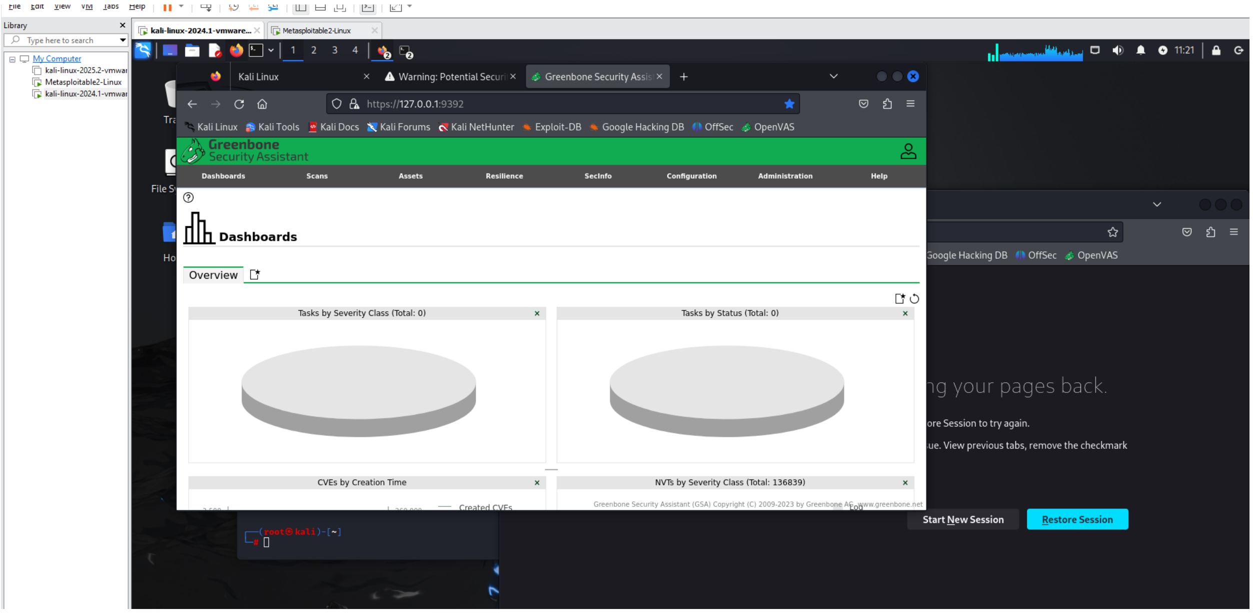
Security Lab10 - Kali & OpenVAS

Fundamentals of Information Security: Cybersecurity (88252)

Ana Herrera Flores

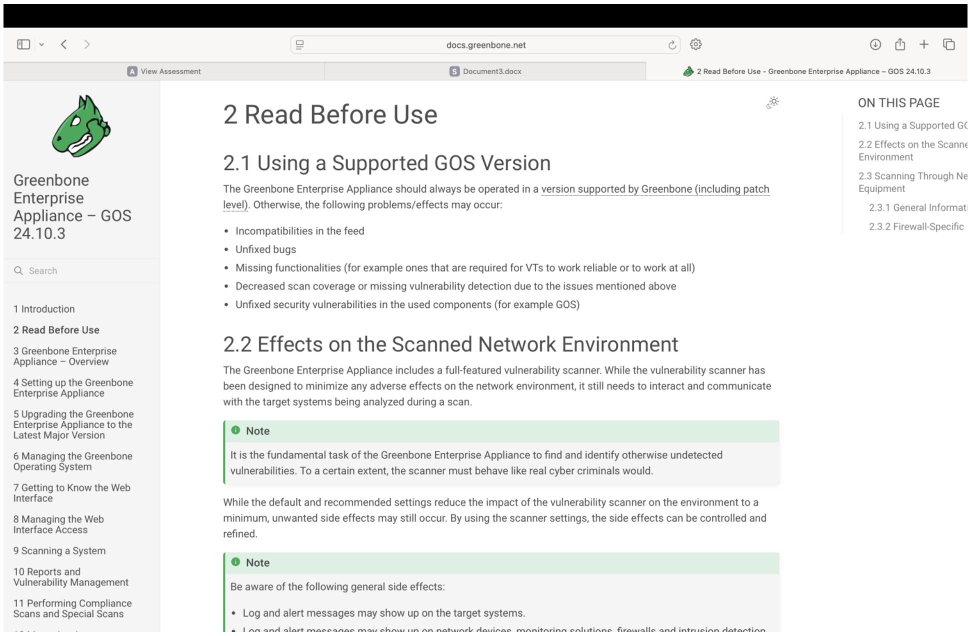
Exercises 1, 2, 3, 4 Completed



OpenVAS is running in Firefox browser.

Exercise 5

Before, we begin with Scanning something. Let’s take a look at the documentation:
Greenbone Enterprise Appliance – GOS 24.10.1
Read the following: Chapter 2 - “Read Before Use” in the Manual.
Read Chapter 7 – Getting to Know the Web Interface
Read Chapter 9 – Scanning a System
Provide snippets of the Chapters above, just the first page.


docs.greenbone.net
View Assessment
Document3.docx
2 Read Before Use - Greenbone Enterprise Appliance – GOS 24.10.3
Greenbone Enterprise Appliance – GOS 24.10.3
Search

1 Introduction
2 Read Before Use
3 Greenbone Enterprise Appliance – Overview
4 Setting up the Greenbone Enterprise Appliance
5 Upgrading the Greenbone Enterprise Appliance to the Latest Major Version
6 Managing the Greenbone Operating System
7 Getting to Know the Web Interface
8 Managing the Web Interface Access
9 Scanning a System
10 Reports and Vulnerability Management
11 Performing Compliance Scans and Special Scans

2 Read Before Use

2.1 Using a Supported GOS Version

The Greenbone Enterprise Appliance should always be operated in a version supported by Greenbone (including patch level). Otherwise, the following problems/effects may occur:

- Incompatibilities in the feed
- Unfixed bugs
- Missing functionalities (for example ones that are required for VTs to work reliable or to work at all)
- Decreased scan coverage or missing vulnerability detection due to the issues mentioned above
- Unfixed security vulnerabilities in the used components (for example GOS)

2.2 Effects on the Scanned Network Environment

The Greenbone Enterprise Appliance includes a full-featured vulnerability scanner. While the vulnerability scanner has been designed to minimize any adverse effects on the network environment, it still needs to interact and communicate with the target systems being analyzed during a scan.

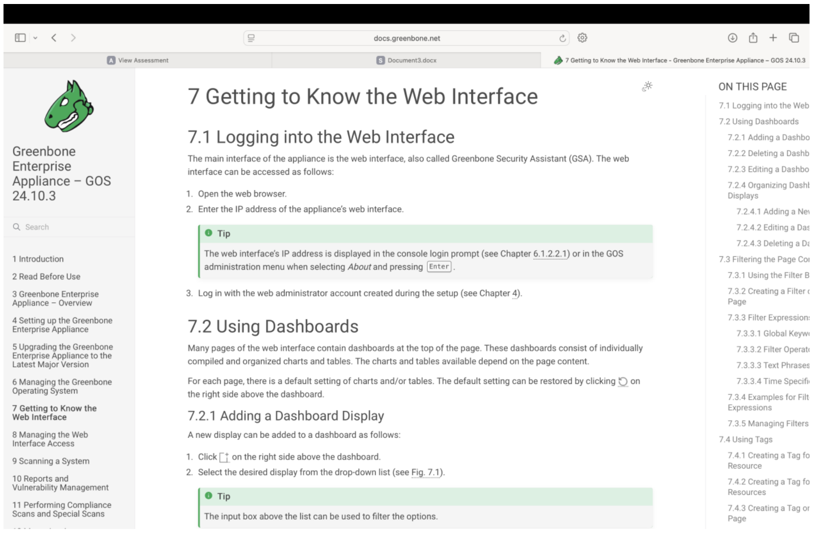
> **Note**
>
> It is the fundamental task of the Greenbone Enterprise Appliance to find and identify otherwise undetected vulnerabilities. To a certain extent, the scanner must behave like real cyber criminals would.

While the default and recommended settings reduce the impact of the vulnerability scanner on the environment to a minimum, unwanted side effects may still occur. By using the scanner settings, the side effects can be controlled and refined.

> **Note**
>
> Be aware of the following general side effects:
>
> - Log and alert messages may show up on the target systems.
> - Log and alert messages may show up on network devices, monitoring solutions, firewalls and intrusion detection

ON THIS PAGE
2.1 Using a Supported GC
2.2 Effects on the Scanne Environment
2.3 Scanning Through Ne Equipment
2.3.1 General Informat
2.3.2 Firewall-Specific

Chapter 2


docs.greenbone.net
View Assessment
Document3.docx
7 Getting to Know the Web Interface - Greenbone Enterprise Appliance – GOS 24.10.3
Greenbone Enterprise Appliance – GOS 24.10.3
Search

1 Introduction
2 Read Before Use
3 Greenbone Enterprise Appliance – Overview
4 Setting up the Greenbone Enterprise Appliance
5 Upgrading the Greenbone Enterprise Appliance to the Latest Major Version
6 Managing the Greenbone Operating System
7 Getting to Know the Web Interface
8 Managing the Web Interface Access
9 Scanning a System
10 Reports and Vulnerability Management
11 Performing Compliance Scans and Special Scans

7 Getting to Know the Web Interface

7.1 Logging into the Web Interface

The main interface of the appliance is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as follows:

1. Open the web browser.
2. Enter the IP address of the appliance's web interface.

> **Tip**
>
> The web interface's IP address is displayed in the console login prompt (see Chapter 6.1.2.2.1) or in the GOS administration menu when selecting *About* and pressing `Enter`.

3. Log in with the web administrator account created during the setup (see Chapter 4).

7.2 Using Dashboards

Many pages of the web interface contain dashboards at the top of the page. These dashboards consist of individually compiled and organized charts and tables. The charts and tables available depend on the page content.

For each page, there is a default setting of charts and/or tables. The default setting can be restored by clicking ↺ on the right side above the dashboard.

7.2.1 Adding a Dashboard Display

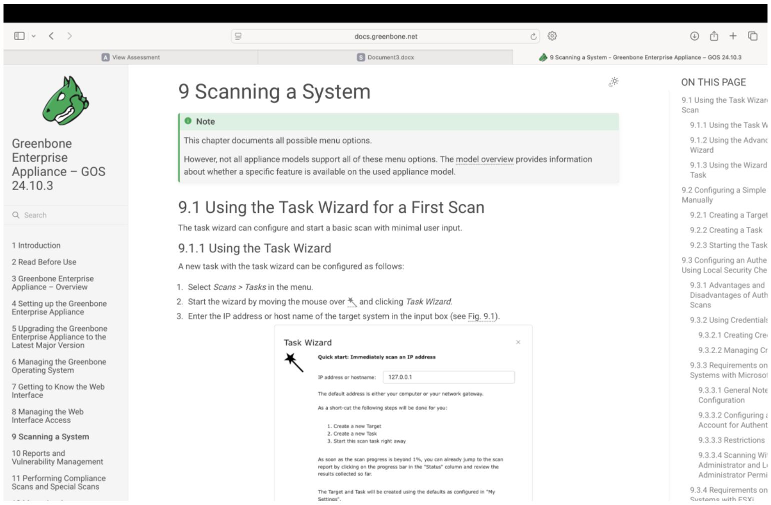
A new display can be added to a dashboard as follows:

1. Click ⊞ on the right side above the dashboard.
2. Select the desired display from the drop-down list (see Fig. 7.1).

> **Tip**
>
> The input box above the list can be used to filter the options.

ON THIS PAGE
7.1 Logging into the Web
7.2 Using Dashboards
7.2.1 Adding a Dashbo
7.2.2 Deleting a Dashb
7.2.3 Editing a Dashbo
7.2.4 Organizing Dashb Displays
7.2.4.1 Adding a Nev
7.2.4.2 Editing a Das
7.2.4.3 Deleting a Da
7.3 Filtering the Page Co
7.3.1 Using the Filter B
7.3.2 Creating a Filter c Page
7.3.3 Filter Expression
7.3.3.1 Global Keyw
7.3.3.2 Filter Operat
7.3.3.3 Text Phrases
7.3.3.4 Time Specifi
7.3.4 Examples for Filt Expressions
7.3.5 Managing Filters
7.4 Using Tags
7.4.1 Creating a Tag fo Resource
7.4.2 Creating a Tag fo Resources
7.4.3 Creating a Tag or Page

Chapter 7


docs.greenbone.net
View Assessment
Document3.docx
9 Scanning a System - Greenbone Enterprise Appliance – GOS 24.10.3
Greenbone Enterprise Appliance – GOS 24.10.3
Search
1 Introduction
2 Read Before Use
3 Greenbone Enterprise Appliance – Overview
4 Setting up the Greenbone Enterprise Appliance
5 Upgrading the Greenbone Enterprise Appliance to the Latest Major Version
6 Managing the Greenbone Operating System
7 Getting to Know the Web Interface
8 Managing the Web Interface Access
9 Scanning a System
10 Reports and Vulnerability Management
11 Performing Compliance Scans and Special Scans
ON THIS PAGE
9.1 Using the Task Wizar Scan
9.1.1 Using the Task W
9.1.2 Using the Advanc Wizard
9.1.3 Using the Wizard Task
9.2 Configuring a Simple Manually
9.2.1 Creating a Target
9.2.2 Creating a Task
9.2.3 Starting the Task
9.3 Configuring an Authe Using Local Security Che
9.3.1 Advantages and Disadvantages of Auth Scans
9.3.2 Using Credentials
9.3.2.1 Creating Cre
9.3.2.2 Managing Cr
9.3.3 Requirements on Systems with Microso
9.3.3.1 General Note Configuration
9.3.3.2 Configuring a Account for Authent
9.3.3.3 Restrictions
9.3.3.4 Scanning Wi Administrator and L Administrator Permi
9.3.4 Requirements on Systems with ESXi

9 Scanning a System

Note

This chapter documents all possible menu options.

However, not all appliance models support all of these menu options. The model overview provides information about whether a specific feature is available on the used appliance model.

9.1 Using the Task Wizard for a First Scan

The task wizard can configure and start a basic scan with minimal user input.

9.1.1 Using the Task Wizard

A new task with the task wizard can be configured as follows:

1. Select *Scans > Tasks* in the menu.
2. Start the wizard by moving the mouse over and clicking *Task Wizard*.
3. Enter the IP address or host name of the target system in the input box (see Fig. 9.1).

Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 127.0.0.1

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

Chapter 9

1. What are the steps for controlling and improving IT Security?

- Discovery of the current state
- Improving the current state
- Reviewing the taken measures

2. What is Greenbone Security Manager (Openvas)?

It is an appliance for the vulnerability management of IT infrastructures, available as physical or virtual models. Assisting companies and agencies with automated and integrated vulnerability assessment and management. Its task is to discover vulnerabilities and security gaps before a potential attacker does.

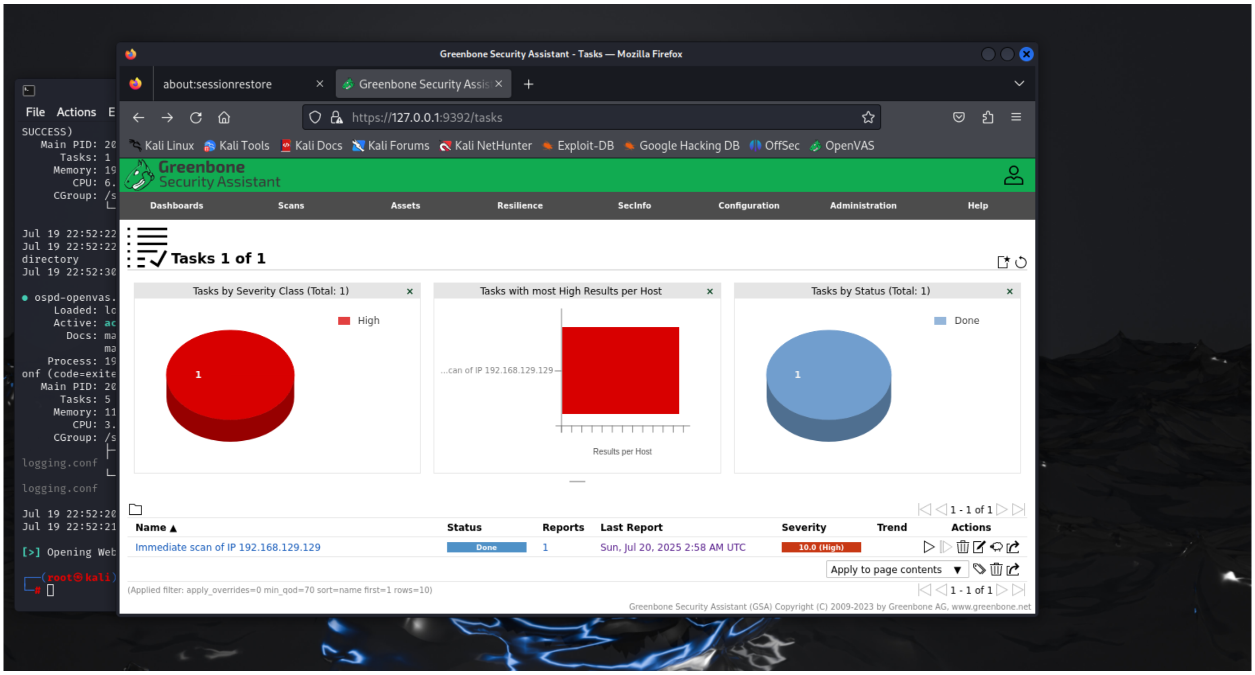
3. What perspectives does GSM discover vulnerabilities from an attacker?

- External: The GSM can simulate an external attack to identify outdated or misconfigured firewalls.
- Demilitarized Zone (DMZ): The GSM can identify actual vulnerabilities that may be exploited by attackers that get past the firewall.
- Internal: The GSM can also identify exploitable vulnerabilities in the internal network, for example those targeted by social engineering or computer worms. Due to the potential impact of such attacks, this perspective is particularly important for the security of any IT infrastructure.

4. What are the two options to deal with vulnerabilities?

- Eliminate the vulnerability by updating the software, removing the component or changing the configuration.
- Implementing a rule in a firewall or an intrusion prevention system (virtual patching).

Exercise 7 Scanning a System OpenVAS



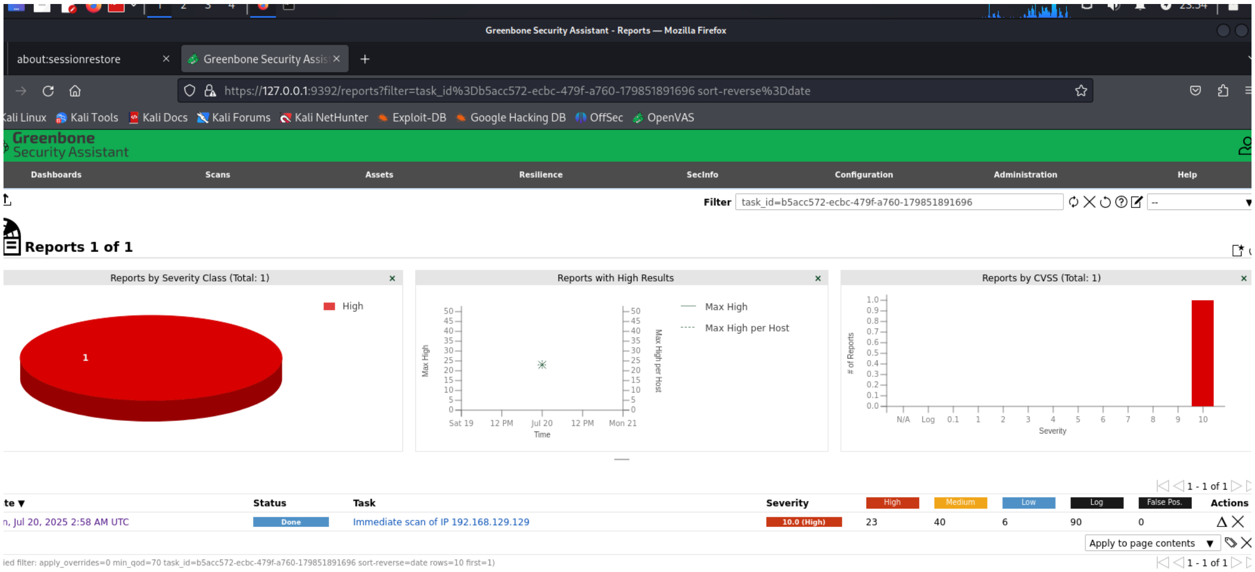
```
SUCCESS)
   Main PID: 20
      Tasks: 1
     Memory: 19
        CPU: 6.
     CGroup: /s
             └

Jul 19 22:52:22
Jul 19 22:52:22
directory
Jul 19 22:52:30

● ospd-openvas.
     Loaded: lo
     Active: ac
       Docs: ma
             ma
    Process: 19
onf (code=exite
   Main PID: 20
      Tasks: 5
     Memory: 11
        CPU: 3.
     CGroup: /s
             ├
logging.conf
             └
logging.conf

Jul 19 22:52:20
Jul 19 22:52:21

[>] Opening Web

┌──(root㉿kali)
└─# 
```

Tasks 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.129.129	Done	1	Sun, Jul 20, 2025 2:58 AM UTC	10.0 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

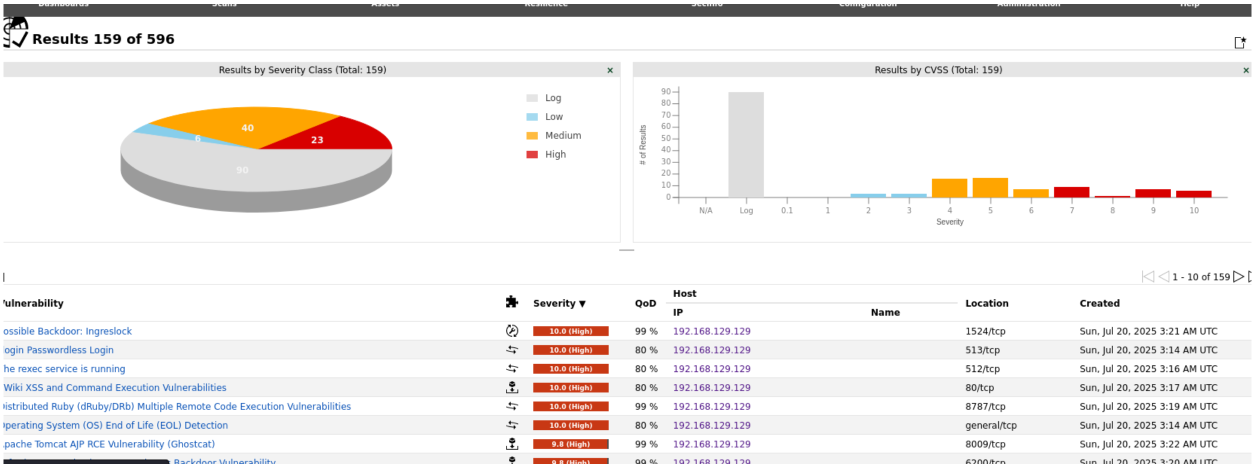


Filter task_id=b5acc572-ecbc-479f-a760-179851891696

Reports 1 of 1

te ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
n, Jul 20, 2025 2:58 AM UTC	Done	Immediate scan of IP 192.168.129.129	10.0 (High)	23	40	6	90	0	

ied filter: apply_overrides=0 min_qod=70 task_id=b5acc572-ecbc-479f-a760-179851891696 sort-reverse=date rows=10 first=1)



Results 159 of 596

1 - 10 of 159

'ulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
ossible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.129.129		1524/tcp	Sun, Jul 20, 2025 3:21 AM UTC
ogin Passwordless Login		10.0 (High)	80 %	192.168.129.129		513/tcp	Sun, Jul 20, 2025 3:14 AM UTC
he rexec service is running		10.0 (High)	80 %	192.168.129.129		512/tcp	Sun, Jul 20, 2025 3:16 AM UTC
Wiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.129.129		80/tcp	Sun, Jul 20, 2025 3:17 AM UTC
istributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99 %	192.168.129.129		8787/tcp	Sun, Jul 20, 2025 3:19 AM UTC
perating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	192.168.129.129		general/tcp	Sun, Jul 20, 2025 3:14 AM UTC
pache Tomcat AJP RCE Vulnerability (Ghostcat)		9.8 (High)	99 %	192.168.129.129		8009/tcp	Sun, Jul 20, 2025 3:22 AM UTC
[redacted] Backdoor Vulnerability		9.8 (High)	99 %	192.168.129.129		6200/tcp	Sun, Jul 20, 2025 3:20 AM UTC

As we can see, our scan is done.

1. Answer the following questions:

   a. How many High Vulnerabilities were found?

   The scanner found 23 high vulnerabilities.

   b. How many Medium Vulnerabilities were found?

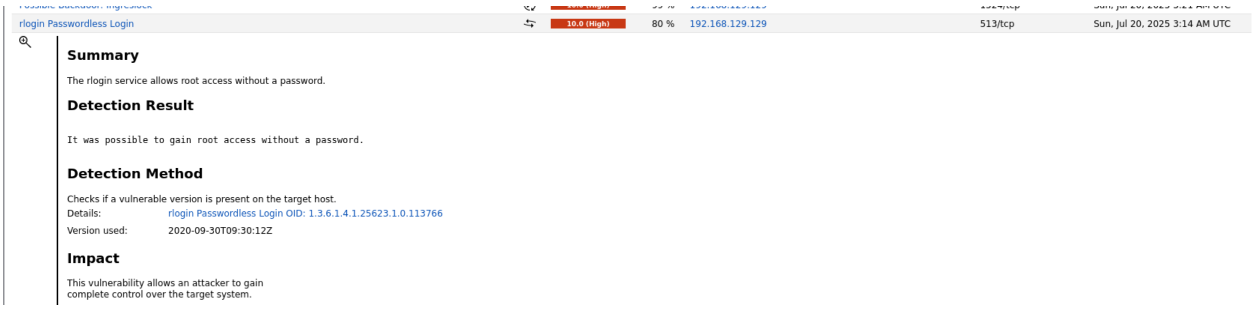
   There were found 40 medium vulnerabilities.

2. Analyze a few, answer the questions below:

   a. Any Password issues?

   i. If so, what was the Password issue and which program(s)?

   ii. What was the mitigation?



rlogin Passwordless Login		10.0 (High)	80 %	192.168.129.129	513/tcp	Sun, Jul 20, 2025 3:14 AM UTC

Summary

The rlogin service allows root access without a password.

Detection Result

```
It was possible to gain root access without a password.
```

Detection Method

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

Details: rlogin Passwordless Login OID: 1.3.6.1.4.1.25623.1.0.113766

Version used: 2020-09-30T09:30:12Z

Impact

This vulnerability allows an attacker to gain
complete control over the target system.

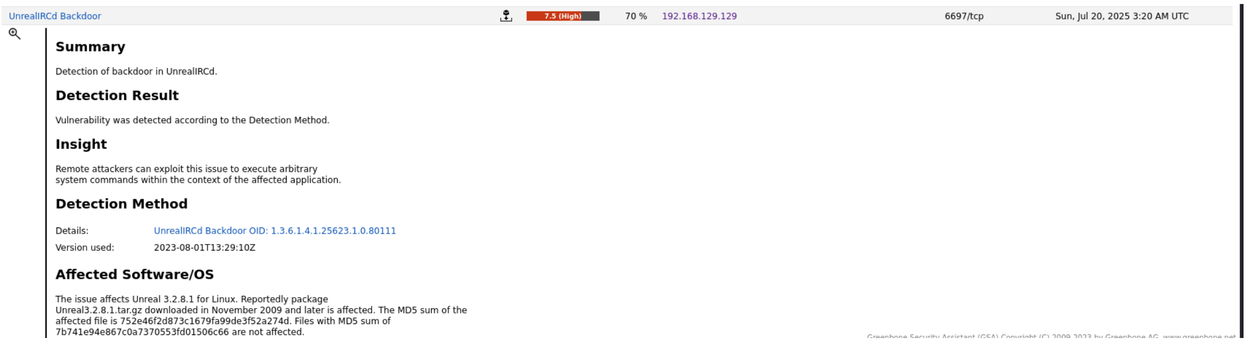
Yes, there was a password issue in the login to gain access to the root. It was possible to obtain access to the root without the need for a password.

The mitigation for this vulnerability is to disable the rlogin service and use an alternative like SSH instead.

   b. Any Backdoors detect?

   i. If so, which program and what was the issue?

   ii. What is the mitigation?



UnrealIRCd Backdoor | 7.5 (High) | 70 % | 192.168.129.129 | 6697/tcp | Sun, Jul 20, 2025 3:20 AM UTC

Summary

Detection of backdoor in UnrealIRCd.

Detection Result

Vulnerability was detected according to the Detection Method.

Insight

Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.

Detection Method

Details:	UnrealIRCd Backdoor OID: 1.3.6.1.4.1.25623.1.0.80111
Version used:	2023-08-01T13:29:10Z

Affected Software/OS

The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

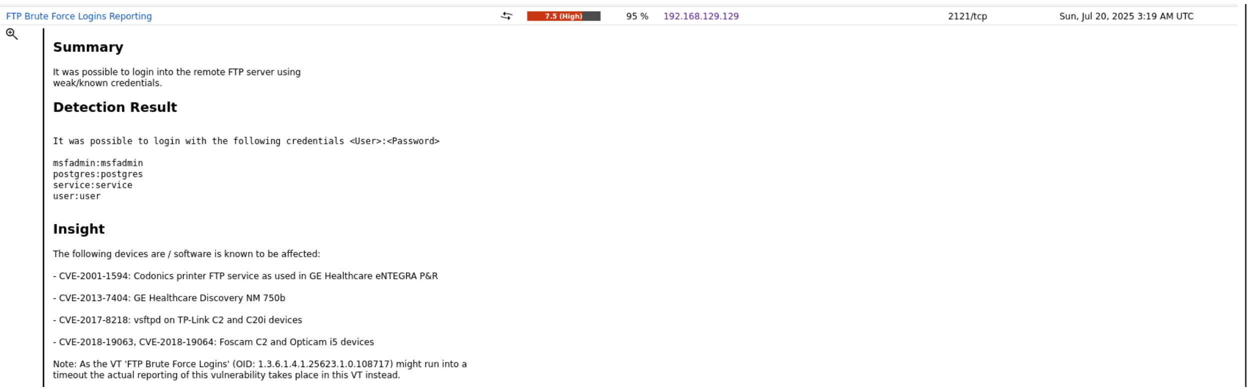
Yes, there was an open back door in UnrealIRCd, this issue affects Unreal 3.2.8.1 for Linux. Attackers can execute commands in the affected application.

The mitigation is to install the latest version of this software.

c. Any Brute Force Logging?

i. If so, which program and what was the issue?

ii. What is the mitigation?



FTP Brute Force Logins Reporting | 7.5 (High) | 95 % | 192.168.129.129 | 2121/tcp | Sun, Jul 20, 2025 3:19 AM UTC

Summary

It was possible to login into the remote FTP server using weak/known credentials.

Detection Result

```
It was possible to login with the following credentials <User>:<Password>

msfadmin:msfadmin
postgres:postgres
service:service
user:user
```

Insight

The following devices are / software is known to be affected:

- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

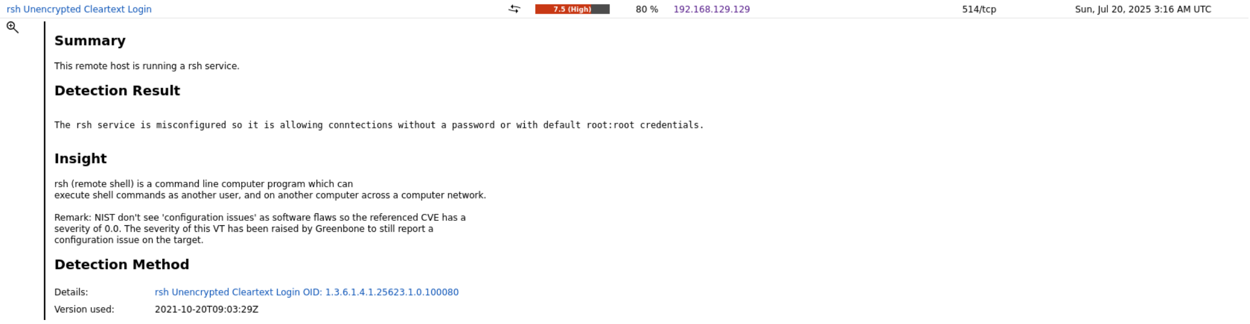
Yes, there were 2 FTP brute force login. The FTP server was accessible due to weak login credentials. A hacker can execute a remote attack to obtain access to sensitive information or change system configuration.

The mitigation is to change these credentials for stronger ones as soon as possible.

d. Any Unencrypted Logins?

i. If so, which program and what was the issue?

ii. What is the mitigation?



rsh Unencrypted Cleartext Login	⇆	7.5 (High)	80 %	192.168.129.129	514/tcp	Sun, Jul 20, 2025 3:16 AM UTC

Summary

This remote host is running a rsh service.

Detection Result

```
The rsh service is misconfigured so it is allowing conntections without a password or with default root:root credentials.
```

Insight

rsh (remote shell) is a command line computer program which can
execute shell commands as another user, and on another computer across a computer network.

Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a
severity of 0.0. The severity of this VT has been raised by Greenbone to still report a
configuration issue on the target.

Detection Method

Details:	rsh Unencrypted Cleartext Login OID: 1.3.6.1.4.1.25623.1.0.100080
Version used:	2021-10-20T09:03:29Z

Yes, the remote host is running a rsh service which is misconfigured and allows connections without a password or with the default credentials. This is a problem because someone else can execute shell commands on another computer across the network.

The mitigation is to disable the remote shell and use a safer option like SSH.