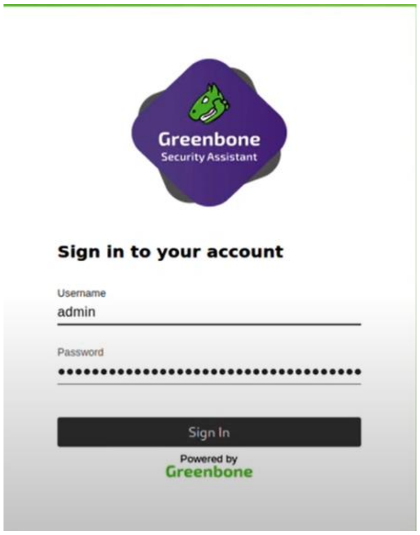
Goal: Identify the tools and techniques to be used to scan for vulnerabilities.

Procedure: List out the tools you plan on using to perform vulnerability scanning and how you will use them. Include both Tenable Nessus and OpenVAS.

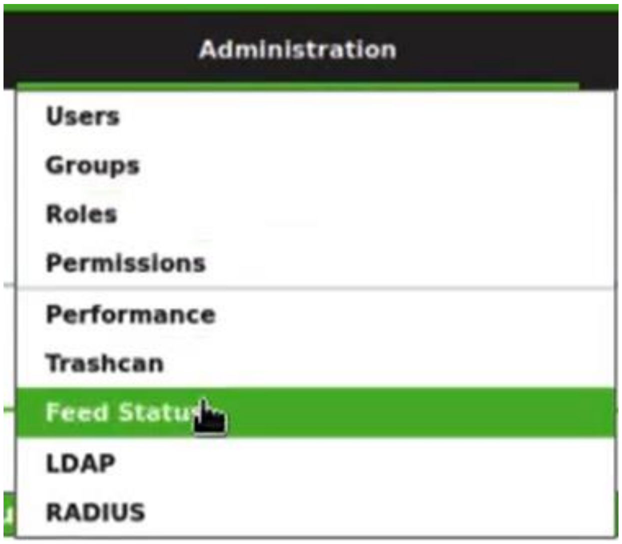
- Tool: OpenVAS
    - Usage:
        - Install and immediately change the admin password
        - Check to make sure that the application and it's feed are up to date
        - I choose to scan every port. << Always check with the client if they have a specified list of ports you can and can't scan
        - Full and fast was the option chosen
        - Set the defaults needed to set up a scan and import the ip or the ip list that will be scanned
        - After awhile the vulnerabilities will show up with a lot of helpful information that can be used for an attacker or to help remedy the vulnerabilities
            - For instance, the application will even give you links to where you can find updates, patches, configurations, etc. that will fix the vulnerability in question.
            - However, some vulnerabilities didn't have fixes. So, those will be tricky to fix but could be very exciting for an attacker since these could take longer, could have poor work arounds, etc.
    - Screenshots:

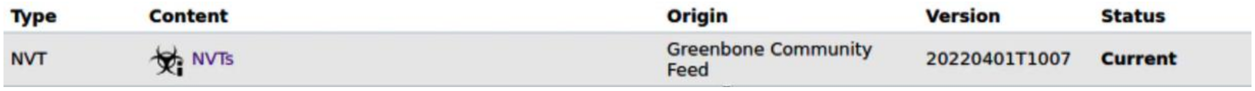
- 

Sign in to your account

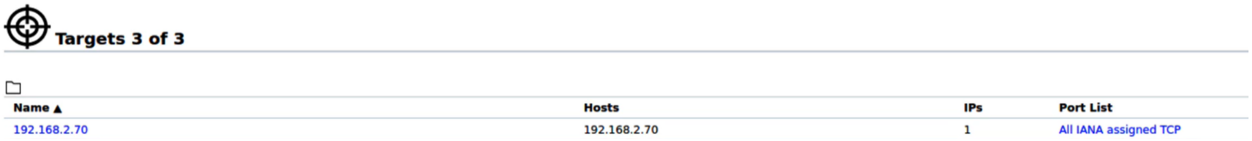
Username
admin

Password
••••••••••••••••••••••••••••••••••••

- 

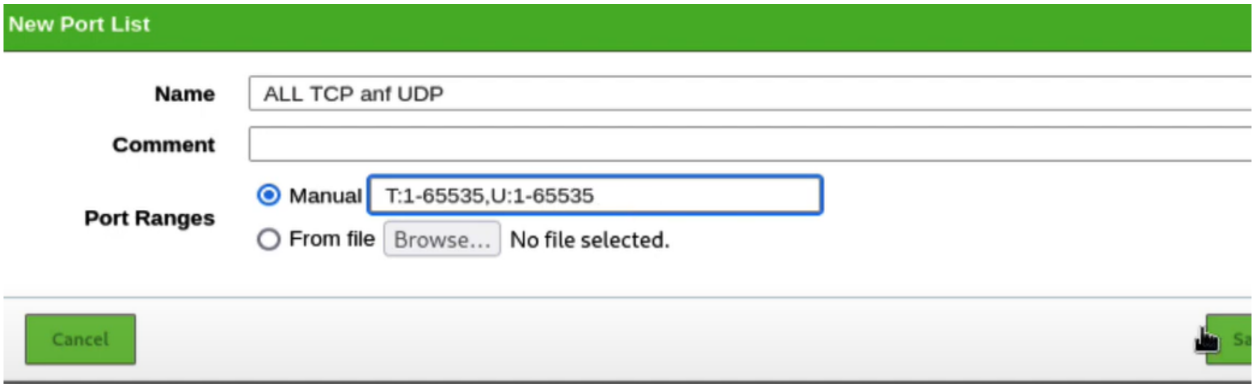


Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20220401T1007	**Current**



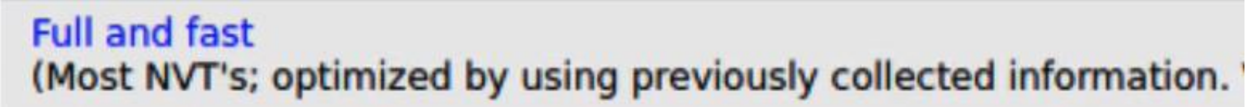
Targets 3 of 3

Name ▲	Hosts	IPs	Port List
192.168.2.70	192.168.2.70	1	All IANA assigned TCP

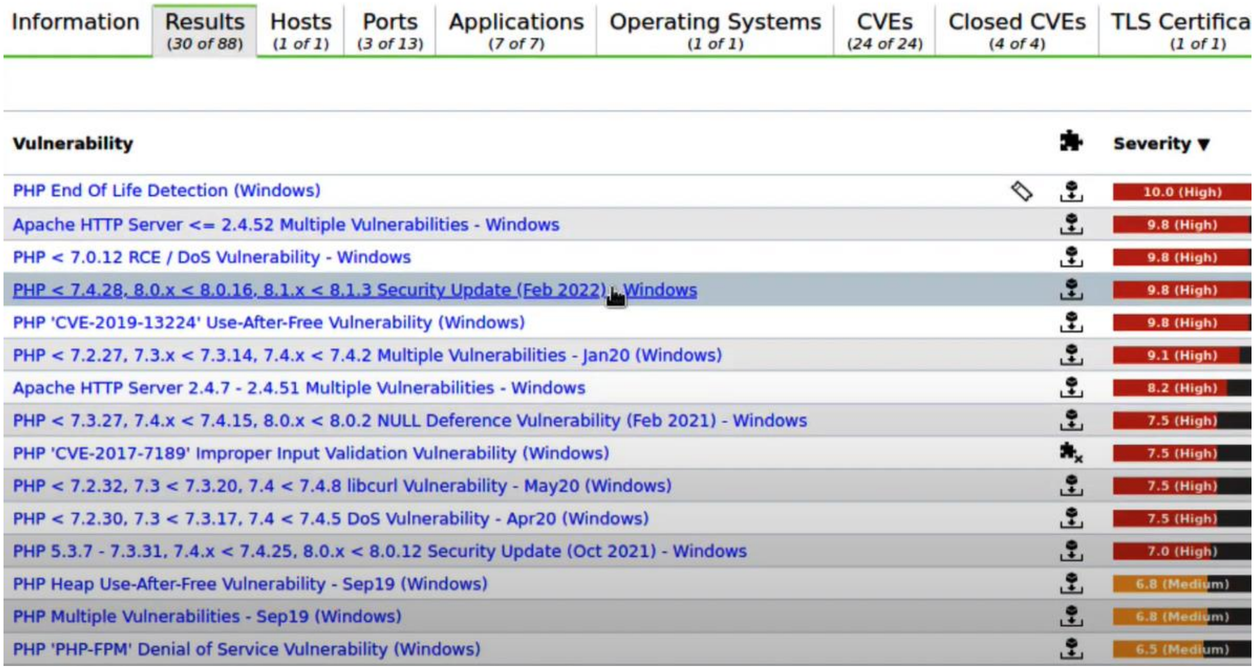


New Port List

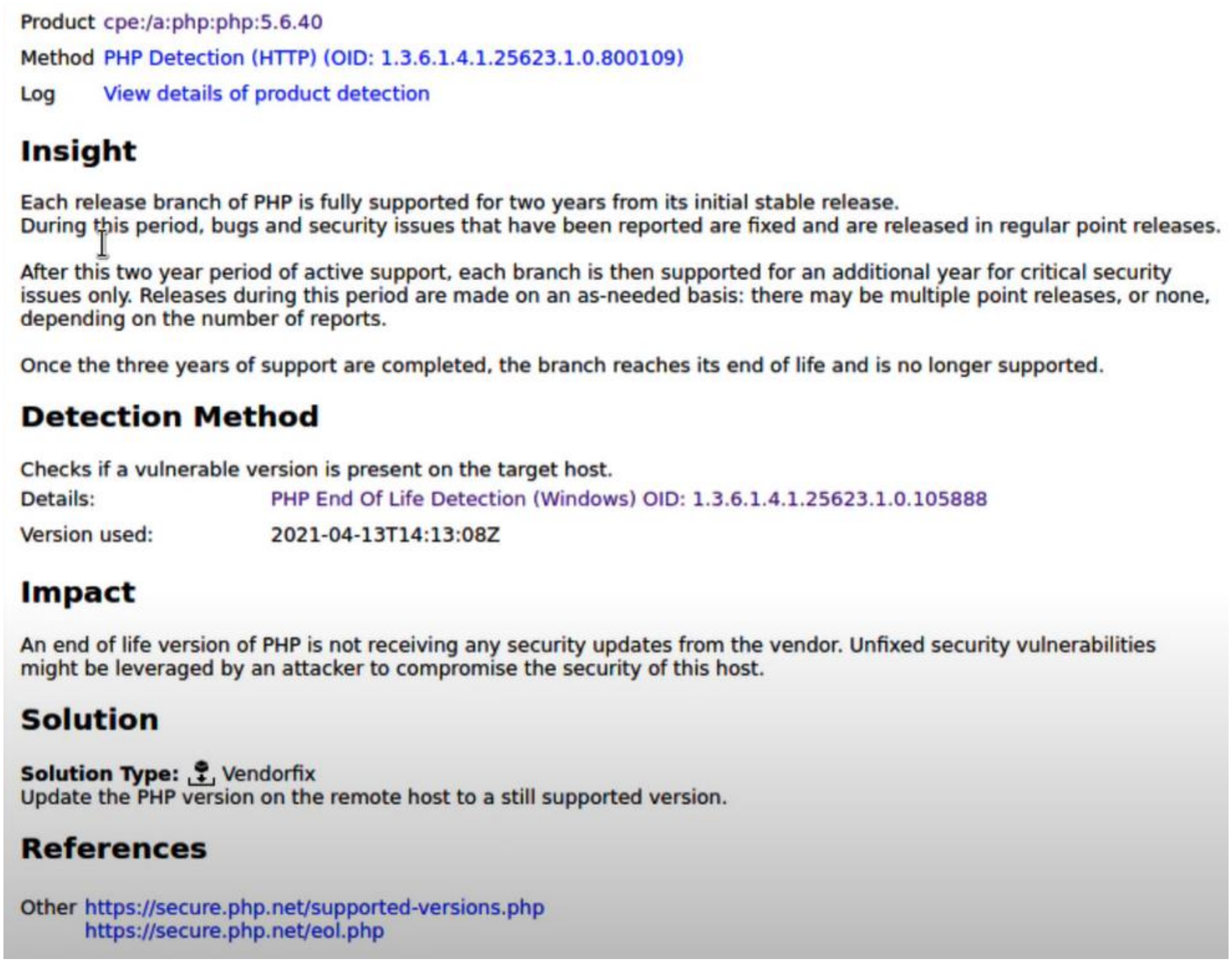
Name	ALL TCP anf UDP
Comment	
Port Ranges	● Manual T:1-65535,U:1-65535
	○ From file Browse… No file selected.



Full and fast
(Most NVT's; optimized by using previously collected information.



Vulnerability	Severity ▼
PHP End Of Life Detection (Windows)	10.0 (High)
Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Windows	9.8 (High)
PHP < 7.0.12 RCE / DoS Vulnerability - Windows	9.8 (High)
PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows	9.8 (High)
PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)	9.8 (High)
PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)	9.1 (High)
Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Windows	8.2 (High)
PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Windows	7.5 (High)
PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows)	7.5 (High)
PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 libcurl Vulnerability - May20 (Windows)	7.5 (High)
PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)	7.5 (High)
PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Windows	7.0 (High)
PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)	6.8 (Medium)
PHP Multiple Vulnerabilities - Sep19 (Windows)	6.8 (Medium)
PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)	6.5 (Medium)



Product cpe:/a:php:php:5.6.40

Method PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Log View details of product detection

Insight

Each release branch of PHP is fully supported for two years from its initial stable release.
During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.

After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.

Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Detection Method

Checks if a vulnerable version is present on the target host.

Details:	PHP End Of Life Detection (Windows) OID: 1.3.6.1.4.1.25623.1.0.105888
Version used:	2021-04-13T14:13:08Z

Impact

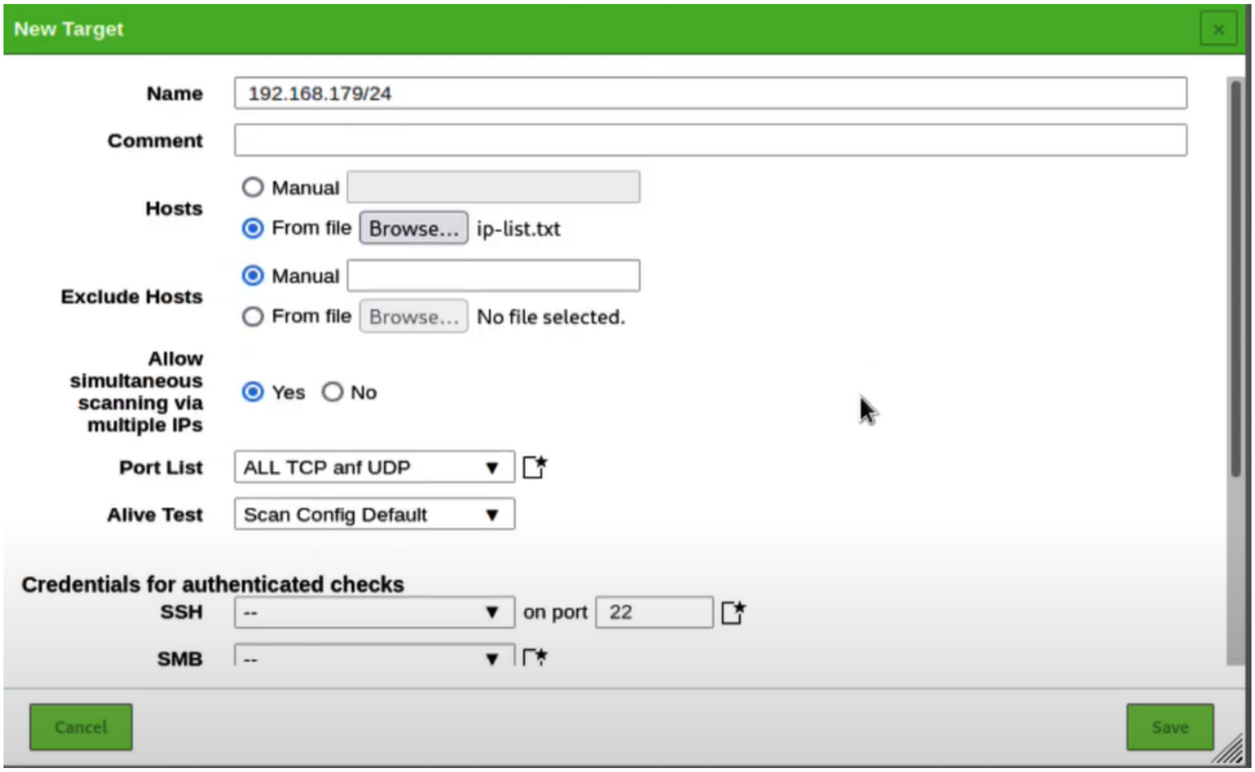
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution Type: Vendorfix
Update the PHP version on the remote host to a still supported version.

References

Other https://secure.php.net/supported-versions.php
https://secure.php.net/eol.php



New Target

Name: 192.168.179/24

Comment:

Hosts: ○ Manual ● From file Browse... ip-list.txt

Exclude Hosts: ● Manual ○ From file Browse... No file selected.

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

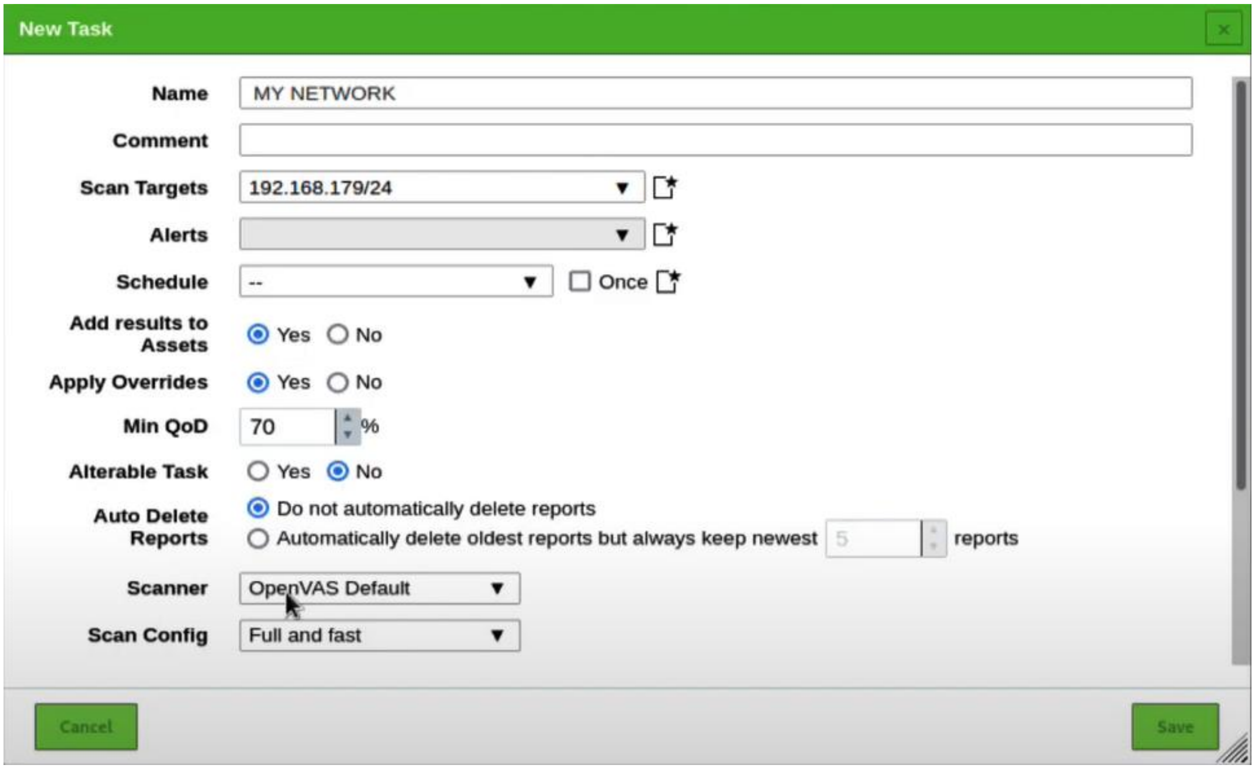
Port List: ALL TCP anf UDP

Alive Test: Scan Config Default

Credentials for authenticated checks

SSH: -- on port 22

SMB: --



New Task

Name: MY NETWORK

Comment:

Scan Targets: 192.168.179/24

Alerts:

Schedule: -- □ Once

Add results to Assets: ● Yes ○ No

Apply Overrides: ● Yes ○ No

Min QoD: 70 %

Alterable Task: ○ Yes ● No

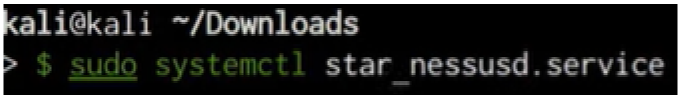
Auto Delete Reports: ● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports

Scanner: OpenVAS Default

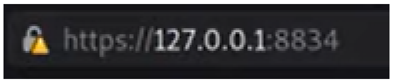
Scan Config: Full and fast

- Pros:
  - Very user friendly

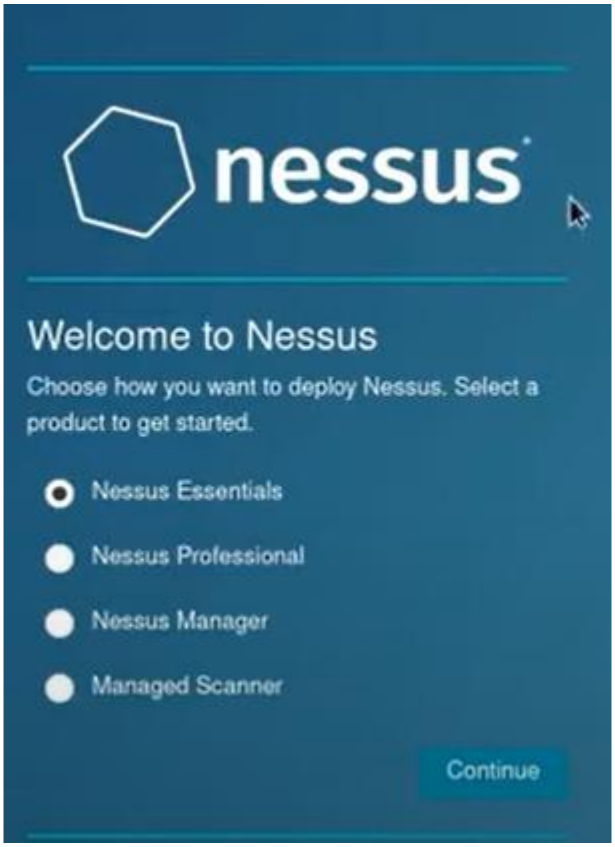
        - Fast
        - Configurations are straightforward and if not, plenty of documentation and tutorials are online.
    - Cons:
        - Need extensive knowledge to set up custom scans.
        - Some scans scan for different things, so you have to make sure you know what you’re looking for and what will or will not come up with said chosen scan.
- Tool: Tenable Nessus
    - Usage:
        - Install Nessus by downloading the needed package from it’s site and using dpkg (if using kali)
        - Then use systemctl to run Nessus when completed
        - Bring up the local host and go to port 8834
        - Select the version for the penetration test
        - Create a strong password for the admin account
        - Check to make sure Nessus is fully updated
        - Verify all paths are correct and the ports to be scanned are ideal
        - Clicked on Host Discovery
        - Input the range of ips to be scanned
        - Set the schedule for the scan
        - Select the Host enumeration scan type
        - Leave defaults unless a change is needed and check slow down the scan when network congestion is detected if needed for the client
        - Run the scan, create reports, and use the vulnerabilities accordingly

- Screenshots:
  - 

    ```
    kali@kali ~/Downloads
    > $ sudo systemctl star_nessusd.service
    ```

  - 

    https://127.0.0.1:8834

  - 

    Welcome to Nessus

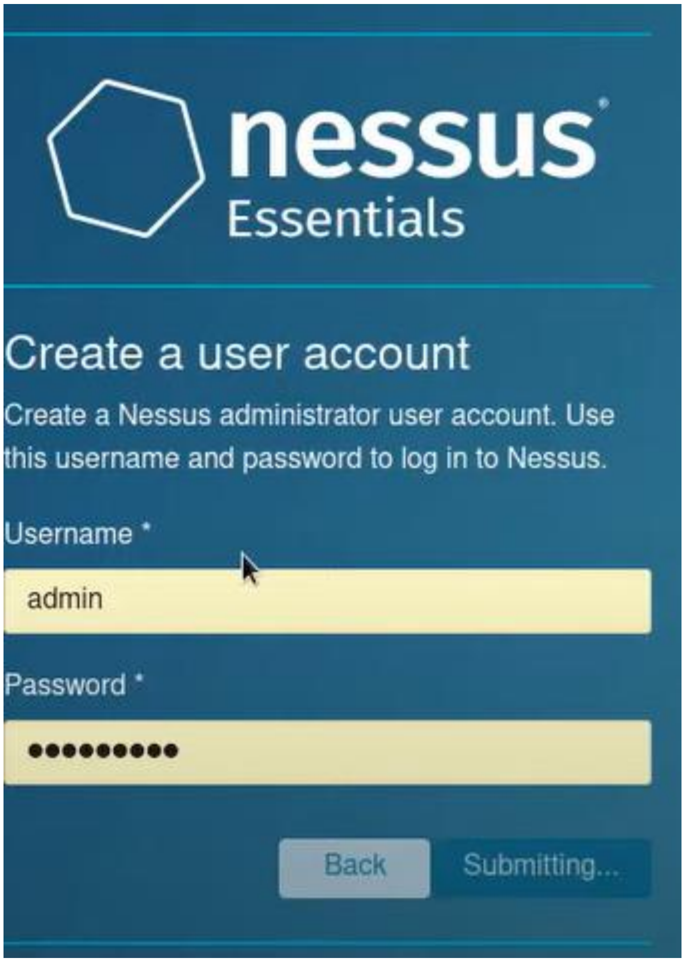
    Choose how you want to deploy Nessus. Select a product to get started.

    ● Nessus Essentials

    ○ Nessus Professional

    ○ Nessus Manager

    ○ Managed Scanner

- 

Create a user account

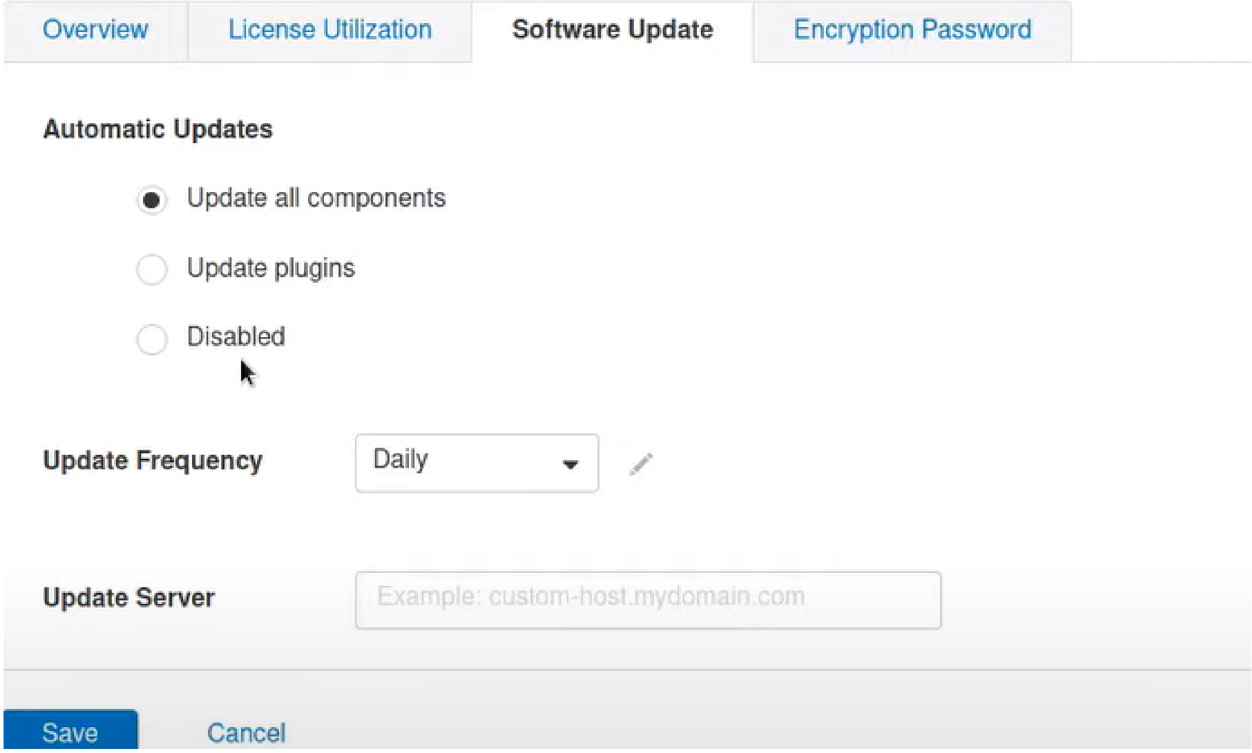
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

admin

Password *

●●●●●●●●●●



Automatic Updates

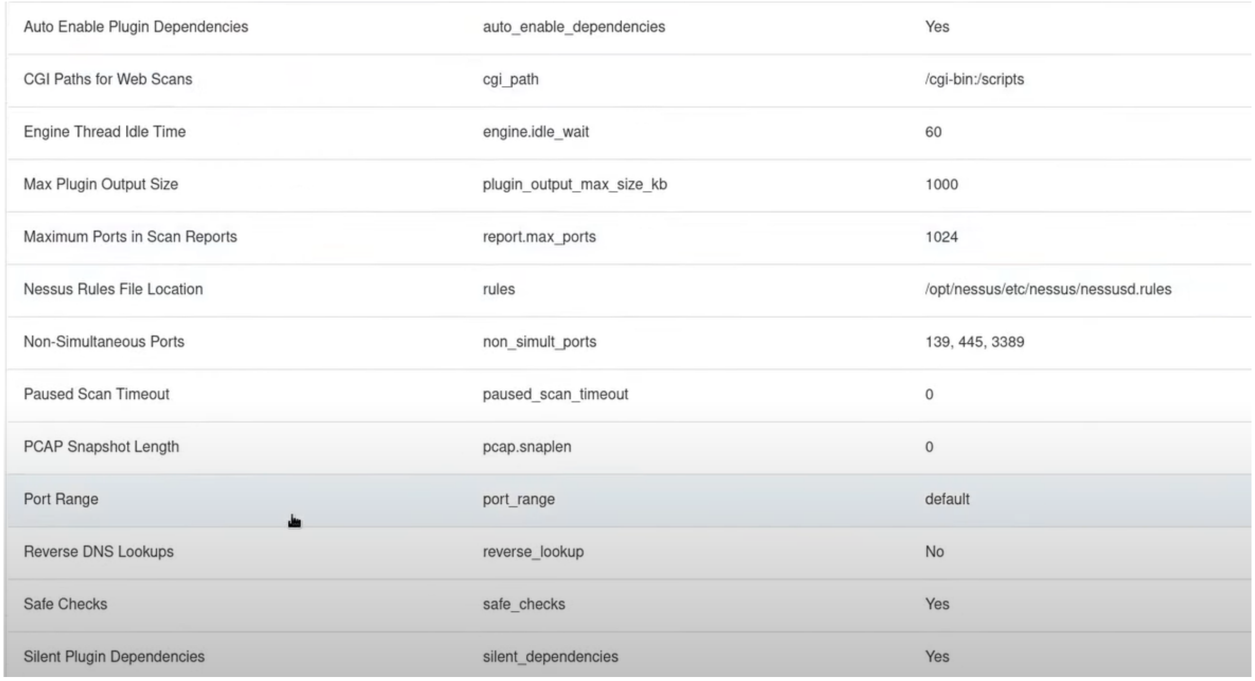
● Update all components

○ Update plugins

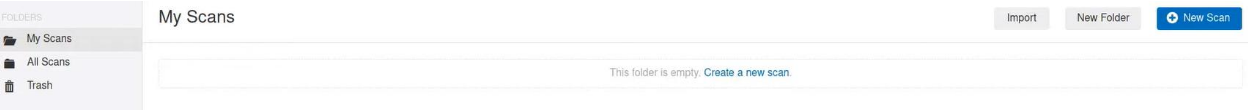
○ Disabled

Update Frequency Daily

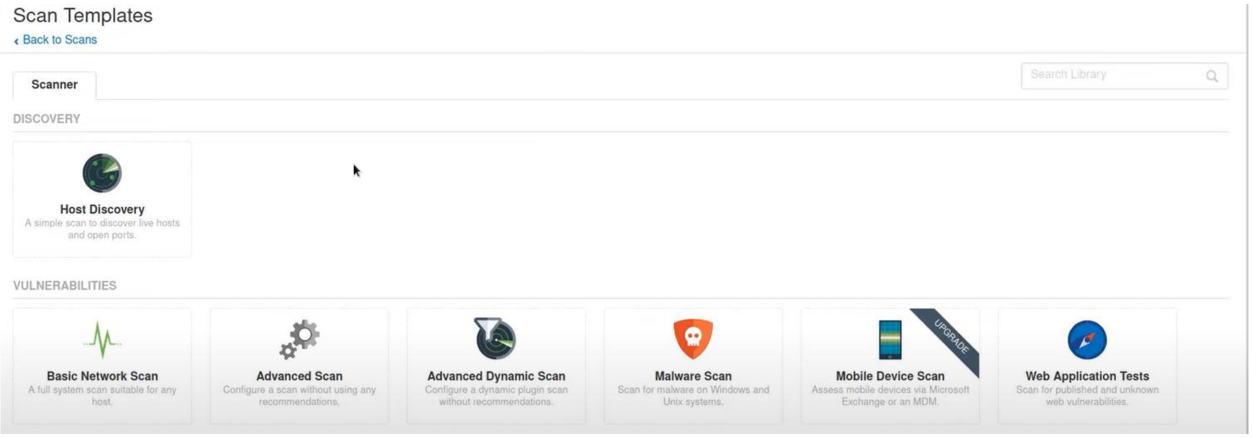
Update Server Example: custom-host.mydomain.com



Auto Enable Plugin Dependencies	auto_enable_dependencies	Yes
CGI Paths for Web Scans	cgi_path	/cgi-bin:/scripts
Engine Thread Idle Time	engine.idle_wait	60
Max Plugin Output Size	plugin_output_max_size_kb	1000
Maximum Ports in Scan Reports	report.max_ports	1024
Nessus Rules File Location	rules	/opt/nessus/etc/nessus/nessusd.rules
Non-Simultaneous Ports	non_simult_ports	139, 445, 3389
Paused Scan Timeout	paused_scan_timeout	0
PCAP Snapshot Length	pcap.snaplen	0
Port Range	port_range	default
Reverse DNS Lookups	reverse_lookup	No
Safe Checks	safe_checks	Yes
Silent Plugin Dependencies	silent_dependencies	Yes



This folder is empty. Create a new scan.



Scan Templates

‹ Back to Scans

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

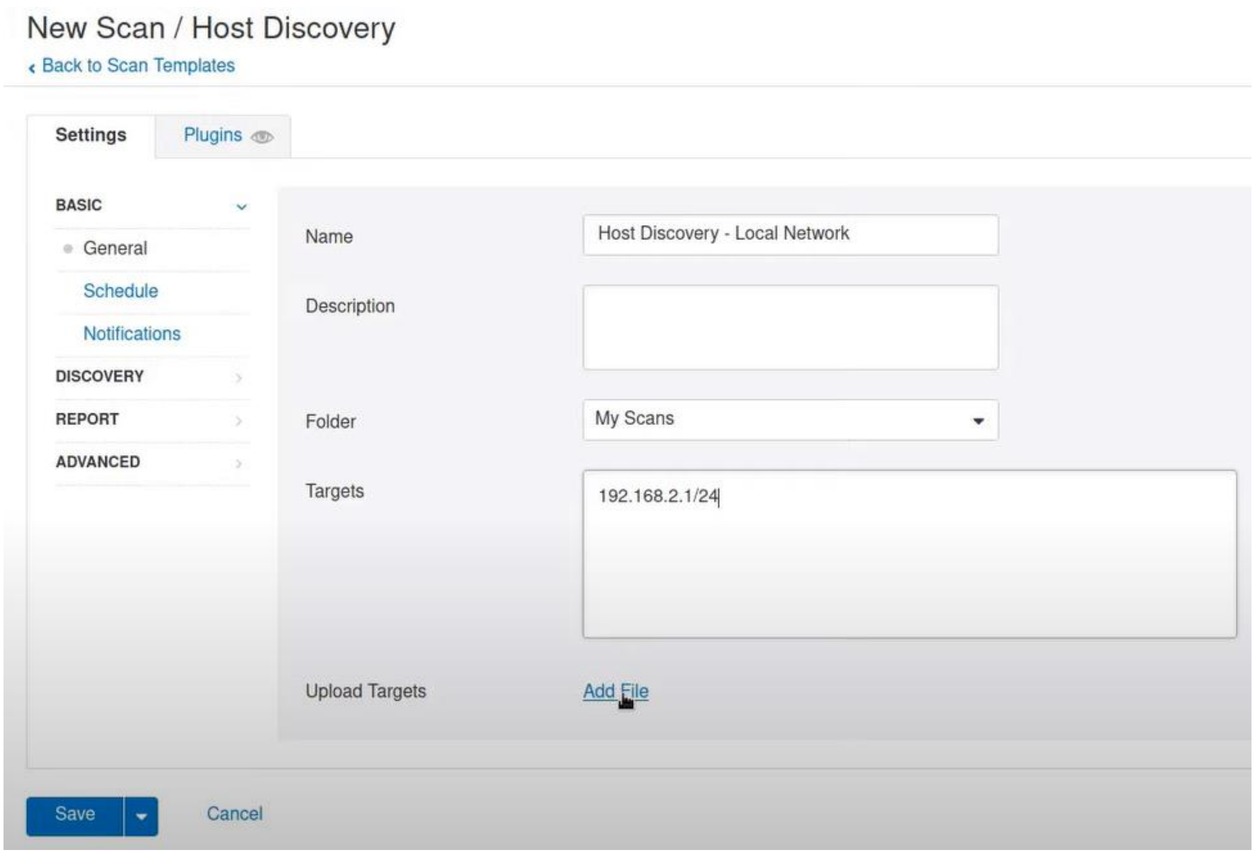
Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities.



New Scan / Host Discovery

‹ Back to Scan Templates

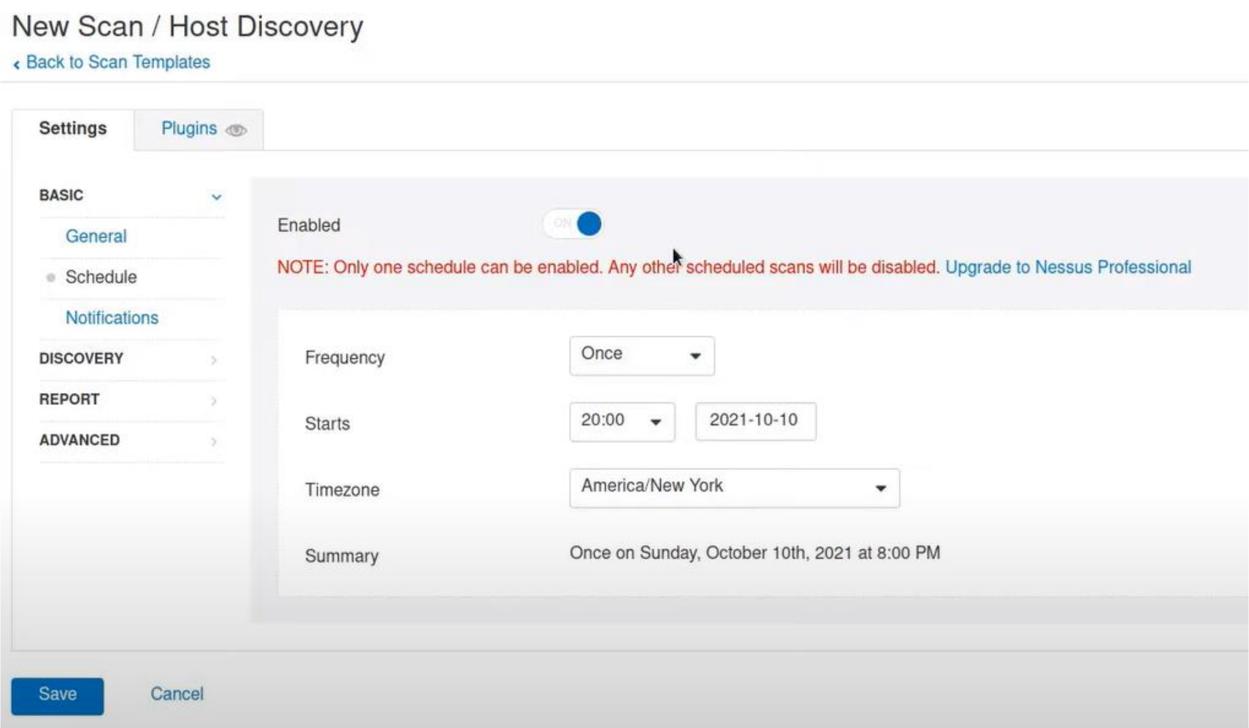
Name: Host Discovery - Local Network

Description:

Folder: My Scans

Targets: 192.168.2.1/24

Upload Targets: Add File



New Scan / Host Discovery

‹ Back to Scan Templates

Enabled: ON

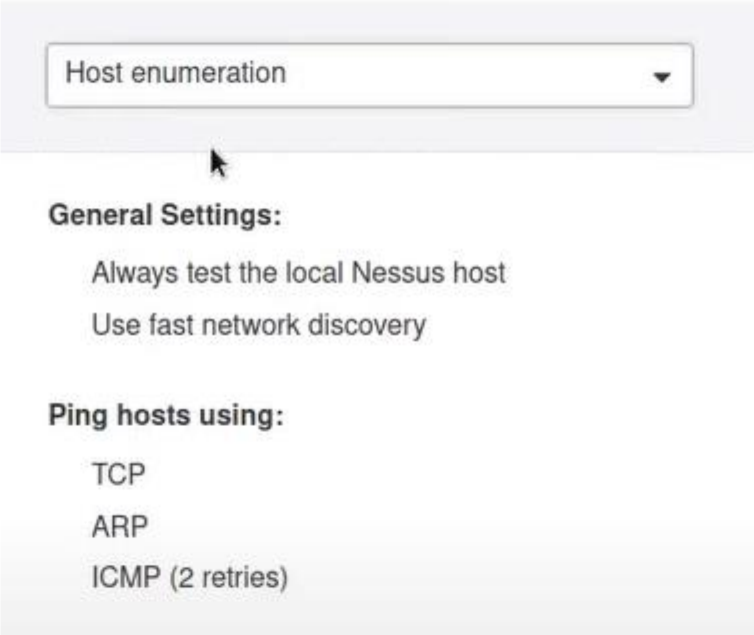
NOTE: Only one schedule can be enabled. Any other scheduled scans will be disabled. Upgrade to Nessus Professional

Frequency: Once

Starts: 20:00 2021-10-10

Timezone: America/New York

Summary: Once on Sunday, October 10th, 2021 at 8:00 PM



Host enumeration

General Settings:

Always test the local Nessus host

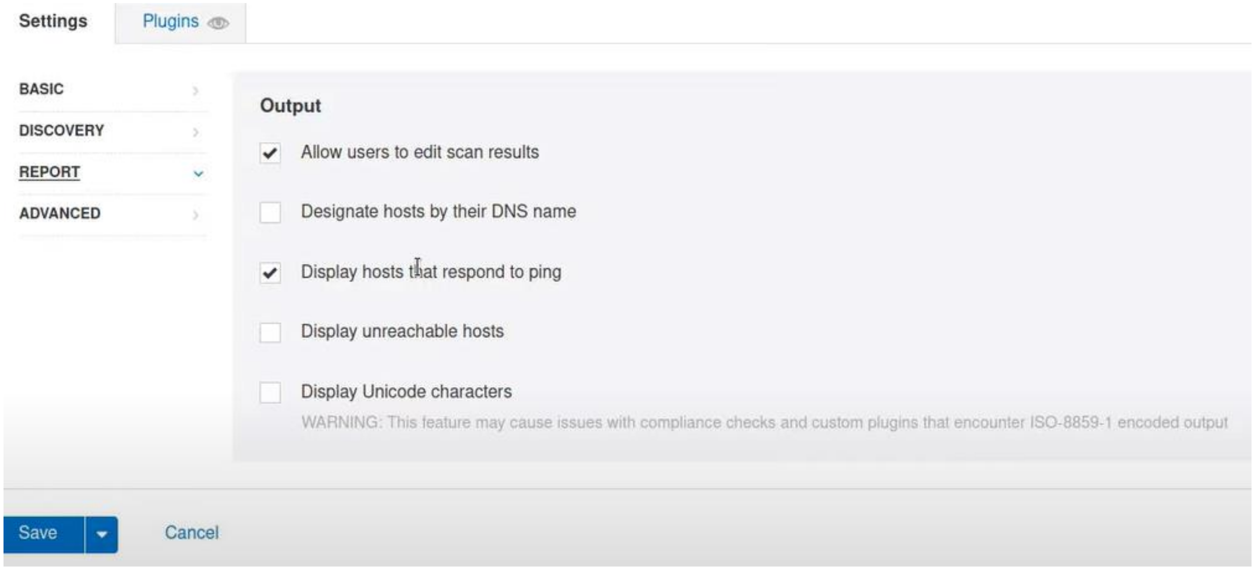
Use fast network discovery

Ping hosts using:

TCP

ARP

ICMP (2 retries)



Output

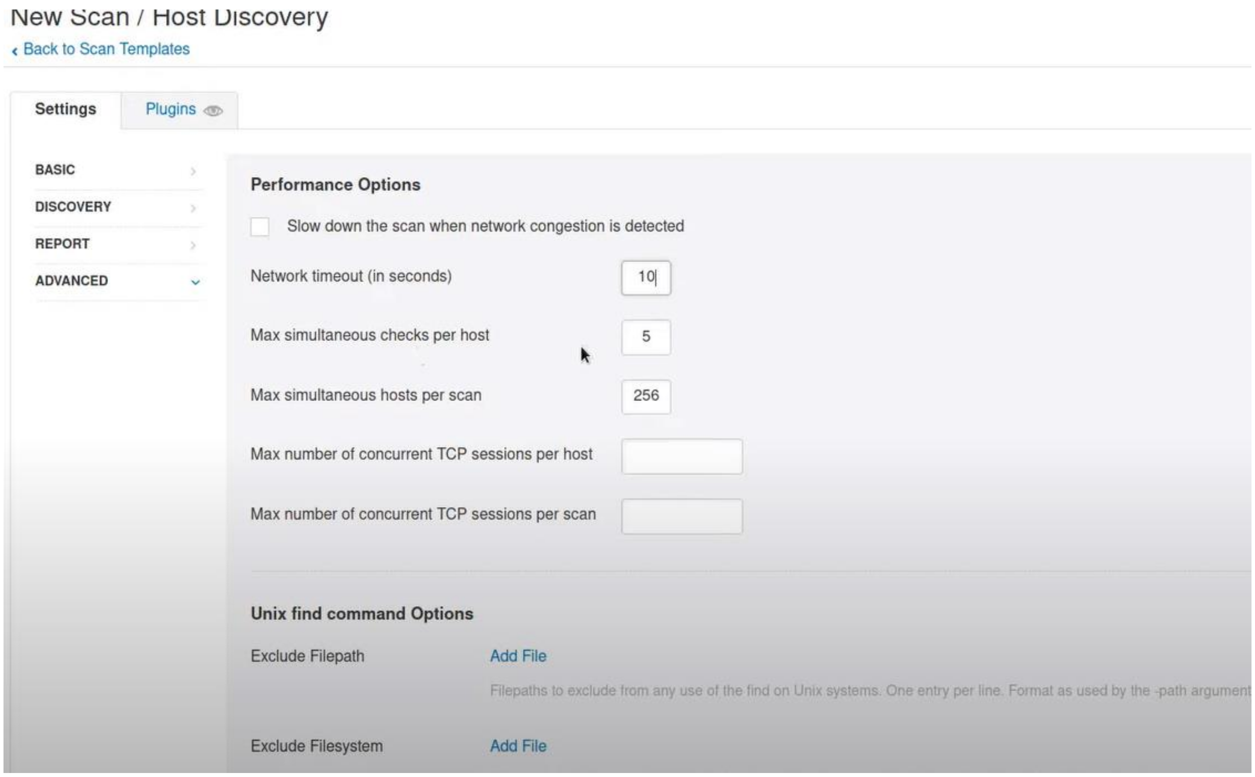
☑ Allow users to edit scan results

☐ Designate hosts by their DNS name

☑ Display hosts that respond to ping

☐ Display unreachable hosts

☐ Display Unicode characters
WARNING: This feature may cause issues with compliance checks and custom plugins that encounter ISO-8859-1 encoded output



New Scan / Host Discovery

Performance Options

☐ Slow down the scan when network congestion is detected

Network timeout (in seconds): 10

Max simultaneous checks per host: 5

Max simultaneous hosts per scan: 256

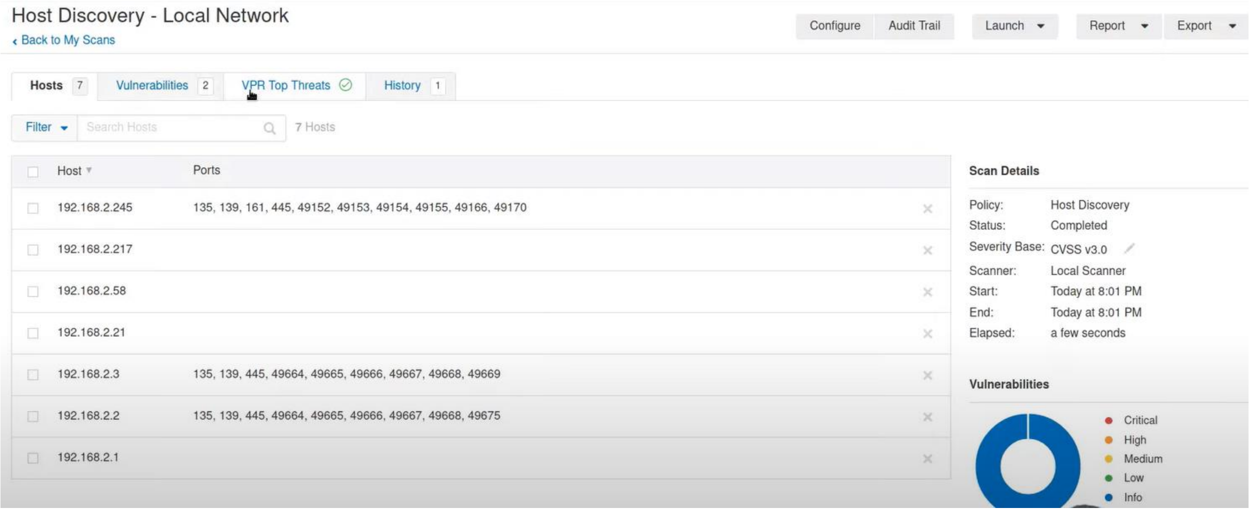
Max number of concurrent TCP sessions per host:

Max number of concurrent TCP sessions per scan:

Unix find command Options

Exclude Filepath — Add File
Filepaths to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument

Exclude Filesystem — Add File



Host Discovery - Local Network

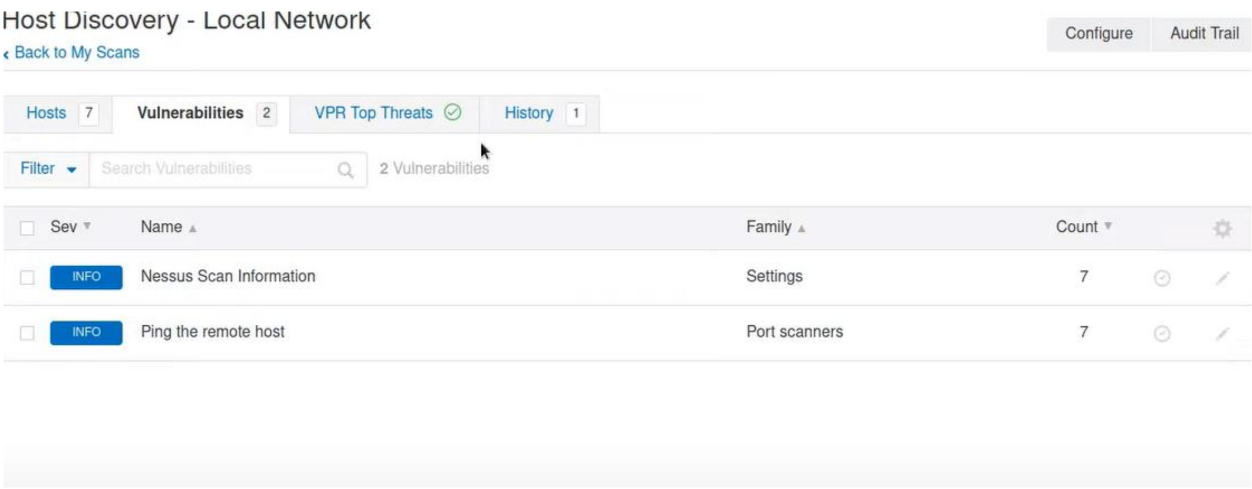
‹ Back to My Scans

Host	Ports
192.168.2.245	135, 139, 161, 445, 49152, 49153, 49154, 49155, 49166, 49170
192.168.2.217	
192.168.2.58	
192.168.2.21	
192.168.2.3	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 49669
192.168.2.2	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 49675
192.168.2.1	

Scan Details

Policy:	Host Discovery
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:01 PM
End:	Today at 8:01 PM
Elapsed:	a few seconds

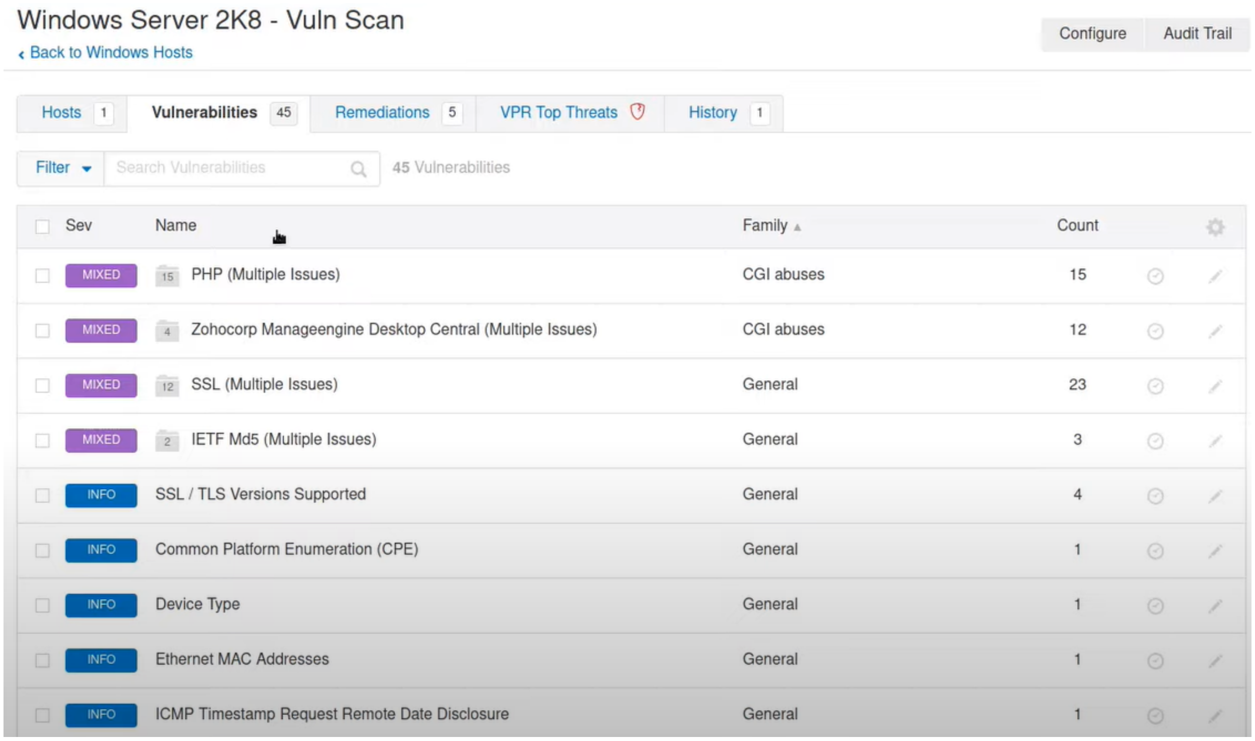
Vulnerabilities



Host Discovery - Local Network

‹ Back to My Scans

Sev	Name	Family	Count
INFO	Nessus Scan Information	Settings	7
INFO	Ping the remote host	Port scanners	7

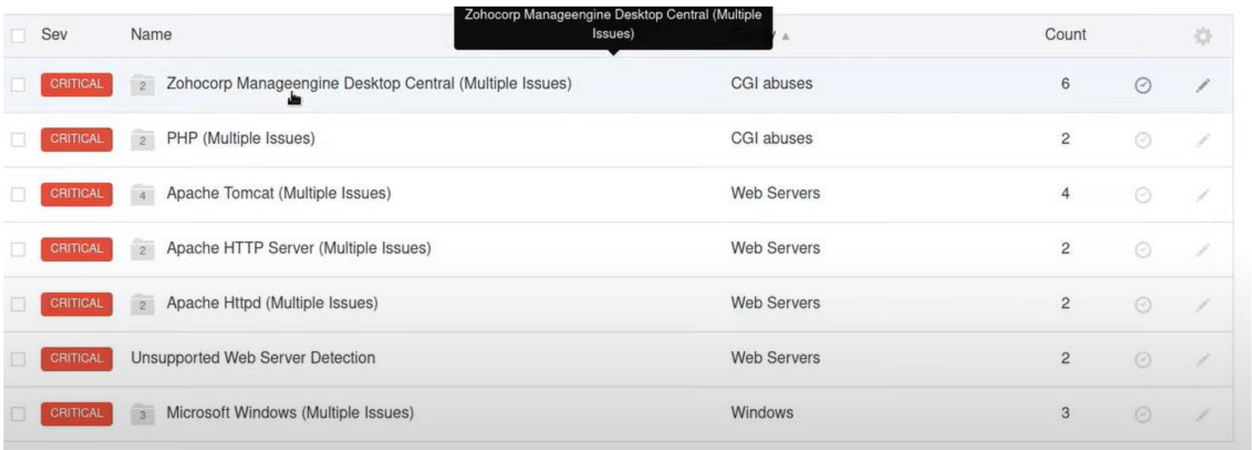


Windows Server 2K8 - Vuln Scan

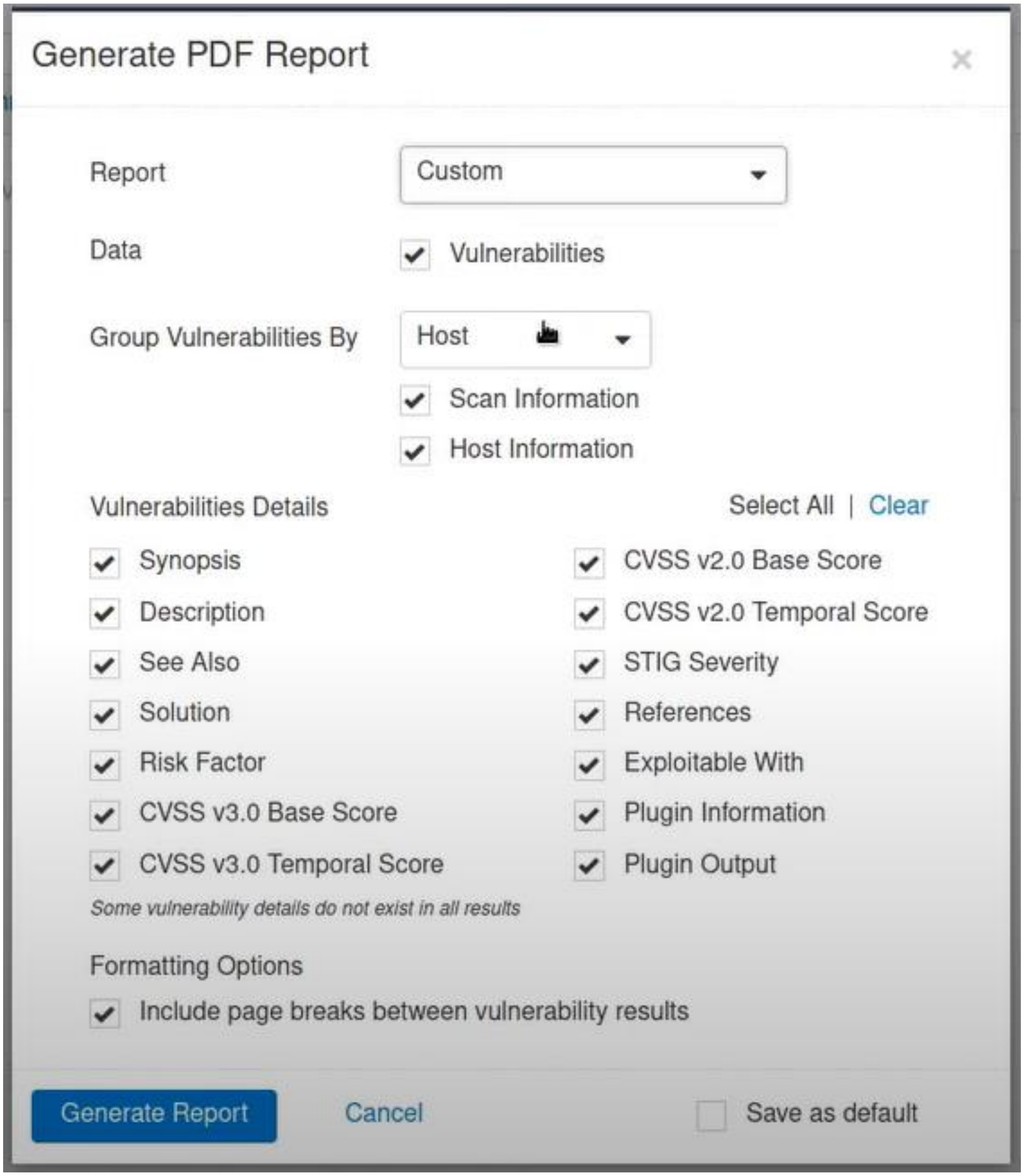
‹ Back to Windows Hosts

45 Vulnerabilities

□	Sev	Name	Family ▲	Count
□	MIXED	15 PHP (Multiple Issues)	CGI abuses	15
□	MIXED	4 Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	12
□	MIXED	12 SSL (Multiple Issues)	General	23
□	MIXED	2 IETF Md5 (Multiple Issues)	General	3
□	INFO	SSL / TLS Versions Supported	General	4
□	INFO	Common Platform Enumeration (CPE)	General	1
□	INFO	Device Type	General	1
□	INFO	Ethernet MAC Addresses	General	1
□	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1



□	Sev	Name	Family ▲	Count
□	CRITICAL	2 Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	6
□	CRITICAL	2 PHP (Multiple Issues)	CGI abuses	2
□	CRITICAL	4 Apache Tomcat (Multiple Issues)	Web Servers	4
□	CRITICAL	2 Apache HTTP Server (Multiple Issues)	Web Servers	2
□	CRITICAL	2 Apache Httpd (Multiple Issues)	Web Servers	2
□	CRITICAL	Unsupported Web Server Detection	Web Servers	2
□	CRITICAL	3 Microsoft Windows (Multiple Issues)	Windows	3



Generate PDF Report

Report: Custom

Data: ☑ Vulnerabilities

Group Vulnerabilities By: Host

☑ Scan Information
☑ Host Information

Vulnerabilities Details

☑ Synopsis	☑ CVSS v2.0 Base Score
☑ Description	☑ CVSS v2.0 Temporal Score
☑ See Also	☑ STIG Severity
☑ Solution	☑ References
☑ Risk Factor	☑ Exploitable With
☑ CVSS v3.0 Base Score	☑ Plugin Information
☑ CVSS v3.0 Temporal Score	☑ Plugin Output

Some vulnerability details do not exist in all results

Formatting Options

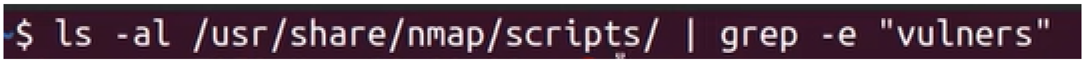
☑ Include page breaks between vulnerability results

□ Save as default

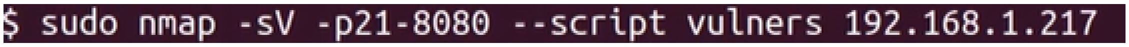
- ➢ Pros:
  - Can quickly and accurately identify vulnerabilities, configuration issues and malware in physical, virtual, and cloud environments
- ➢ Cons:
  - Scans and the application can become very slow if run on large networks

❖ Tool: Nmap

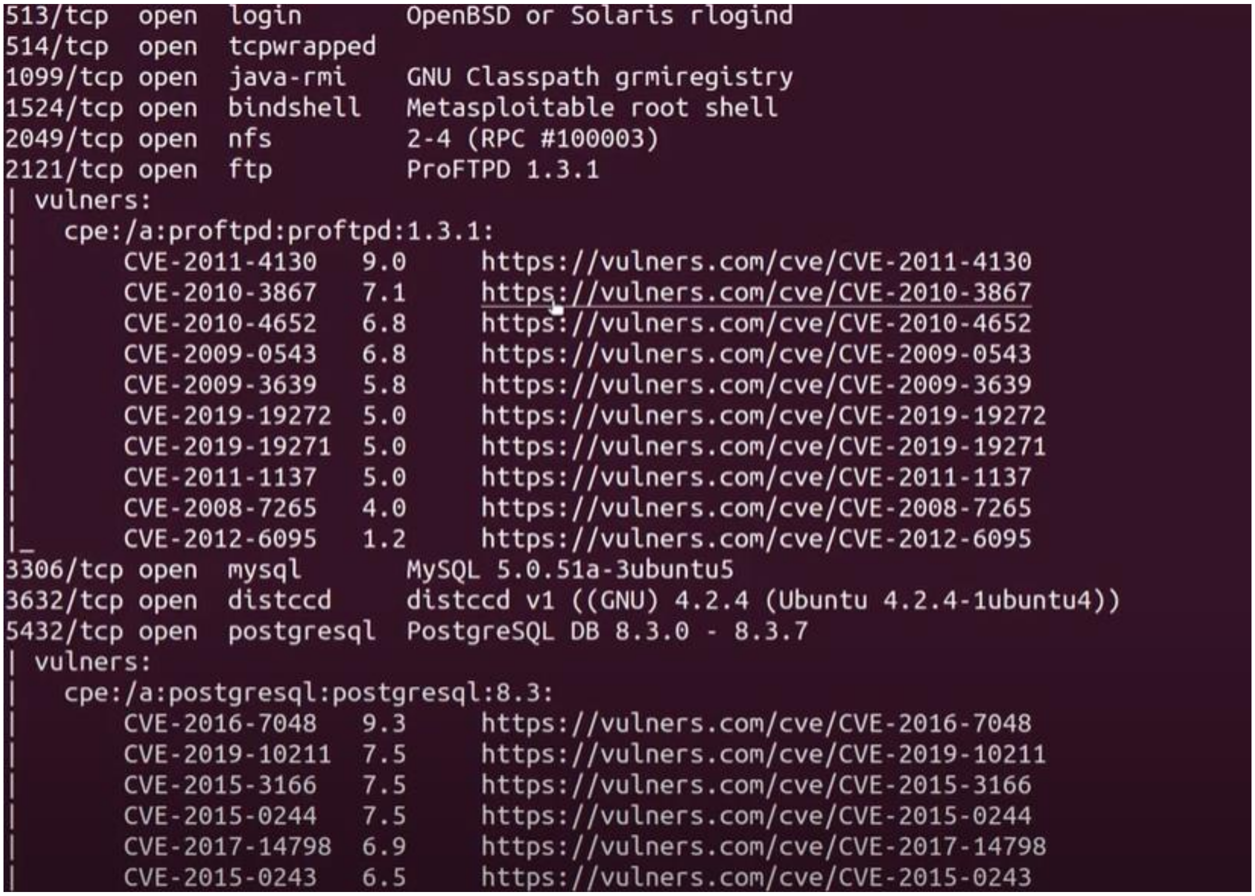
- Usage:
  - Vulnerability scripts are built in with Nmap within the Kali Linux OS
  - Look in the /usr/share/nmap/scripts directory to see them
  - Run with sudo privileges and use the services flag and the ports needed to scan. (This can be combined with other flags)
  - After the scan completes, all of the vulnerabilities that the script could fine will be seen with their corresponding CVEs
  - Exploit these vulnerabilities as needed for the test
- Screenshots:



```
$ ls -al /usr/share/nmap/scripts/ | grep -e "vulners"
```



```
$ sudo nmap -sV -p21-8080 --script vulners 192.168.1.217
```

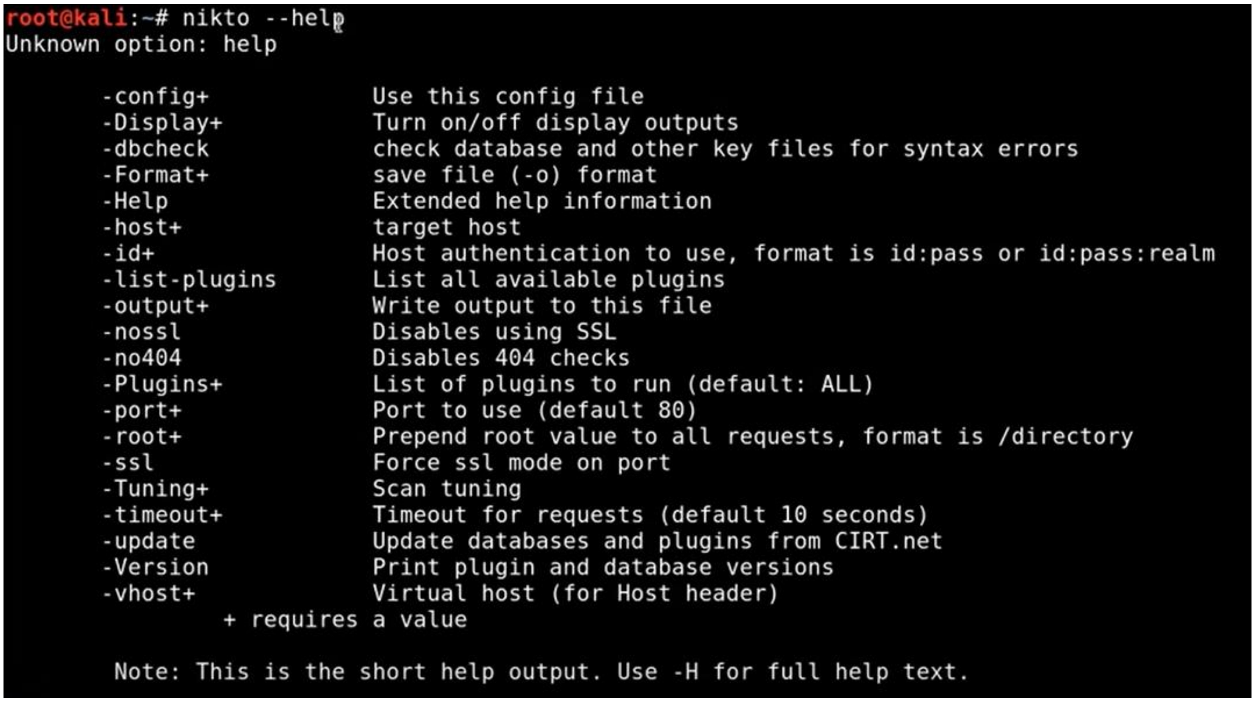


```
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.1:
|       CVE-2011-4130   9.0     https://vulners.com/cve/CVE-2011-4130
|       CVE-2010-3867   7.1     https://vulners.com/cve/CVE-2010-3867
|       CVE-2010-4652   6.8     https://vulners.com/cve/CVE-2010-4652
|       CVE-2009-0543   6.8     https://vulners.com/cve/CVE-2009-0543
|       CVE-2009-3639   5.8     https://vulners.com/cve/CVE-2009-3639
|       CVE-2019-19272  5.0     https://vulners.com/cve/CVE-2019-19272
|       CVE-2019-19271  5.0     https://vulners.com/cve/CVE-2019-19271
|       CVE-2011-1137   5.0     https://vulners.com/cve/CVE-2011-1137
|       CVE-2008-7265   4.0     https://vulners.com/cve/CVE-2008-7265
|_      CVE-2012-6095   1.2     https://vulners.com/cve/CVE-2012-6095
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|       CVE-2016-7048   9.3     https://vulners.com/cve/CVE-2016-7048
|       CVE-2019-10211  7.5     https://vulners.com/cve/CVE-2019-10211
|       CVE-2015-3166   7.5     https://vulners.com/cve/CVE-2015-3166
|       CVE-2015-0244   7.5     https://vulners.com/cve/CVE-2015-0244
|       CVE-2017-14798  6.9     https://vulners.com/cve/CVE-2017-14798
|       CVE-2015-0243   6.5     https://vulners.com/cve/CVE-2015-0243
```

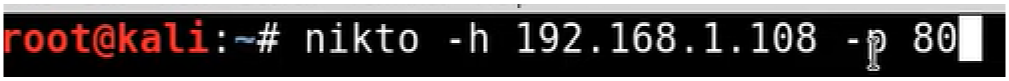
- ➢ Pros:
    - ■ Very straightforward
    - ■ Built in with Nmap which is preloaded with Kali
    - ■ Simple commands
    - ■ Can easily be combined with bash or python scripts
- ➢ Cons:
    - ■ When combined with other scans, the time required for the scan can exponentially increase
    - ■ Scripts need to be updated regularly
    - ■ Scripts need to be altered if an issue arises with the client

❖ Tool: Nikto

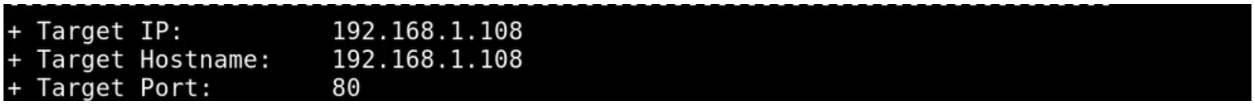
- ➢ Usage:
    - ■ On Kali Linux, run the nikto command with - - help to see flags to use
    - ■ Run nikto on the desired ip or ip addresses specifying the ports to scan
    - ■ After the scan completes, the vulnerabilities will be seen and can be used accordingly.
        - ● The output can be placed in a file as needed (see last screenshot)
- ➢ Screenshots:



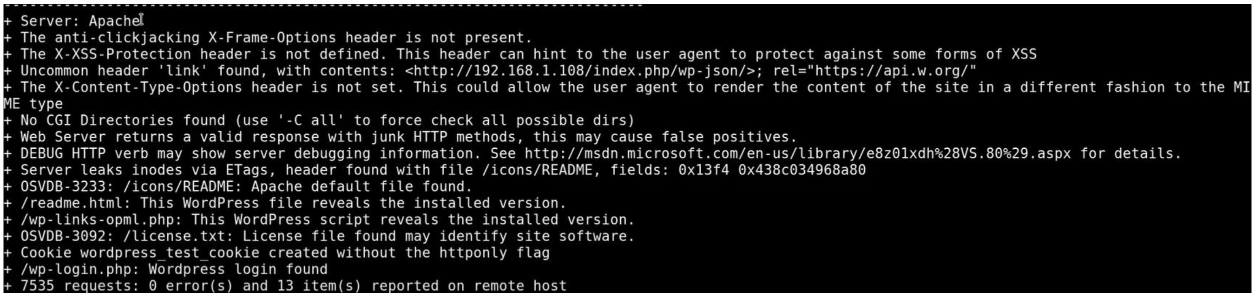
```
root@kali:~# nikto --help
Unknown option: help

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```



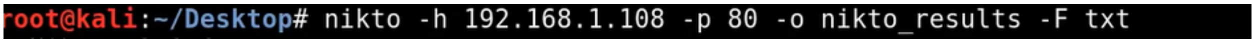
```
root@kali:~# nikto -h 192.168.1.108 -p 80
```



```
---------------------------------------------------------------------------
+ Target IP:          192.168.1.108
+ Target Hostname:    192.168.1.108
+ Target Port:        80
```



```
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'link' found, with contents: <http://192.168.1.108/index.php/wp-json/>; rel="https://api.w.org/"
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MI
ME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
+ /readme.html: This WordPress file reveals the installed version.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login.php: Wordpress login found
+ 7535 requests: 0 error(s) and 13 item(s) reported on remote host
```

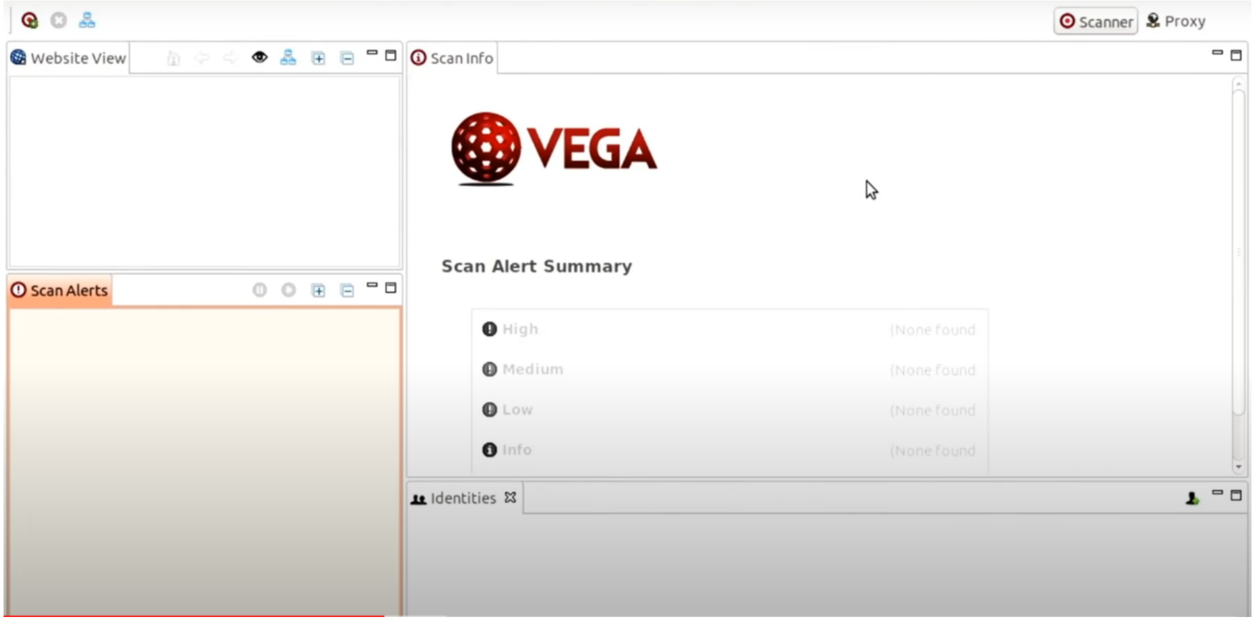


```
root@kali:~/Desktop# nikto -h 192.168.1.108 -p 80 -o nikto_results -F txt
```

- Pros:
  - Not even a little bit stealthy and will be caught almost immediately by IDSs
- Cons:
  - No GUI interface.

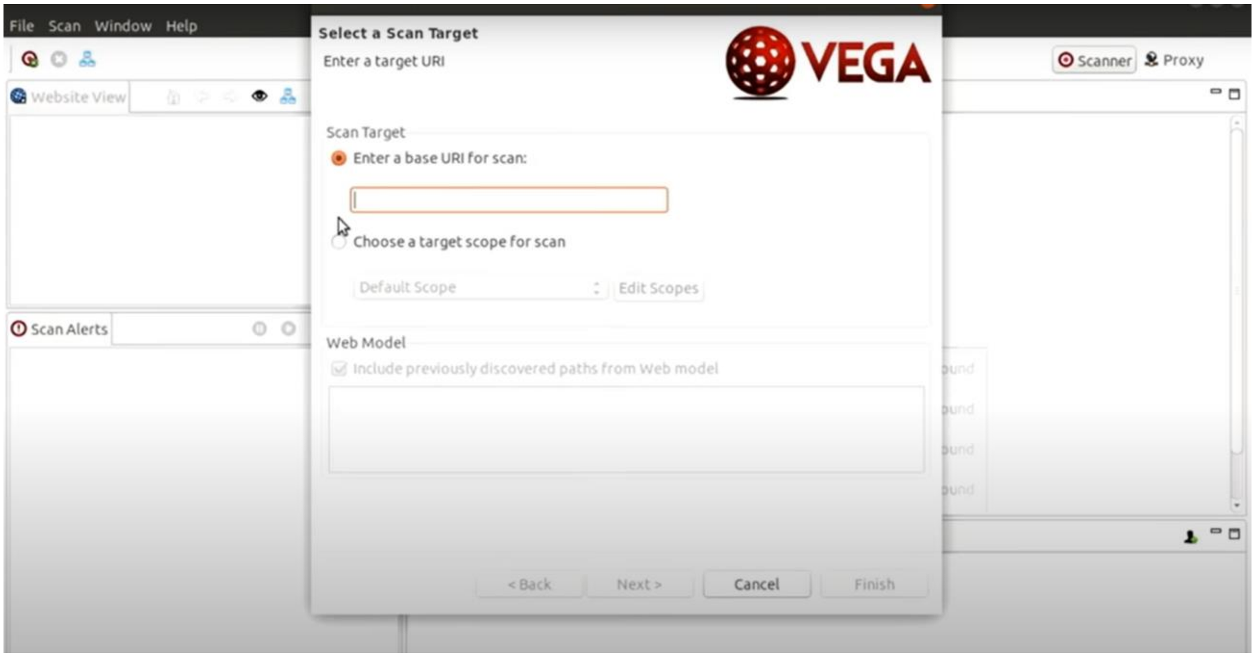
        - No development and support team.
        - No community forum.

- Tool: Vega
    - Usage:
        - Start up Kali Linux, go to applications, and choose Vega
        - Configure the proxy to use as needed (bare in mind, using tor will slow this down a lot)
        - Set the Scanner Preferences to fit client, attack device, and server resource needs
        - Select scan and enter the target/s to scan
        - Select the modules (vulnerability libraries) to run << discuss this with client
        - Click through the defaults to run the scan << change the defaults based on client needs
        - The vulnerabilities to exploit will show during and after scan completes
        - Click into the alerts and exploit accordingly
    - Screenshots:



Scan Alert Summary

High	(None found
Medium	(None found
Low	(None found
Info	(None found



Select a Scan Target

Enter a target URI

Scan Target

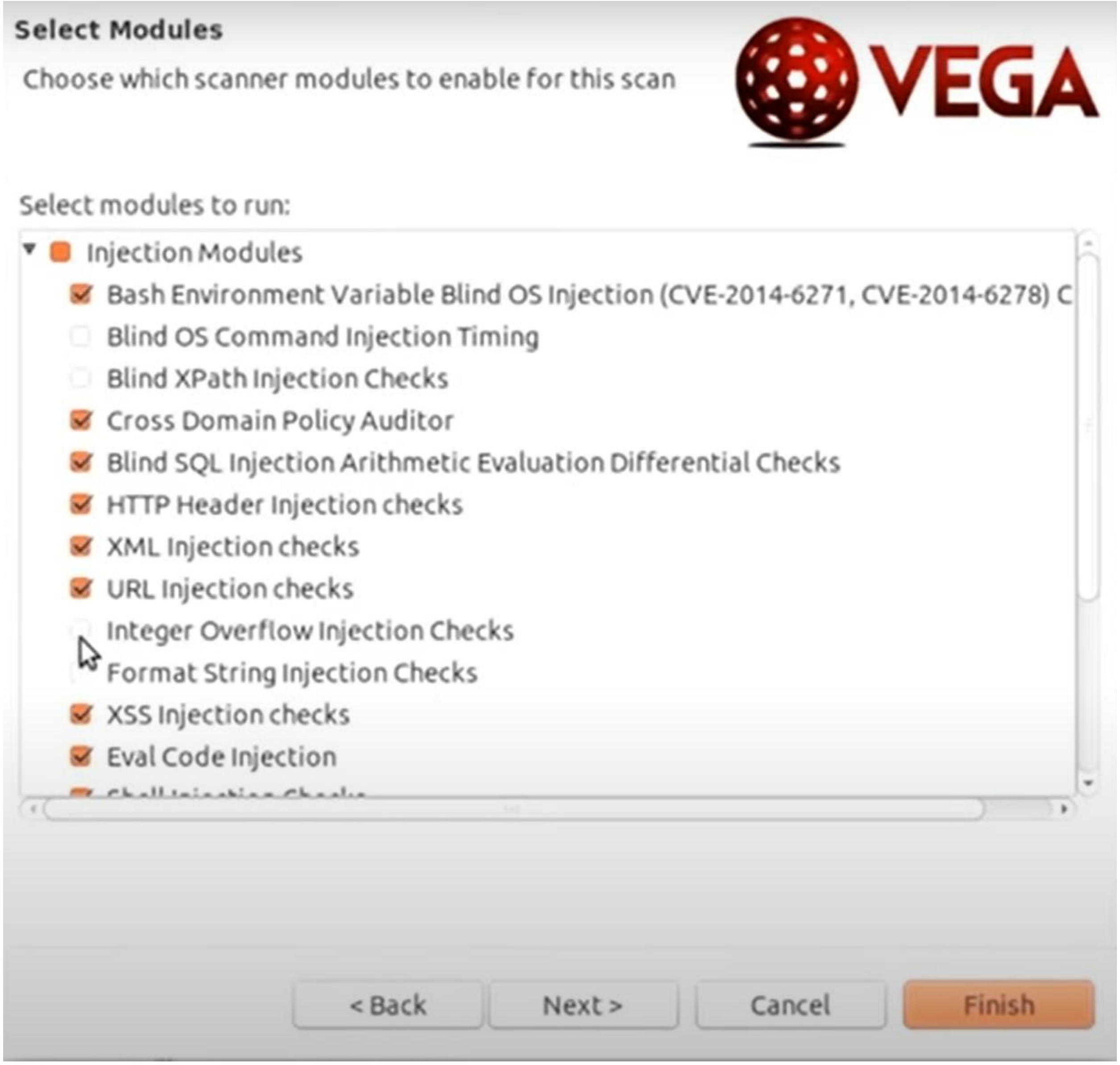
● Enter a base URI for scan:

○ Choose a target scope for scan

Default Scope   Edit Scopes

Web Model

☑ Include previously discovered paths from Web model

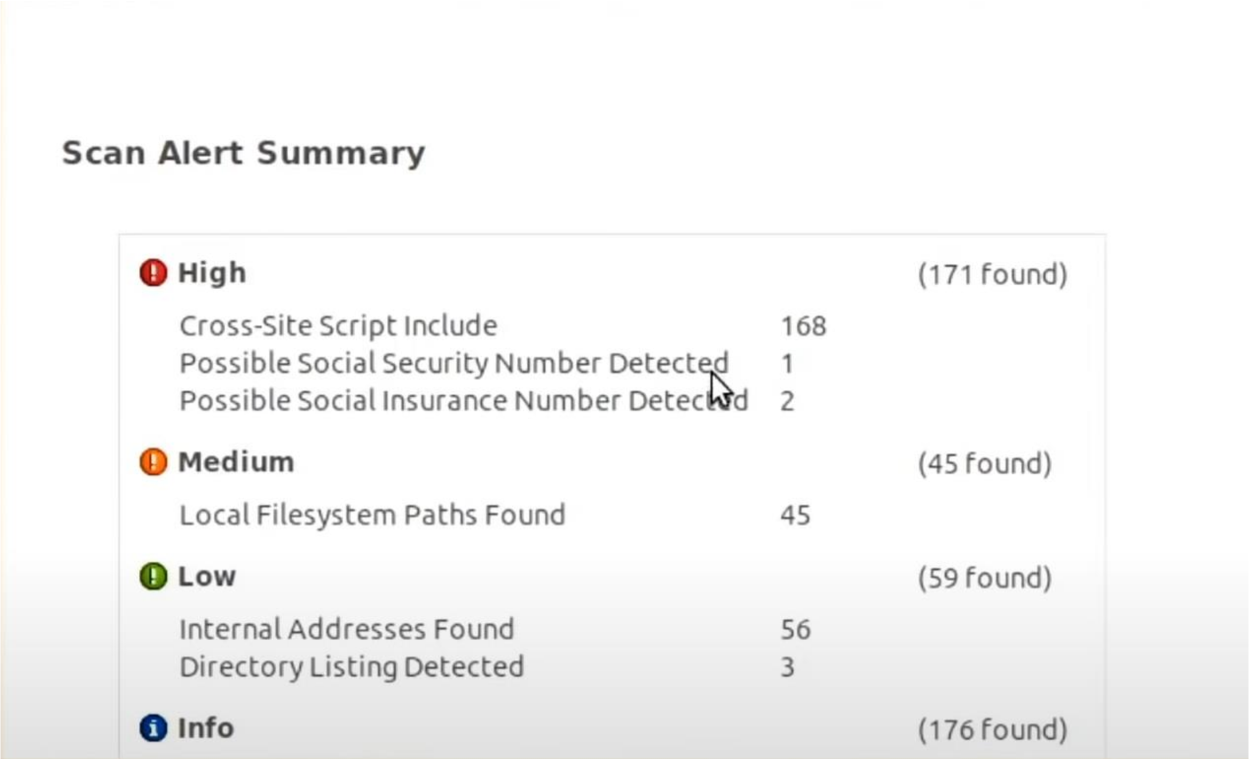


Select Modules

Choose which scanner modules to enable for this scan

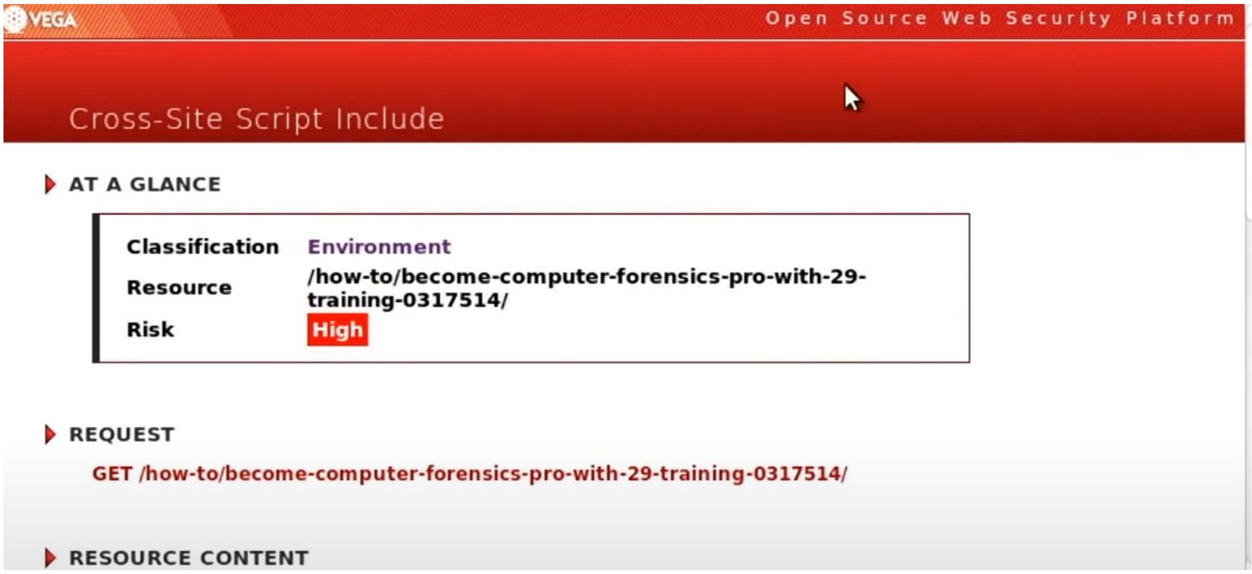
Select modules to run:

- ▼ ■ Injection Modules
  - ☑ Bash Environment Variable Blind OS Injection (CVE-2014-6271, CVE-2014-6278) C
  - □ Blind OS Command Injection Timing
  - □ Blind XPath Injection Checks
  - ☑ Cross Domain Policy Auditor
  - ☑ Blind SQL Injection Arithmetic Evaluation Differential Checks
  - ☑ HTTP Header Injection checks
  - ☑ XML Injection checks
  - ☑ URL Injection checks
  - □ Integer Overflow Injection Checks
  - □ Format String Injection Checks
  - ☑ XSS Injection checks
  - ☑ Eval Code Injection
  - ☑ Shell Injection Checks



Scan Alert Summary

High		(171 found)
Cross-Site Script Include	168	
Possible Social Security Number Detected	1	
Possible Social Insurance Number Detected	2	
Medium		(45 found)
Local Filesystem Paths Found	45	
Low		(59 found)
Internal Addresses Found	56	
Directory Listing Detected	3	
Info		(176 found)



Cross-Site Script Include

AT A GLANCE

Classification	Environment
Resource	/how-to/become-computer-forensics-pro-with-29-training-0317514/
Risk	High

REQUEST

GET /how-to/become-computer-forensics-pro-with-29-training-0317514/

RESOURCE CONTENT

- Pros:
  - Easy to use GUI
  - Can locate possible sensitive data based on formats. I.E. XXX-XXX-XXXX
  - Preloaded in Kali Linux

- Cons:
    - Sometimes vulnerabilities can be too complex for the tool to find. Combining the tool with an IDS or another tool can help optimize it even further.

References

havlikgear. (2022, April 3). *Complete beginner openvas vulnerability scanning tutorial - cyber security*. YouTube. Retrieved May 20, 2022, from https://www.youtube.com/watch?v=LGh2SetiKaY

YouTube. (2021, October 6). *Introduction to vulnerability scanning*. YouTube. Retrieved May 20, 2022, from https://www.youtube.com/watch?v=fG7HhqEJbTs

YouTube. (2021, October 10). *Host discovery & vulnerability scanning with nessus*. YouTube. Retrieved May 20, 2022, from https://www.youtube.com/watch?v=TA1rCRyHRsM

YouTube. (2020, August 15). *Vulnerability scanning with nmap*. YouTube. Retrieved May 20, 2022, from https://www.youtube.com/watch?v=W0KRYkZppIw

YouTube. (2018, January 31). *Nikto web vulnerability scanner - web penetration testing - #1*. YouTube. Retrieved May 20, 2022, from https://www.youtube.com/watch?v=GH9qn_DBzCk

YouTube. (2020, November 25). *Scan websites for potential vulnerabilities using Vega in Kali linux [tutorial]*. YouTube. Retrieved May 20, 2022, from https://www.youtube.com/watch?v=1HDC6fKsKYE