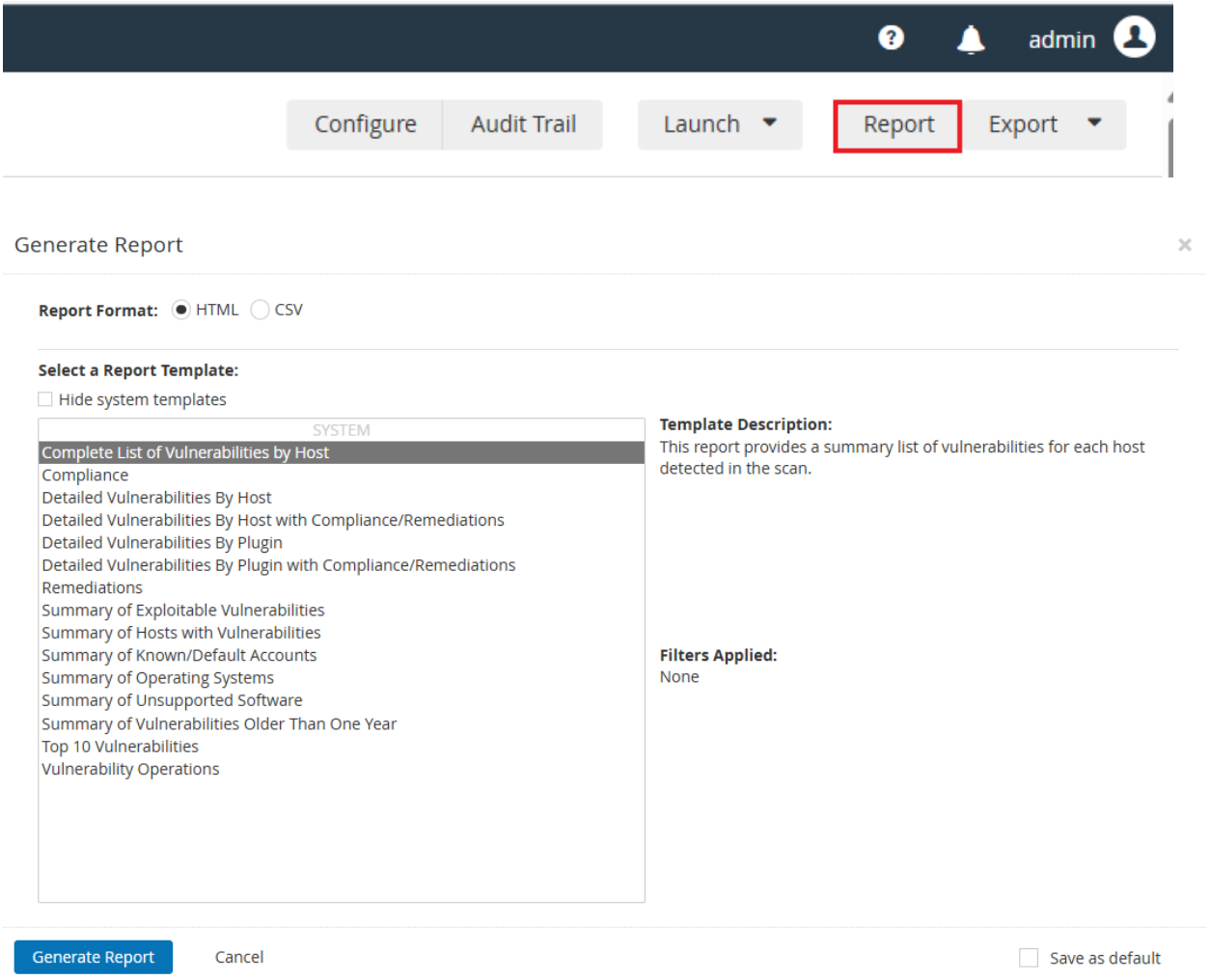
Reports Lab:



tenable Nessus

Report generated by Tenable Nessus™

Active-Directory-SCAN

Thu, 08 May 2025 12:07:23 EEST

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
34	38	6	0	99

Show

Exploitable Vulnerabilities: Top 25

The Exploitable Vulnerabilities: Top 25 table uses the plugin attribute "exploit_available" to identify software that has working exploits in the wild. The data is then sorted using the count, which is a representation of the affected hosts. While some plugins may be present more than one time on a single host, for the most part a plugin will only be present once on each host. This list of vulnerabilities exposes the organization to many different attach frameworks and script kiddie attacks. These vulnerabilities should be prioritized and the software removed or updated to a supported version as soon as possible.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Count
MEDIUM	171859	Curl Use-After-Free < 7.87 (CVE-2022-43552)	2
CRITICAL	151571	Mozilla Firefox < 90.0	1
CRITICAL	155917	Mozilla Firefox < 95.0	1
CRITICAL	156606	Mozilla Firefox < 96.0	1
CRITICAL	157443	Mozilla Firefox < 97.0	1
CRITICAL	158654	Mozilla Firefox < 97.0.2	1
CRITICAL	158694	Mozilla Firefox < 98.0	1
CRITICAL	160465	Mozilla Firefox < 100.0	1
CRITICAL	162602	Mozilla Firefox < 102.0	1

Active-Directory-SCAN

Thu, 08 May 2025 12:07:23 EEST

TABLE OF CONTENTS

TABLE OF CONTENTS

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 96% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Mozilla Firefox < 138.0: Upgrade to Mozilla Firefox version 138.0 or later.	668	1
PuTTY < 0.81 Key Recovery Attack Vulnerability: Upgrade to PuTTY version 0.81 or later.	2	1
Curl Use-After-Free < 7.87 (CVE-2022-43552): Upgrade Curl to version 7.87.0 or later	1	1
WinSCP < 6.3.3 Key Recovery Attack Vulnerability: Upgrade to WinSCP version 6.3.3 or later.	1	1