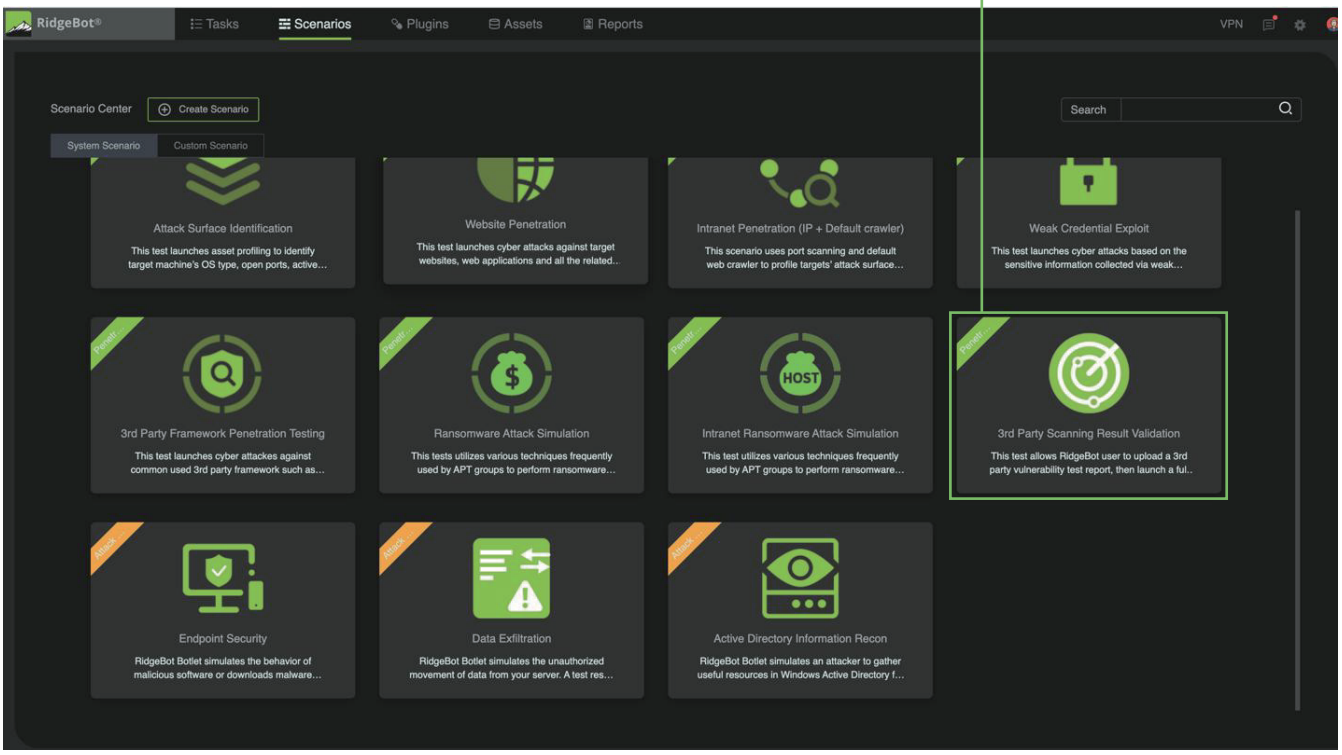

Figure 2: Sample Report for Validating Nessus Vulnerability Findings

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output	Host Active	RidgeBot Discovered	RidgeBot Exploited
84215	CVE-2015-	10	Critical	172.16.10	tcp	21	ProFTPD m	The remote host is running a ProFTPD module that is affected by an information disclosure vulnerability.	The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.	Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.	http://bug	Nessus received a 350 response from sending the following unauthenticated request : SITE CPFR /etc/passwd	TRUE	TRUE	TRUE
********	********	********	********	********	********	********	**********	**********	**********	********	********	**********	**********	**********	**********
				Additional risks and vulnerabilities discovered by RidgeBot penetration testing											
	CVE-2013-	10	HIGH	172.16.10	http	80	phpMyAdmin Authenticat		This module exploits a PREG_REPLACE_	Please follow vendor	http://www.wara xe.us/adv		TRUE	TRUE	TRUE
		8.6	HIGH	http://172	http	80	Backend Weak Password		When the application permits weak pa	1.Implement multi-fact	https://owasp.org /www-pr		TRUE		TRUE
		10	HIGH	172.16.10	http	8080	Apache Continuum Arbitr		This module exploits a command inject	At present, th			TRUE		TRUE
		8.6	HIGH	http://172	http	80	Backend Weak Password		When the application permits weak pa	1.Implement	https://owasp.org		TRUE		TRUE
	CVE-2016-	10	HIGH	172.16.10	http	3500	Ruby on Rails ActionPack		This module exploits a remote code ex	At present, the			TRUE	TRUE	TRUE
		8.6	HIGH	http://172	http	80	SQL Injection		An SQL Injection vulnerability may affe	The only sure way	https://www.owas		TRUE		TRUE

Figure 3: Sample Report for Validating Nexpose Vulnerability Findings

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
********	********	********	********	********	********	**********	********	**********	**********	********	********	********	**********		
				Additional risks and vulnerabilities discovered by RidgeBot penetration testing											
CVE	CVSS v2.0	Risk	IP	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Out	Host Activ	RidgeBot Discovered	RidgeBot Exploited	
CVE-2021-	9.8	HIGH	172.16.10	ssl/http	443	Exchange Server Remote Code Execution (CVE-2021 -34523)		Three vulnerabilities exist in Exchange, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, forming a chain of exploits that allow attackers to gain privileges on windows servers	Install the latest security patches	http://packetstorms		TRUE	TRUE		
	0	INFO	172.16.10	ssl/http	443	Microsoft IIS Version Disclosure		The HTTP responses returned by this web application include a header named 'Server'. The value of this header includes the version of Microsoft IIS server.	Microsoft IIS should be configured to remove unwanted HTTP response headers from the response.	https://owasp.org/w		TRUE	TRUE		
	0	INFO	172.16.10	ssl/http	443	Password Type Input with auto-comp lete Enabled		When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the clear-text password from the browser cache.	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: INPUT TYPE="password" AUTOCOMPLETE="off".	https://owasp.org/w		TRUE	TRUE		
	0	INFO	172.16.10	ssl/http	443	Exchange Mail Domain Info Leak		Get the FQDN of the exchange server by requesting the page		https://docs.microsc		TRUE	TRUE		