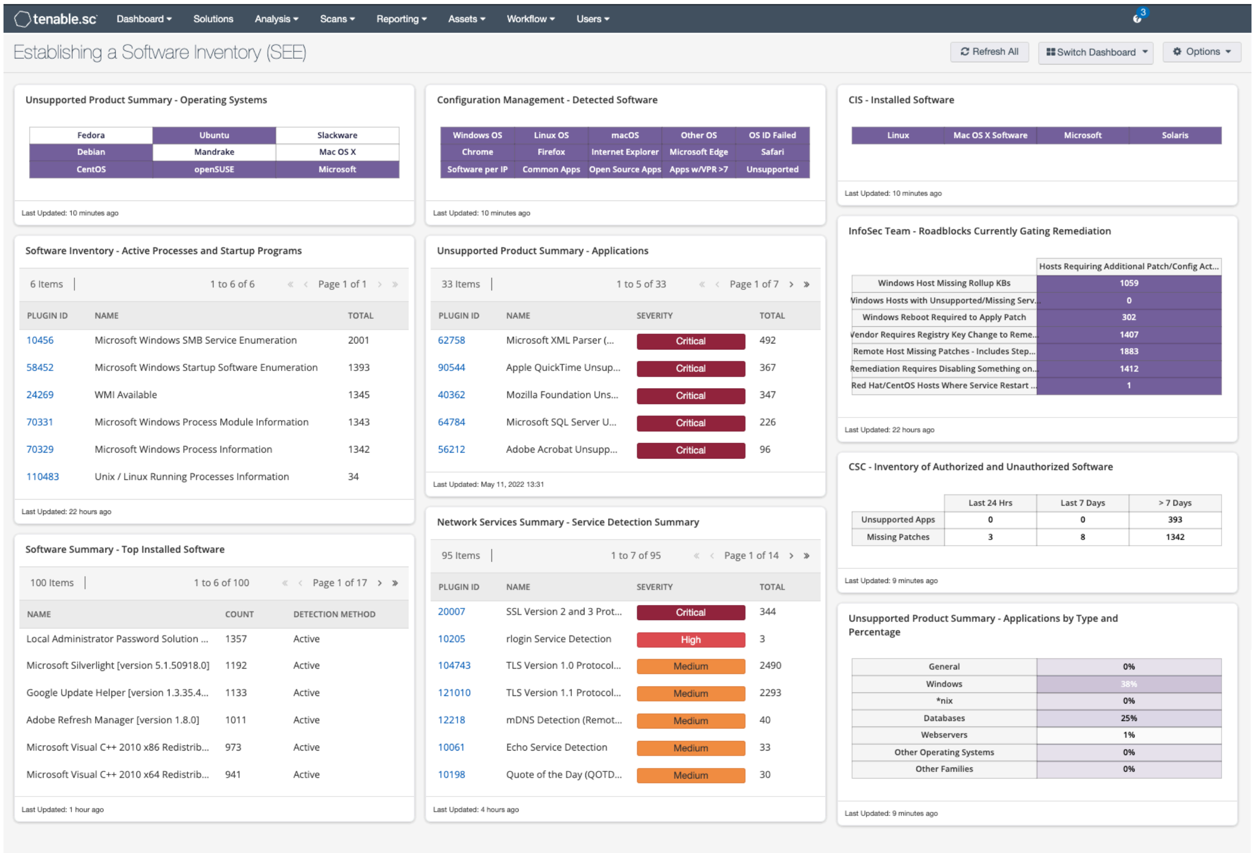
Simeon Hawkins
Capstone Phase 3: Identify Vulnerabilities

Tools for Vulnerability Scanning

1. Tenable Nessus

Purpose: Comprehensive vulnerability scanning across a wide range of systems and applications.
Usage:

- **Setup:** Install Nessus and configure it through the web interface
- **Scan Configuration:** Create new scans by selecting templates based on the target environment (e.g., Basic Network Scan, Advanced Scan).
- **Running Scans:** Schedule scans or run them on demand.
- **Reporting:** Analyze the results and export reports in various formats (PDF, CSV)



Establishing a Software Inventory (SEE)

Unsupported Product Summary - Operating Systems

Fedora	Ubuntu	Slackware
Debian	Mandrake	Mac OS X
CentOS	openSUSE	Microsoft

Last Updated: 10 minutes ago

Software Inventory - Active Processes and Startup Programs

6 Items | 1 to 6 of 6 « ‹ Page 1 of 1 › »

PLUGIN ID	NAME	TOTAL
10456	Microsoft Windows SMB Service Enumeration	2001
58452	Microsoft Windows Startup Software Enumeration	1393
24269	WMI Available	1345
70331	Microsoft Windows Process Module Information	1343
70329	Microsoft Windows Process Information	1342
110483	Unix / Linux Running Processes Information	34

Last Updated: 22 hours ago

Software Summary - Top Installed Software

100 Items | 1 to 6 of 100 « ‹ Page 1 of 17 › »

NAME	COUNT	DETECTION METHOD
Local Administrator Password Solution ...	1357	Active
Microsoft Silverlight [version 5.1.50918.0]	1192	Active
Google Update Helper [version 1.3.35.4...	1133	Active
Adobe Refresh Manager [version 1.8.0]	1011	Active
Microsoft Visual C++ 2010 x86 Redistrib...	973	Active
Microsoft Visual C++ 2010 x64 Redistrib...	941	Active

Last Updated: 1 hour ago

Configuration Management - Detected Software

Windows OS	Linux OS	macOS	Other OS	OS ID Failed
Chrome	Firefox	Internet Explorer	Microsoft Edge	Safari
Software per IP	Common Apps	Open Source Apps	Apps w/VPR >7	Unsupported

Last Updated: 10 minutes ago

Unsupported Product Summary - Applications

33 Items | 1 to 5 of 33 « ‹ Page 1 of 7 › »

PLUGIN ID	NAME	SEVERITY	TOTAL
62758	Microsoft XML Parser (...	Critical	492
90544	Apple QuickTime Unsup...	Critical	367
40362	Mozilla Foundation Uns...	Critical	347
64784	Microsoft SQL Server U...	Critical	226
56212	Adobe Acrobat Unsupp...	Critical	96

Last Updated: May 11, 2022 13:31

Network Services Summary - Service Detection Summary

95 Items | 1 to 7 of 95 « ‹ Page 1 of 14 › »

PLUGIN ID	NAME	SEVERITY	TOTAL
20007	SSL Version 2 and 3 Prot...	Critical	344
10205	rlogin Service Detection	High	3
104743	TLS Version 1.0 Protocol...	Medium	2490
121010	TLS Version 1.1 Protocol...	Medium	2293
12218	mDNS Detection (Remot...	Medium	40
10061	Echo Service Detection	Medium	33
10198	Quote of the Day (QOTD...	Medium	30

Last Updated: 4 hours ago

CIS - Installed Software

Linux	Mac OS X Software	Microsoft	Solaris

Last Updated: 10 minutes ago

InfoSec Team - Roadblocks Currently Gating Remediation

	Hosts Requiring Additional Patch/Config Act...
Windows Host Missing Rollup KBs	1059
Vindows Hosts with Unsupported/Missing Serv...	0
Windows Reboot Required to Apply Patch	302
Vendor Requires Registry Key Change to Reme...	1407
Remote Host Missing Patches - Includes Step...	1883
Remediation Requires Disabling Something on...	1412
Red Hat/CentOS Hosts Where Service Restart ...	1

Last Updated: 22 hours ago

CSC - Inventory of Authorized and Unauthorized Software

	Last 24 Hrs	Last 7 Days	> 7 Days
Unsupported Apps	0	0	393
Missing Patches	3	8	1342

Last Updated: 9 minutes ago

Unsupported Product Summary - Applications by Type and Percentage

General	0%
Windows	38%
*nix	0%
Databases	25%
Webservers	1%
Other Operating Systems	0%
Other Families	0%

Last Updated: 9 minutes ago

Pros:

- Wide range of pre-configured scan templates.
- Detailed vulnerability descriptions and remediation steps.
- Regular updates with new vulnerability signatures.

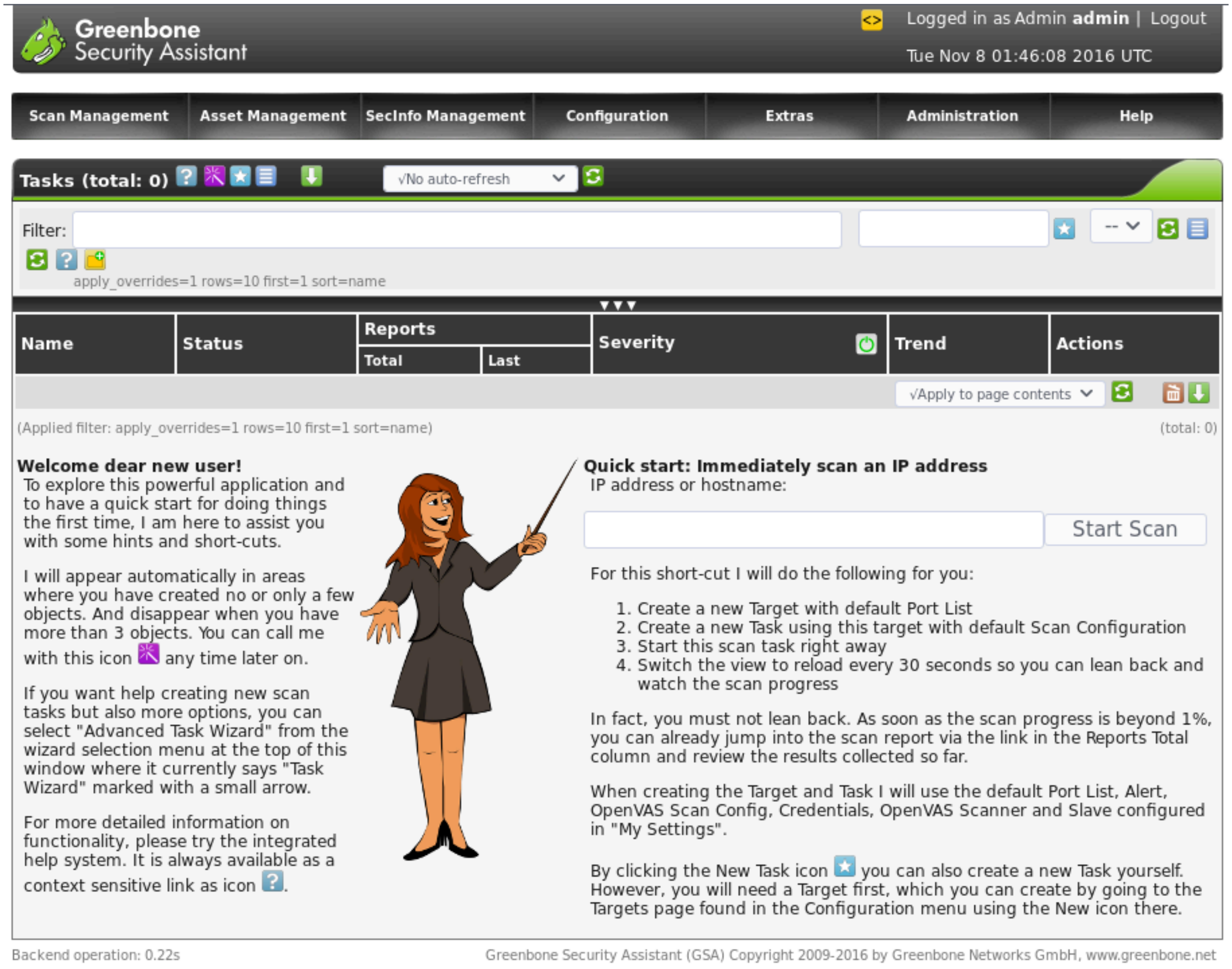
Cons:

- Licensing costs can be high
- Can be resource-intensive, potentially impacting network performance during scans.

2. OpenVAS

Purpose: Open-source vulnerability scanning solution
Usage:

- **Setup:** Install OpenVAS and configure it through the Greenbone Security Assistant web interface.
- **Scan Configuration:** Define scan tasks, targets, and schedules.
- **Running Scans:** Launch scans and monitor progress.
- **Reporting:** Review scan results and generate reports.



Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon ✳ any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon ?.

Quick start: Immediately scan an IP address

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the default Port List, Alert, OpenVAS Scan Config, Credentials, OpenVAS Scanner and Slave configured in "My Settings".

By clicking the New Task icon ★ you can also create a new Task yourself. However, you will need a Target first, which you can create by going to the Targets page found in the Configuration menu using the New icon there.

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Pros:

- Free and open-source

- Regular updates and community support
- Comprehensive vulnerability database.

Cons:

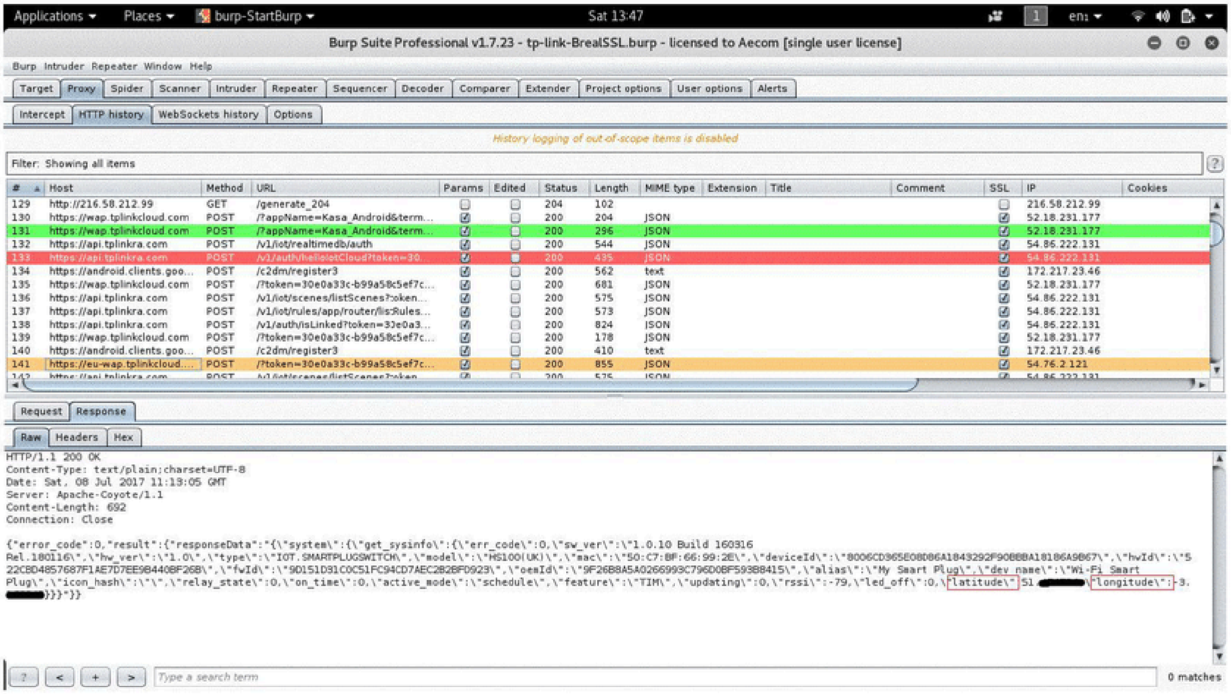
- Initial setup and configuration can be complex
- May generate more false positives compared to commercial solutions.

3. **Burp Suite**

Purpose: Web application security testing and vulnerability scanning.

Usage:

- **Setup:** Install Burp Suite and configure it for intercepting and analyzing web traffic.
- **Scan Configuration:** Use the scanner to perform automated vulnerability scans on web applications.
- **Manual Testing:** Utilize various Burp Suite tools (e.g., Intruder, Repeater) for manual testing.
- **Reporting:** Generate detailed reports on discovered vulnerabilities.



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies
129	http://216.58.212.99	GET	/generate_204	☐	☐	204	102					☐	216.58.212.99	
130	https://wap.tplinkcloud.com	POST	/?appName=Kasa_Android&term...	☑	☐	200	204	JSON				☑	52.18.231.177	
131	https://wap.tplinkcloud.com	POST	/?appName=Kasa_Android&term...	☑	☐	200	296	JSON				☑	52.18.231.177	
132	https://api.tplinkra.com	POST	/v1/iot/realtimedb/auth	☑	☐	200	544	JSON				☑	54.86.222.131	
133	https://api.tplinkra.com	POST	/v1/auth/helloIotCloud?token=30...	☑	☐	200	435	JSON				☑	54.86.222.131	
134	https://android.clients.goo...	POST	/c2dm/register3	☑	☐	200	562	text				☑	172.217.23.46	
135	https://wap.tplinkcloud.com	POST	/?token=30e0a33c-b99a58c5ef7c...	☑	☐	200	681	JSON				☑	52.18.231.177	
136	https://api.tplinkra.com	POST	/v1/iot/scenes/listScenes?token...	☑	☐	200	575	JSON				☑	54.86.222.131	
137	https://api.tplinkra.com	POST	/v1/iot/rules/app/router/listRules...	☑	☐	200	573	JSON				☑	54.86.222.131	
138	https://api.tplinkra.com	POST	/v1/auth/isLinked?token=30e0a3...	☑	☐	200	824	JSON				☑	54.86.222.131	
139	https://wap.tplinkcloud.com	POST	/?token=30e0a33c-b99a58c5ef7c...	☑	☐	200	178	JSON				☑	52.18.231.177	
140	https://android.clients.goo...	POST	/c2dm/register3	☑	☐	200	410	text				☑	172.217.23.46	
141	https://eu-wap.tplinkcloud....	POST	/?token=30e0a33c-b99a58c5ef7c...	☑	☐	200	855	JSON				☑	54.76.2.121	
142	https://api.tplinkra.com	POST	/v1/iot/scenes/listScenes?token	☑	☐	200	575	JSON				☑	54.86.222.131	

```
HTTP/1.1 200 OK
Content-Type: text/plain;charset=UTF-8
Date: Sat, 08 Jul 2017 11:13:05 GMT
Server: Apache-Coyote/1.1
Content-Length: 692
Connection: Close

{"error_code":0,"result":{"responseData":"{\"system\":{\"get_sysinfo\":{\"err_code\":0,\"sw_ver\":\"1.0.10 Build 160316
Rel.180116\",\"hw_ver\":\"1.0\",\"type\":\"IOT.SMARTPLUGSWITCH\",\"model\":\"HS100(UK)\",\"mac\":\"50:C7:BF:66:99:2E\",\"deviceId\":\"8006CD365E08D86A1843292F90BBBA18186A9B67\",\"hwId\":\"5
22CBD4857687F1AE7D7EE9B440BF26B\",\"fwId\":\"9D151D91C0C51FC94CD7AEC2B2BFD923\",\"oemId\":\"9F26B8A5A0266993C796D0BF593B8415\",\"alias\":\"My Smart Plug\",\"dev_name\":\"Wi-Fi Smart
Plug\",\"icon_hash\":\"\",\"relay_state\":0,\"on_time\":0,\"active_mode\":\"schedule\",\"feature\":\"TIM\",\"updating\":0,\"rssi\":-79,\"led_off\":0,\"latitude\":51[redacted]\"longitude\":-3.
[redacted]}}}"}}
```

Pros:

- Comprehensive toolset for web application security testing
- Strong support for manual testing and exploitation
- Regular updates with new features and vulnerabilities.

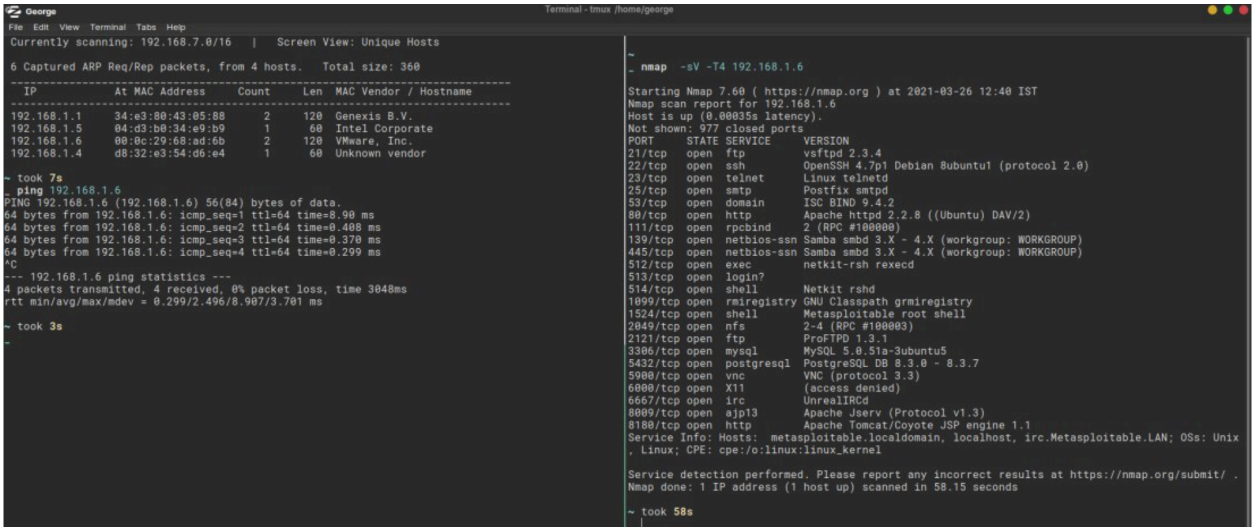
Cons:

- Requires a good understanding of web application security.
- Can be time-consuming for large applications.

4. Nmap with NSE Scripts

Purpose: Network scanning and vulnerability detection using Nmap Scripting Engine (NSE).
Usage:

- **Setup:** Install Nmap and run commands from the command line.
- **Scan Configuration:** Use NSE scripts for vulnerability scanning (e.g., nmap –script vuln 192.168.1.1).
- **Custom Scripts:** Write and use custom NSE scripts for specific vulnerabilities.
- **Reporting:** Analyze scan outputs for identified vulnerabilities.


George
Terminal - tmux /home/george
File Edit View Terminal Tabs Help

```
 Currently scanning: 192.168.7.0/16   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     34:e3:80:43:05:88      2     120  Genexis B.V.
 192.168.1.5     04:d3:b0:34:e9:b9      1      60  Intel Corporate
 192.168.1.6     00:0c:29:68:ad:6b      2     120  VMware, Inc.
 192.168.1.4     d8:32:e3:54:d6:e4      1      60  Unknown vendor

~ took 7s
_ ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=8.90 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=0.408 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=64 time=0.370 ms
64 bytes from 192.168.1.6: icmp_seq=4 ttl=64 time=0.299 ms
^C
--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3048ms
rtt min/avg/max/mdev = 0.299/2.496/8.907/3.701 ms

~ took 3s
_
```

```
~
_ nmap  -sV -T4 192.168.1.6

Starting Nmap 7.60 ( https://nmap.org ) at 2021-03-26 12:40 IST
Nmap scan report for 192.168.1.6
Host is up (0.00035s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.15 seconds

~ took 58s
```

Pros:

- Highly flexible and customizable.
- Can perform both general and specific vulnerability scans.
- Widely used and well-documented.

Cons:

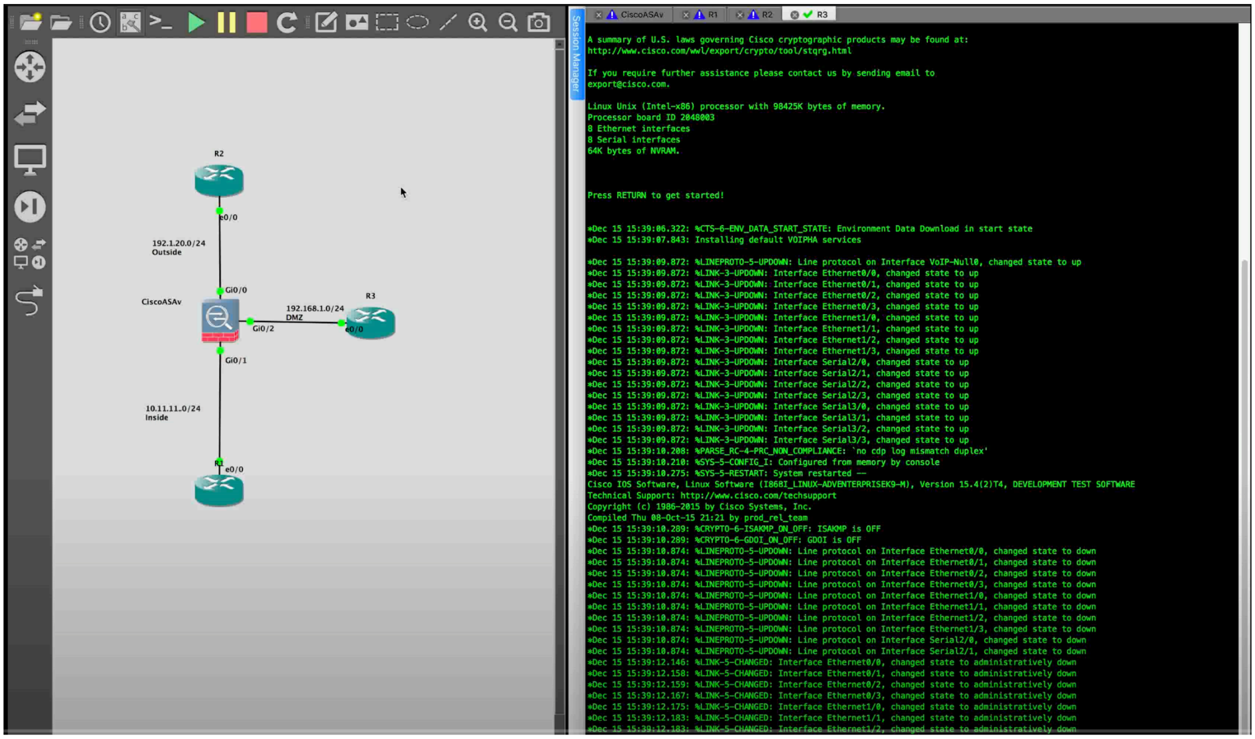
- Requires knowledge of scripting for custom scans.

- Output can be verbose and require careful analysis.

5. **Cisco Adaptive Security Appliance (ASA) Vulnerability Scanner**

Purpose: Specific to Cisco ASA devices, identifying misconfigurations and vulnerabilities.
Usage:

- **Setup:** Install and configure the ASA scanner tool
- **Scan Configuration:** Define the IP range and credentials for scanning Cisco ASA devices.
- **Running Scans:** Launch scans and monitor progress.
- **Reporting:** Review detailed reports on configuration issues and vulnerabilities.



```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Linux Unix (Intel-x86) processor with 98425K bytes of memory.
Processor board ID 2048003
8 Ethernet interfaces
8 Serial interfaces
64K bytes of NVRAM.



Press RETURN to get started!


*Dec 15 15:39:06.322: %CTS-6-ENV_DATA_START_STATE: Environment Data Download in start state
*Dec 15 15:39:07.843: Installing default VOIPHA services

*Dec 15 15:39:09.872: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial2/2, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial2/3, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial3/1, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial3/2, changed state to up
*Dec 15 15:39:09.872: %LINK-3-UPDOWN: Interface Serial3/3, changed state to up
*Dec 15 15:39:10.208: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no cdp log mismatch duplex'
*Dec 15 15:39:10.210: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 15 15:39:10.275: %SYS-5-RESTART: System restarted --
Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.4(2)T4, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 08-Oct-15 21:21 by prod_rel_team
*Dec 15 15:39:10.289: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Dec 15 15:39:10.289: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
*Dec 15 15:39:10.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
*Dec 15 15:39:12.146: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Dec 15 15:39:12.158: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Dec 15 15:39:12.159: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Dec 15 15:39:12.167: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*Dec 15 15:39:12.175: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
*Dec 15 15:39:12.183: %LINK-5-CHANGED: Interface Ethernet1/1, changed state to administratively down
*Dec 15 15:39:12.183: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
```

Pros:

- Tailored specifically for Cisco ASA devices.
- Identifies both vulnerabilities and misconfigurations.
- Provides actionable remediation steps.

Cons:

- Limited to Cisco ASA devices
- Requires specific expertise in Cisco AS configurations.