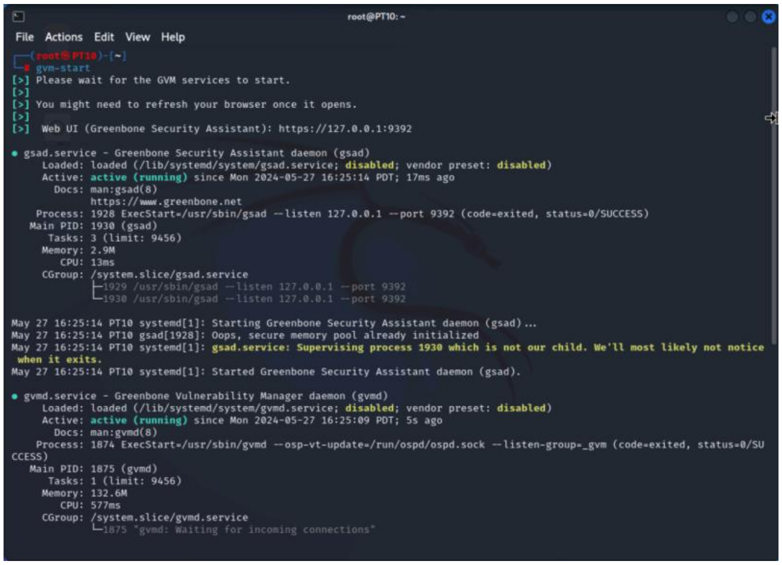
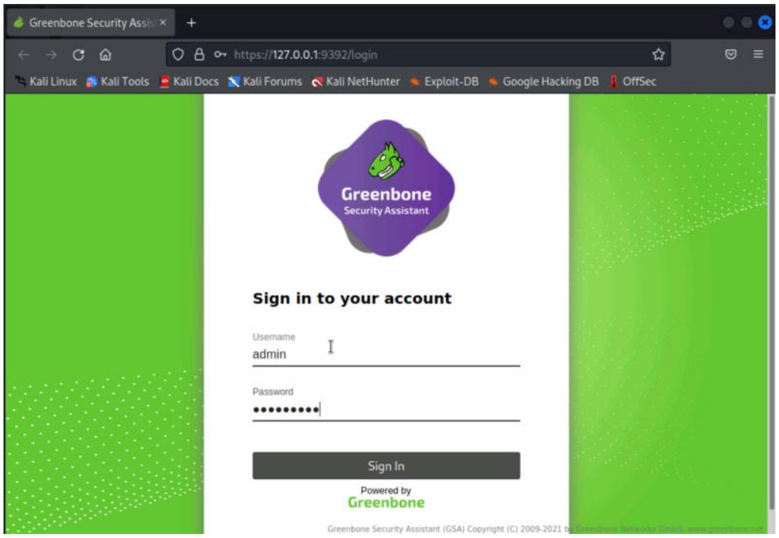
Vulnerability scanning using Greenbone Security Assistant (GSA)

Initiate using gvm-start



```
┌──(root㉿PT10)-[~]
└─# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/lib/systemd/system/gsad.service; disabled; vendor preset: disabled)
     Active: active (running) since Mon 2024-05-27 16:25:14 PDT; 17ms ago
       Docs: man:gsad(8)
             https://www.greenbone.net
    Process: 1928 ExecStart=/usr/sbin/gsad --listen 127.0.0.1 --port 9392 (code=exited, status=0/SUCCESS)
   Main PID: 1930 (gsad)
      Tasks: 3 (limit: 9456)
     Memory: 2.9M
        CPU: 13ms
     CGroup: /system.slice/gsad.service
             ├─1929 /usr/sbin/gsad --listen 127.0.0.1 --port 9392
             └─1930 /usr/sbin/gsad --listen 127.0.0.1 --port 9392

May 27 16:25:14 PT10 systemd[1]: Starting Greenbone Security Assistant daemon (gsad)...
May 27 16:25:14 PT10 gsad[1928]: Oops, secure memory pool already initialized
May 27 16:25:14 PT10 systemd[1]: gsad.service: Supervising process 1930 which is not our child. We'll most likely not notice
 when it exits.
May 27 16:25:14 PT10 systemd[1]: Started Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; vendor preset: disabled)
     Active: active (running) since Mon 2024-05-27 16:25:09 PDT; 5s ago
       Docs: man:gvmd(8)
    Process: 1874 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SU
CCESS)
   Main PID: 1875 (gvmd)
      Tasks: 1 (limit: 9456)
     Memory: 132.6M
        CPU: 577ms
     CGroup: /system.slice/gvmd.service
             └─1875 "gvmd: Waiting for incoming connections"
```

Sign into GSM



Sign in to your account

Username
admin

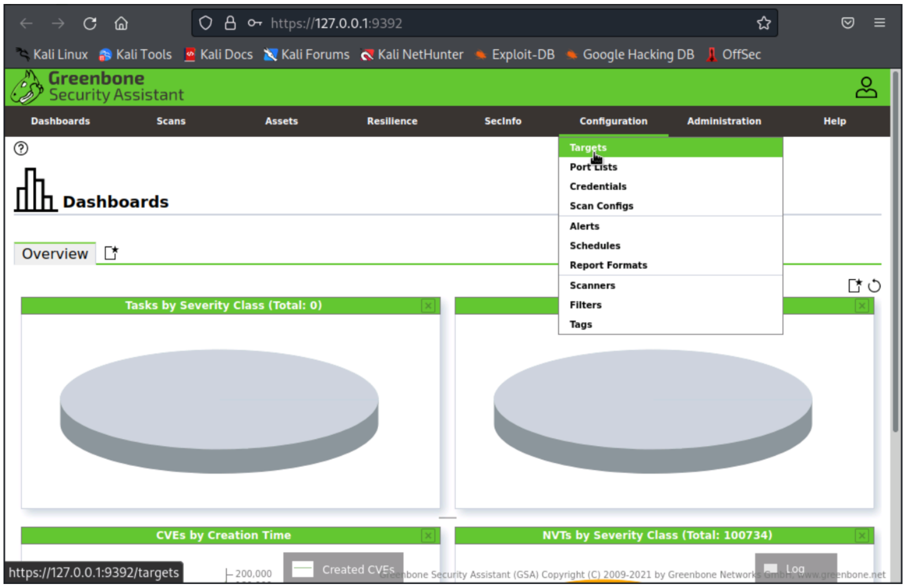
Password
•••••••••

Sign In

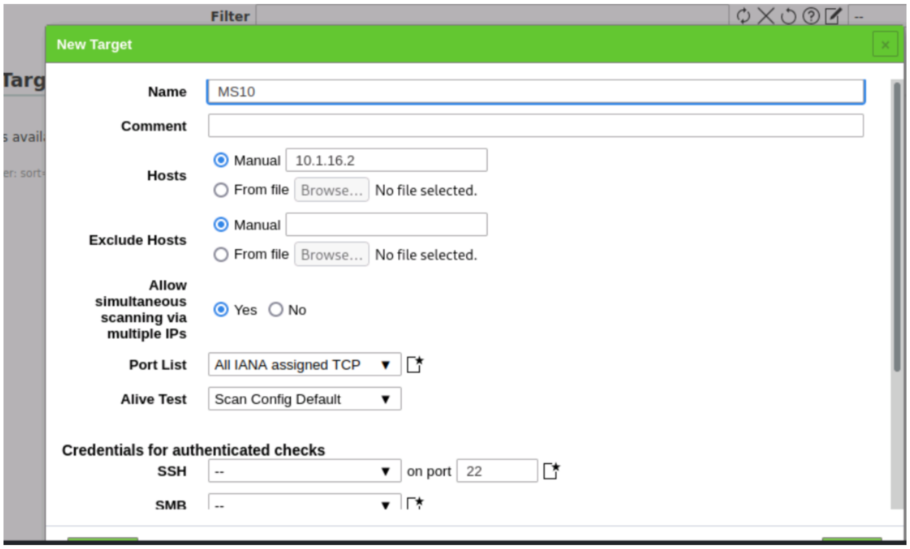
Powered by
Greenbone

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Config > targets



Select target

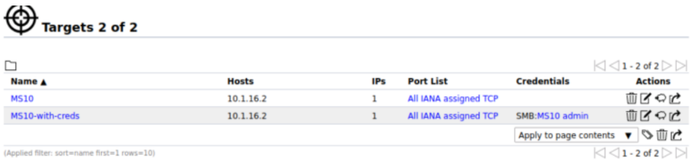


Name	MS10
Comment	
Hosts	● Manual 10.1.16.2 ○ From file Browse... No file selected.
Exclude Hosts	● Manual ○ From file Browse... No file selected.
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	All IANA assigned TCP ▼
Alive Test	Scan Config Default ▼

Credentials for authenticated checks

SSH	-- ▼ on port 22
SMB	-- ▼

Create credentialed and non-credentialed scan



Targets 2 of 2

1 - 2 of 2

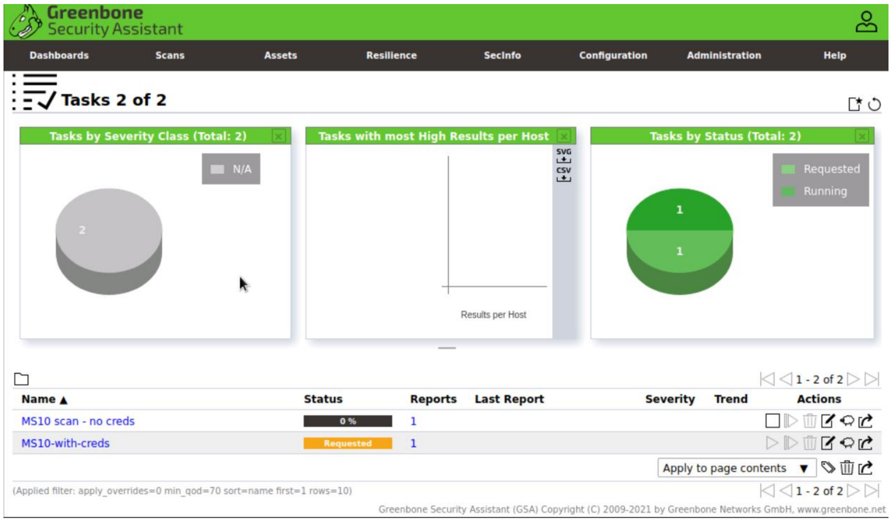
Name ▲	Hosts	IPs	Port List	Credentials	Actions
MS10	10.1.16.2	1	All IANA assigned TCP		
MS10-with-creds	10.1.16.2	1	All IANA assigned TCP	SMB:MS10 admin	

Apply to page contents ▼

(Applied filter: sort=name first=1 rows=10)

1 - 2 of 2

Initiate scans



Tasks 2 of 2

1 - 2 of 2

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
MS10 scan - no creds	0 %	1				
MS10-with-creds	Requested	1				

Apply to page contents ▼

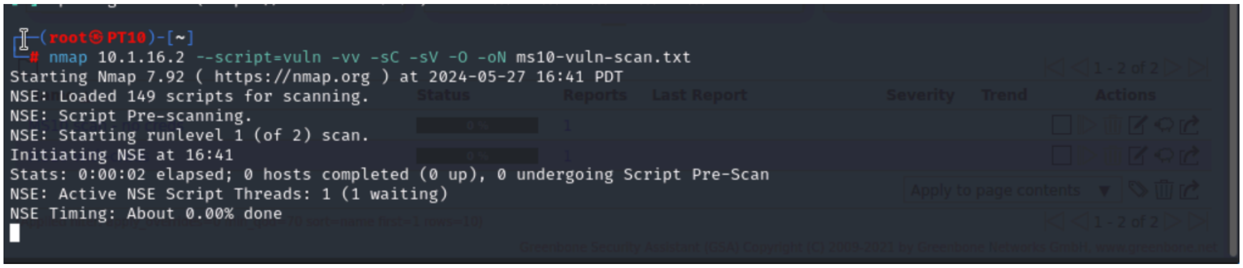
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 2 of 2

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

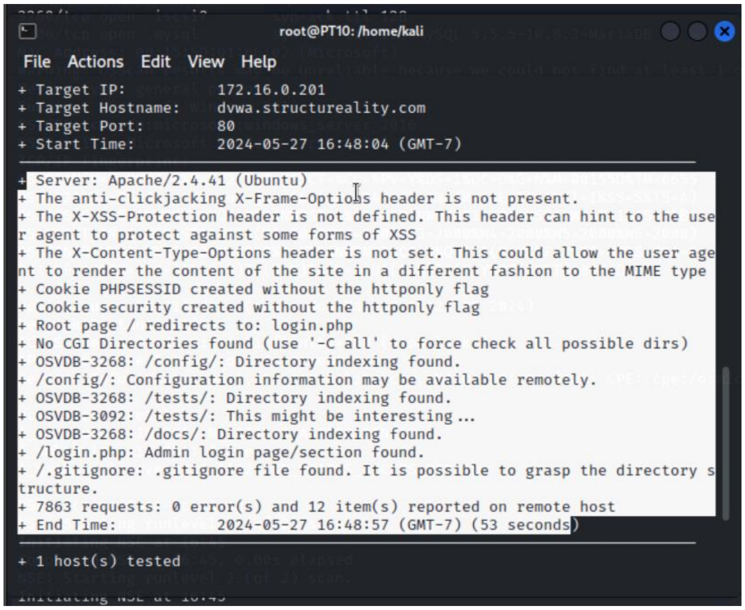
Initiate nmap scan against target system.

--script=vuln: Runs vulnerability detection scripts, -vv: Increases verbosity level, -sC: Uses default scripts, -sV: Enables service version detection, -O: Enables OS detection, -oN ms10-vuln-scan.txt: Saves output to ms10-vuln-scan.txt.



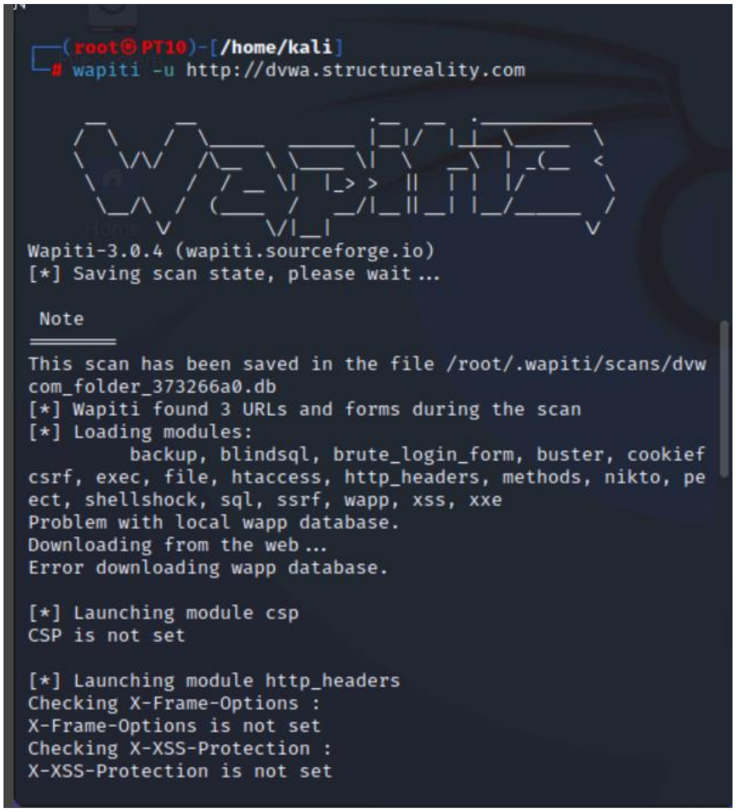
```
┌──(root㉿PT10)-[~]
└─# nmap 10.1.16.2 --script=vuln -vv -sC -sV -O -oN ms10-vuln-scan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-27 16:41 PDT
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:41
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 0.00% done
```

Run Nikto scan



```
+ Target IP:          172.16.0.201
+ Target Hostname:    dvwa.structureality.com
+ Target Port:        80
+ Start Time:         2024-05-27 16:48:04 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Cookie security created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /tests/: Directory indexing found.
+ OSVDB-3092: /tests/: This might be interesting...
+ OSVDB-3268: /docs/: Directory indexing found.
+ /login.php: Admin login page/section found.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory s
tructure.
+ 7863 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2024-05-27 16:48:57 (GMT-7) (53 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

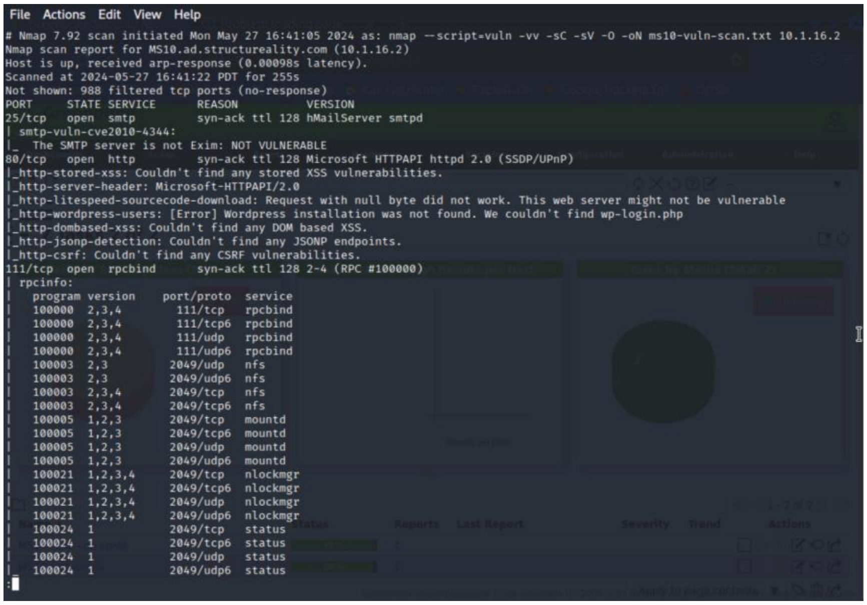
Launch wapiti



```
┌──(root㉿PT10)-[/home/kali]
└─# wapiti -u http://dvwa.structureality.com

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait...

 Note
 ========
This scan has been saved in the file /root/.wapiti/scans/dvw
com_folder_373266a0.db
[*] Wapiti found 3 URLs and forms during the scan
[*] Loading modules:
         backup, blindsql, brute_login_form, buster, cookief
csrf, exec, file, htaccess, http_headers, methods, nikto, pe
ect, shellshock, sql, ssrf, wapp, xss, xxe
Problem with local wapp database.
Downloading from the web...
Error downloading wapp database.

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
```

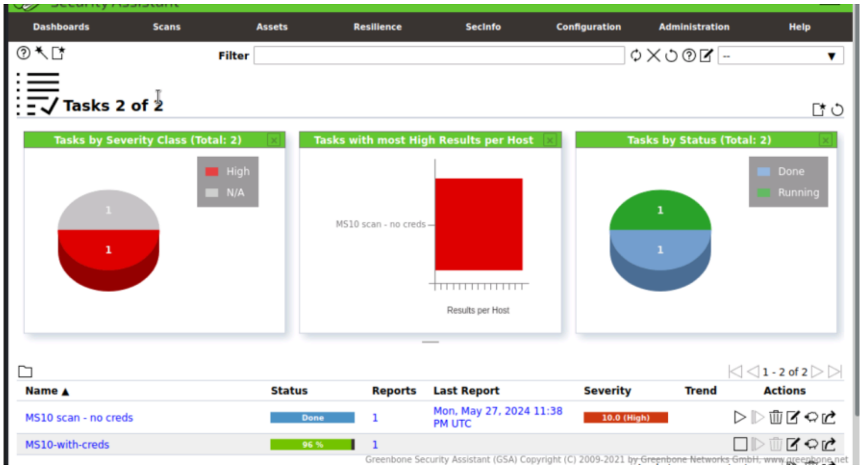
Review Wapiti output file using generated string in output

Review NMAP output file using cat ms10-vuln-scan.txt



```
# Nmap 7.92 scan initiated Mon May 27 16:41:05 2024 as: nmap --script=vuln -vv -sC -sV -O -oN ms10-vuln-scan.txt 10.1.16.2
Nmap scan report for MS10.ad.structureality.com (10.1.16.2)
Host is up, received arp-response (0.00098s latency).
Scanned at 2024-05-27 16:41:22 PDT for 255s
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE      REASON          VERSION
25/tcp   open  smtp         syn-ack ttl 128 hMailServer smtpd
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp   open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
111/tcp  open  rpcbind      syn-ack ttl 128 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
:
```

Review GSA Scan, reports, and hosts

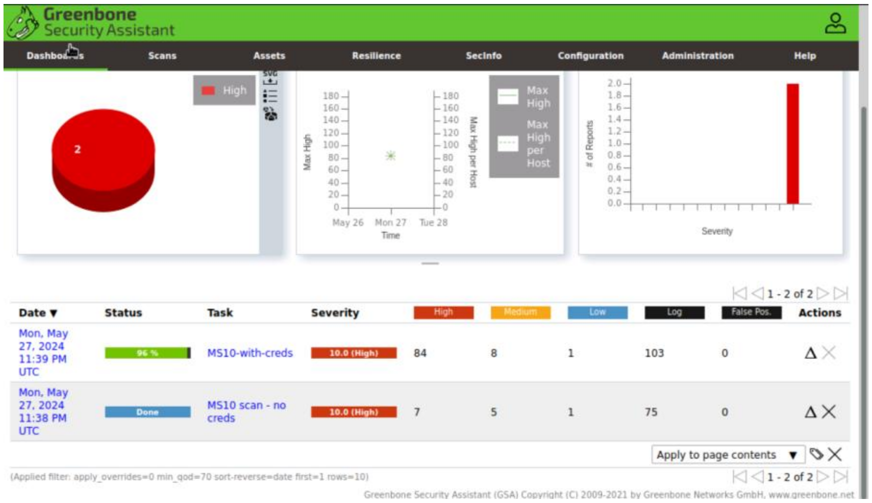


Tasks 2 of 2

1 - 2 of 2

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
MS10 scan - no creds	Done	1	Mon, May 27, 2024 11:38 PM UTC	10.0 (High)		
MS10-with-creds	96 %	1				

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



1 - 2 of 2

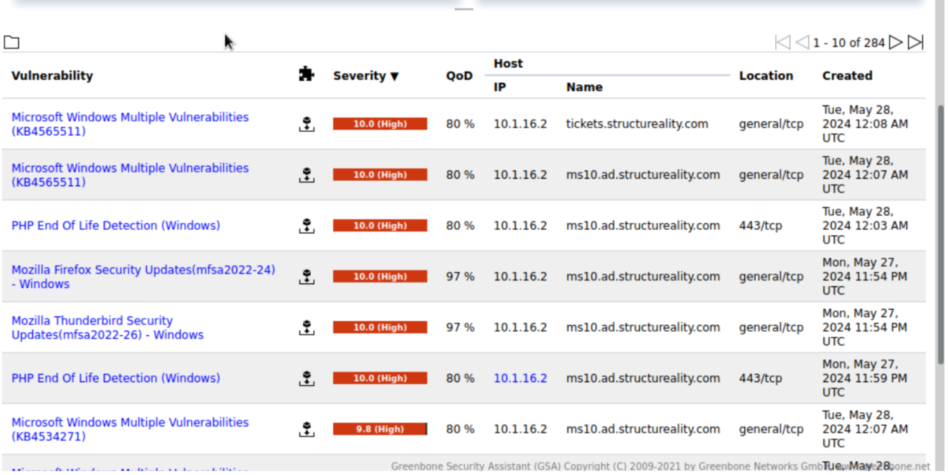
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Mon, May 27, 2024 11:39 PM UTC	96 %	MS10-with-creds	10.0 (High)	84	8	1	103	0	
Mon, May 27, 2024 11:38 PM UTC	Done	MS10 scan - no creds	10.0 (High)	7	5	1	75	0	

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)

1 - 2 of 2

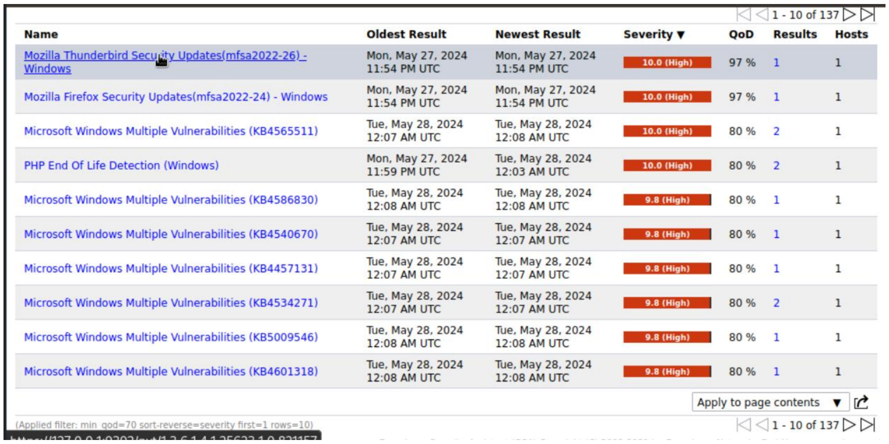
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



1 - 10 of 284

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Microsoft Windows Multiple Vulnerabilities (KB4565511)		10.0 (High)	80 %	10.1.16.2	tickets.structureality.com	general/tcp	Tue, May 28, 2024 12:08 AM UTC
Microsoft Windows Multiple Vulnerabilities (KB4565511)		10.0 (High)	80 %	10.1.16.2	ms10.ad.structureality.com	general/tcp	Tue, May 28, 2024 12:07 AM UTC
PHP End Of Life Detection (Windows)		10.0 (High)	80 %	10.1.16.2	ms10.ad.structureality.com	443/tcp	Tue, May 28, 2024 12:03 AM UTC
Mozilla Firefox Security Updates(mfsa2022-24) - Windows		10.0 (High)	97 %	10.1.16.2	ms10.ad.structureality.com	general/tcp	Mon, May 27, 2024 11:54 PM UTC
Mozilla Thunderbird Security Updates(mfsa2022-26) - Windows		10.0 (High)	97 %	10.1.16.2	ms10.ad.structureality.com	general/tcp	Mon, May 27, 2024 11:54 PM UTC
PHP End Of Life Detection (Windows)		10.0 (High)	80 %	10.1.16.2	ms10.ad.structureality.com	443/tcp	Mon, May 27, 2024 11:59 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4534271)		9.8 (High)	80 %	10.1.16.2	ms10.ad.structureality.com	general/tcp	Tue, May 28, 2024 12:07 AM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

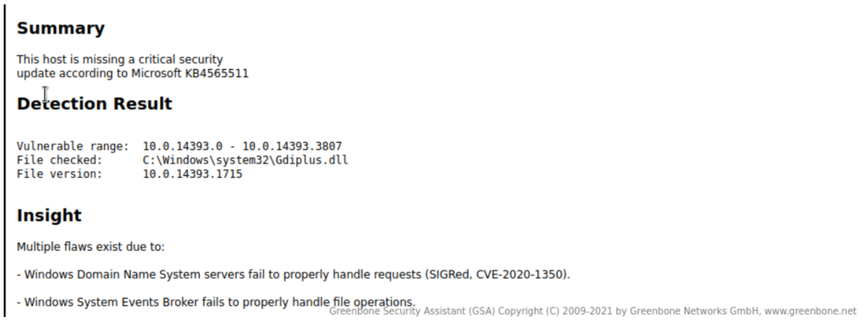


◁ ◁ 1 - 10 of 137 ▷ ▷

Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
Mozilla Thunderbird Security Updates(mfsa2022-26) - Windows	Mon, May 27, 2024 11:54 PM UTC	Mon, May 27, 2024 11:54 PM UTC	10.0 (High)	97 %	1	1
Mozilla Firefox Security Updates(mfsa2022-24) - Windows	Mon, May 27, 2024 11:54 PM UTC	Mon, May 27, 2024 11:54 PM UTC	10.0 (High)	97 %	1	1
Microsoft Windows Multiple Vulnerabilities (KB4565511)	Tue, May 28, 2024 12:07 AM UTC	Tue, May 28, 2024 12:08 AM UTC	10.0 (High)	80 %	2	1
PHP End Of Life Detection (Windows)	Mon, May 27, 2024 11:59 PM UTC	Tue, May 28, 2024 12:03 AM UTC	10.0 (High)	80 %	2	1
Microsoft Windows Multiple Vulnerabilities (KB4586830)	Tue, May 28, 2024 12:08 AM UTC	Tue, May 28, 2024 12:08 AM UTC	9.8 (High)	80 %	1	1
Microsoft Windows Multiple Vulnerabilities (KB4540670)	Tue, May 28, 2024 12:07 AM UTC	Tue, May 28, 2024 12:07 AM UTC	9.8 (High)	80 %	1	1
Microsoft Windows Multiple Vulnerabilities (KB4457131)	Tue, May 28, 2024 12:07 AM UTC	Tue, May 28, 2024 12:07 AM UTC	9.8 (High)	80 %	1	1
Microsoft Windows Multiple Vulnerabilities (KB4534271)	Tue, May 28, 2024 12:07 AM UTC	Tue, May 28, 2024 12:07 AM UTC	9.8 (High)	80 %	2	1
Microsoft Windows Multiple Vulnerabilities (KB5009546)	Tue, May 28, 2024 12:08 AM UTC	Tue, May 28, 2024 12:08 AM UTC	9.8 (High)	80 %	1	1
Microsoft Windows Multiple Vulnerabilities (KB4601318)	Tue, May 28, 2024 12:08 AM UTC	Tue, May 28, 2024 12:08 AM UTC	9.8 (High)	80 %	1	1

(Applied filter: min_qod=70 sort-reverse=severity first=1 rows=10)

◁ ◁ 1 - 10 of 137 ▷ ▷



Summary

This host is missing a critical security
update according to Microsoft KB4565511

Detection Result

```
Vulnerable range:  10.0.14393.0 - 10.0.14393.3807
File checked:      C:\Windows\system32\Gdiplus.dll
File version:      10.0.14393.1715
```

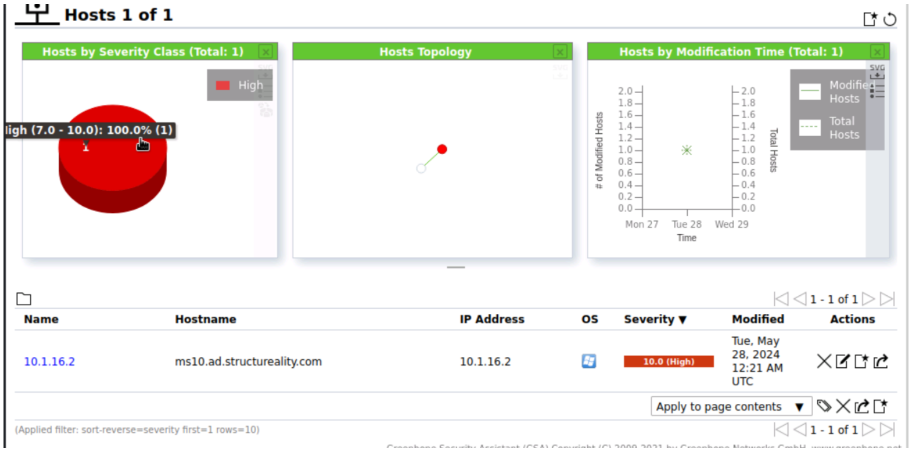
Insight

Multiple flaws exist due to:

- Windows Domain Name System servers fail to properly handle requests (SIGRed, CVE-2020-1350).

- Windows System Events Broker fails to properly handle file operations.

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



Hosts 1 of 1

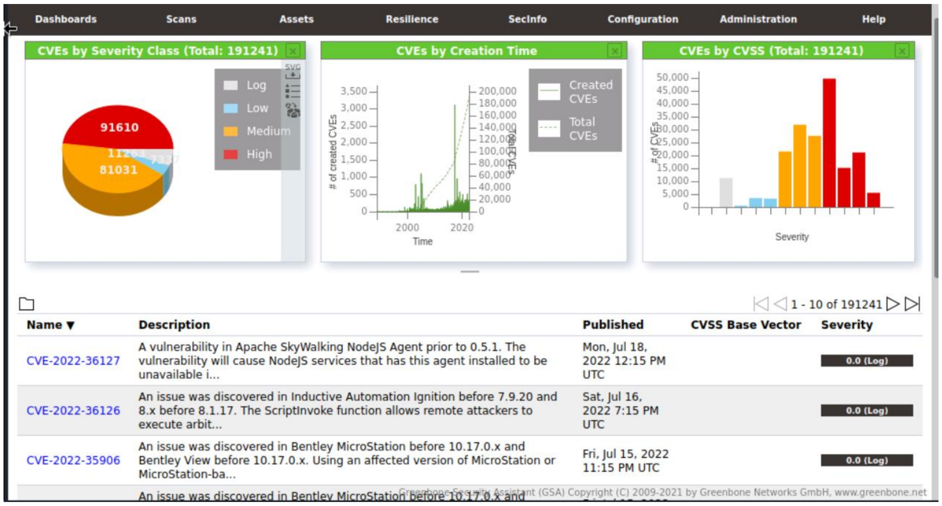
1 - 1 of 1

Name	Hostname	IP Address	OS	Severity ▼	Modified	Actions
10.1.16.2	ms10.ad.structureality.com	10.1.16.2		10.0 (High)	Tue, May 28, 2024 12:21 AM UTC	

Apply to page contents ▼

(Applied filter: sort-reverse=severity first=1 rows=10)

1 - 1 of 1



1 - 10 of 191241

Name ▼	Description	Published	CVSS Base Vector	Severity
CVE-2022-36127	A vulnerability in Apache SkyWalking NodeJS Agent prior to 0.5.1. The vulnerability will cause NodeJS services that has this agent installed to be unavailable i...	Mon, Jul 18, 2022 12:15 PM UTC		0.0 (Log)
CVE-2022-36126	An issue was discovered in Inductive Automation Ignition before 7.9.20 and 8.x before 8.1.17. The ScriptInvoke function allows remote attackers to execute arbit...	Sat, Jul 16, 2022 7:15 PM UTC		0.0 (Log)
CVE-2022-35906	An issue was discovered in Bentley MicroStation before 10.17.0.x and Bentley View before 10.17.0.x. Using an affected version of MicroStation or MicroStation-ba...	Fri, Jul 15, 2022 11:15 PM UTC		0.0 (Log)
	An issue was discovered in Bentley MicroStation before 10.17.0.x and			