

Vu Nguyen

UID: u1483046

Assignment 1 - Vulnerability Scanning with OpenVAS (Lab and Quiz)

1. Section 1, Step 13

The screenshot shows the Greenbone Security Assistant (Iceweasel) interface. The browser address bar displays the URL: `https://127.0.0.1:9392/omp?cmd=cvs_calculator&token=05b4bf6-06d7-4521`. The interface includes a navigation menu with options like Scan Management, Asset Management, Backups Management, Configuration, Extras, Administration, and Help. The main content area features the 'CVSS Base Score Calculator' with two sections: 'From Metrics' and 'From Vector'. The 'From Metrics' section has dropdown menus for Access Vector (Local), Access Complexity (High), Authentication (Multiple), Confidentiality (None), Integrity (None), and Availability (None). The 'From Vector' section has a text input field. A 'Calculate' button is present at the bottom right of the calculator. A message at the bottom of the interface states: 'It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!'. A 'Rfresh Iceweasel...' button is also visible.

2. Section 2, Step 5

The screenshot shows the Greenbone Security Assistant (Iceweasel) interface. The browser address bar displays the URL: `https://127.0.0.1:9392/omp?cmd=get_reports&replace_task_id=1&filter_id=266`. The interface includes a navigation menu with options like Scan Management, Asset Management, Backups Management, Configuration, Extras, Administration, and Help. The main content area features the 'Reports' section, which displays a table of scan results. The table has columns for Status, Task, Severity, and Scan Results. The 'Scan Results' column shows a table with columns for Status, Task, Severity, and Scan Results. The 'Status' column shows 'Completed' and the 'Task' column shows '192.168.48.12'. The 'Severity' column shows '20' and the 'Scan Results' column shows '60' and '118'. A message at the bottom of the interface states: 'It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!'. A 'Rfresh Iceweasel...' button is also visible.

3. Section 3, Step 5

David Eccles School of Business THE UNIVERSITY OF UTAH

MyNETLAB > NDG Ethical Hacking POD 2 > Reservation 69644 > Lab 07: Vulnerability Scanning with OpenVAS

Toplogy Content Status OpenSUSE Security Onion OWASP BWA pfSense Kali

Time Remaining 3 01 hrs. min.

Greenbone Security Assistant - Icwessel

https://127.0.0.1:9392/omp

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Greenbone Security Assistant

Scan Management Asset Management Security Management Configuration Entries Administration Help

Target Details

Name:	OWASP	ID:	3860a6fa-9537-433a-b721-013a6f4a0009
Comment:		Created:	Thu Feb 15 17:48:50 2024
Hosts:	192.168.68.12	Last modified:	Thu Feb 15 17:48:50 2024
Exclude Hosts:		Owner:	admin
Reverse Look-up Only:	No		
Reverse Look-up (info):	No		
Maximum number of hosts:	1		
Port List:	All tasks assigned TCP 2012-02-10		
Alive Test:	Consider Alive		
Credentials for authenticated checks:			
SSM:			
SMB:			
ESM:			

Tasks using this Target: None

User Tags for "OWASP": none

Revised operation: 3.10a Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net

It looks like you haven't started icwessel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Icwessel...

4. Section 3, Step 9

David Eccles School of Business THE UNIVERSITY OF UTAH

MyNETLAB > NDG Ethical Hacking POD 2 > Reservation 69644 > Lab 07: Vulnerability Scanning with OpenVAS

Toplogy Content Status OpenSUSE Security Onion OWASP BWA pfSense Kali

Time Remaining 3 00 hrs. min.

Greenbone Security Assistant - Icwessel

https://127.0.0.1:9392/omp/cmd=new_task&next=get_task&filter=apply_over

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

New Task

Name: OWASP-Scan

Comment (optional):

Scan Targets: OWASP

Alerts (optional):

Schedule (optional): Once

Add results to Asset Management: ☒ yes ☐ no

Alterable Task: ☐ yes ☒ no

Scanner

OpenVAS Scanner: OpenVAS Default

Scan Config: Full and very deep ultimate

Slave (optional):

Network Source Interface:

Order for target hosts: Sequential

Maximum concurrently executed RVTs per host: 4

Maximum concurrently scanned hosts: 20

Create Task

New Container Task

It looks like you haven't started icwessel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Icwessel...

5. Section 3, Step 11

Applications Places Icweasel Thu 11:50

Greenbone Security Assistant - Icweasel

https://127.0.0.1:9392/omp

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Greenbone Security Assistant

Logged in as Admin admin Logout
Thu Feb 15 17:50:30 2024 UTC

Scan Management Asset Management Settings Management Configuration Status Administration Help

Task Details

Names: OWASP-Scan ID: 66666666-6666-6666-6666-666666666666
Comments: Created: Thu Feb 15 17:50:30 2024
Target: OWASP Last modified: Thu Feb 15 17:50:30 2024
Alerts: Owner: admin
Schedule: (Next due: over)
Add to Assets: yes
Assignable Task: no
Scanners: OpenVAS Default (Type: OpenVAS Scanner)
Scan Config: Full and very deep ultimate
Slaves:
Order for target hosts: Sequential
Network Source Interface:
Maximum concurrently executed RUTs per host: 4
Maximum concurrently scanned hosts: 20
Status: **Completed**
Reports: 1, Current: Feb 15 2024 (Finished: 0)
Notes: 0
Overides: 0

User Tags for "OWASP-Scan": none

Permissions for "OWASP-Scan": none

Grant Read permissions to User

It looks like you haven't started Icweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Rfresh Icweasel...