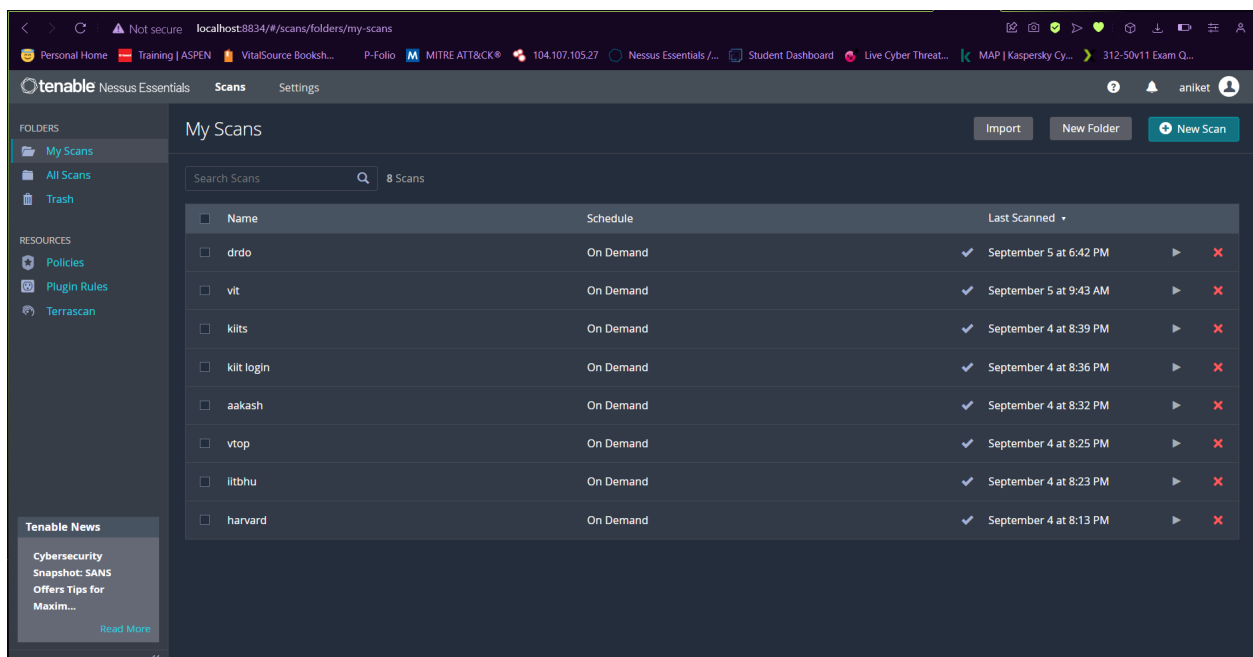


task 8

(04/09/23): Scan any website to check the vulnerabilities in the website using nessus and make a report on it

so for scanning of vulnerabilities we will use nessus tool. Nessus is a platform developed by Tenable that **scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.**



so in this i have performed the scans on many websites just out of curiosity to explore more about the tool so we will take example of some of websites one is our very favourite website vit.ac.in and one is certifiedhacker.com this website so we will go step by step

1..... we want to get the ipv4 address to start with so we will go to nslookup.io to get the ipv4 address of the website

www.nslookup.io/domains/certifiedhacker.com/dns-records/

Personal Home Training | ASPEN VitalSource Booksh... P-Folio MITRE ATT&CK® 104.107.105.27 Nessus Essentials /... Student Dashboard Live Cyber Threat... MAP | Kaspersky Cy... 312-50v11 Exam Q...

DNS for developers module 3 just dropped — 10 lessons on operational DNS

Nslookup.io Learning Browser extension API

DNS records for **certifiedhacker.com**

Cloudflare Google DNS OpenDNS Authoritative Local DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 162.241.216.11	4h

AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

By Nslookup.io

DNS for Developers

Never be confused about DNS again.

162.241.216.11

2..... now we will go back to nessus and we will click on new scan then we will click on basic network scan to start the setup phase and we will enter all the data required in this case and will click on start button

localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2f0619c19d7bd788d6be818b65/settings/basic/general

Personal Home Training | ASPEN VitalSource Booksh... P-Folio MITRE ATT&CK® 104.107.105.27 Nessus Essentials /... Student Dashboard Live Cyber Threat... MAP | Kaspersky Cy... 312-50v11 Exam Q...

tenable Nessus Essentials Scans Settings

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
TerraScan

New Scan / Basic Network Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: certified hacker

Description:

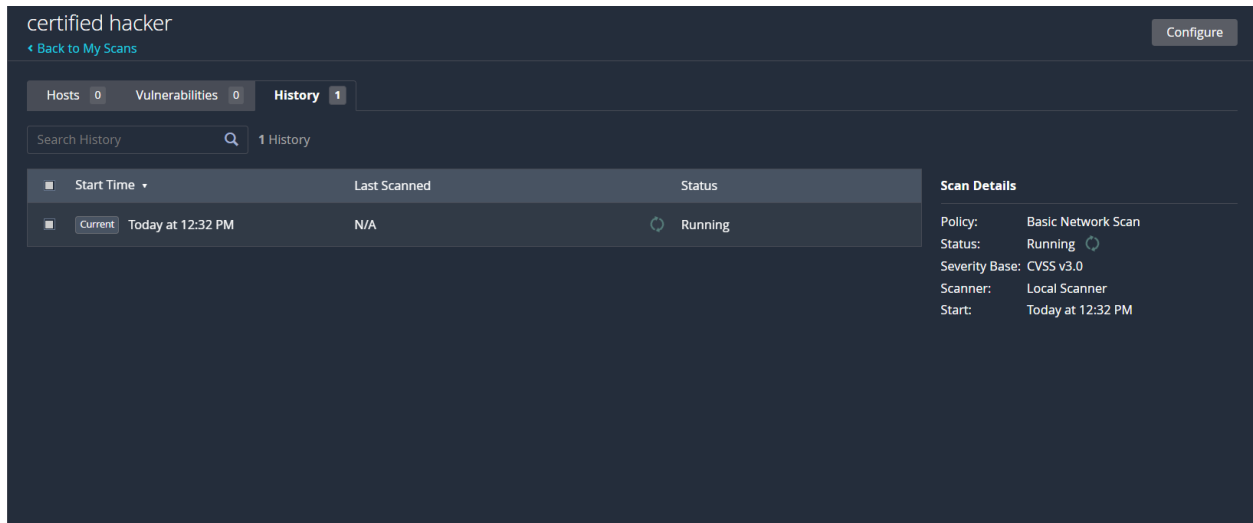
Folder: My Scans

Targets: 162.241.216.11

Upload Targets [Add File](#)

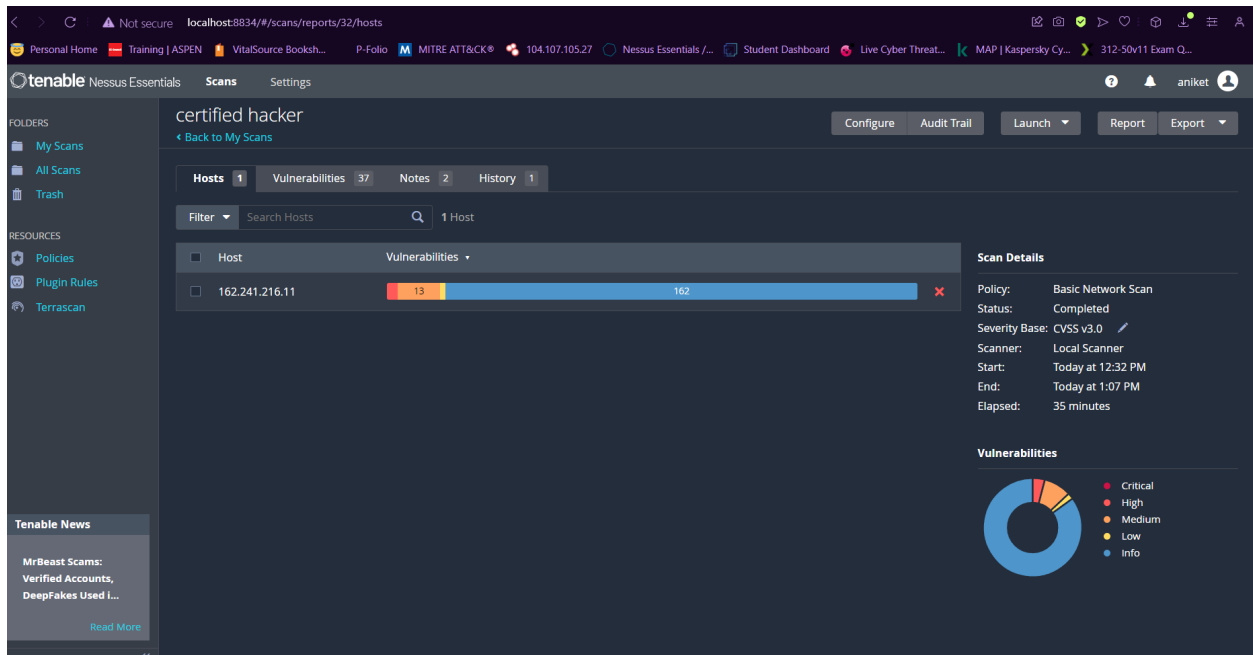
Tenable News
Moxa MXSecurity Unauthenticated Device Registratio...
[Read More](#)

it will start scanning and will take some time as this website have a lot of open ports



so after 35 minutes we got our final report of the scan

3 high 13 medium and so on



tenable Nessus Essentials Scans Settings

certified hacker / 162.241.216.11

Configure Audit Trail Launch Report Export

Vulnerabilities 37

Filter Search Vulnerabilities 37 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	31
MIXED	DNS (Multiple Issues)	DNS	4
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Sup...	Service detection	1
MIXED	TLS (Multiple Issues)	Service detection	22
LOW	2.6	...	SMTP Service Cleartext Login Perm...	SMTP problems	1
INFO	IETF Md5 (Multiple Issues)	General	16
INFO	TLS (Multiple Issues)	General	13
INFO	HTTP (Multiple Issues)	Web Servers	5
INFO	TLS (Multiple Issues)	Misc.	3
INFO	ISC Bind (Multiple Issues)	DNS	2

Host Details

IP: 162.241.216.11
 DNS: box5331.bluehost.com
 OS: Linux Kernel 2.6
 Start: Today at 12:32 PM
 End: Today at 1:07 PM
 Elapsed: 35 minutes
 KB: Download

Vulnerabilities

Critical
 High
 Medium
 Low
 Info

see one of the high vulnerability rating is 7.5

tenable Nessus Essentials Scans Settings

certified hacker / Plugin #42873

Configure Audit Trail Launch Report Export

Vulnerabilities 37

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Plugin Details

Severity: High
 ID: 42873
 Version: 1.21
 Type: remote
 Family: General
 Published: November 23, 2009
 Modified: February 3, 2021

VPR Key Drivers

Threat Recency: No recorded events
 Threat Intensity: Very Low
 Exploit Code Maturity: PoC
 Age of Vuln: 730 days +
 Product Coverage: High
 CVSSV3 Impact Score: 3.6
 Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.1

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Output

Name	Code	KEY	Auth	Encryption	MAC
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC(168)	SHA1
ADH-DES-CBC3-SHA	0x00, 0x1b	DH	None	3DES-CBC(168)	SHA1
ECDHE-RSA-DES-CBC3-SHA	0xc0, 0x12	ECDH	RSA	3DES-CBC(168)	SHA1
AECDH-DES-CBC3-SHA	0xc0, 0x17	ECDH	None	3DES-CBC(168)	SHA1
EDH-RSA-DES-CBC3-SHA	0xc0, 0x18	ECDH	RSA	3DES-CBC(168)	SHA1

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also
<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Output

```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name                      Code      KEX      Auth    Encryption      MAC
-----
EDH-RSA-DES-CBC3-SHA      0x00, 0x16 DH      RSA     3DES-CBC (168)  SHA1
ADH-DES-CBC3-SHA          0x00, 0x1B DH      None    3DES-CBC (168)  SHA1
ECDHE-RSA-DES-CBC3-SHA    0xC0, 0x12 ECDH    RSA     3DES-CBC (168)  SHA1
AECDH-DES-CBC3-SHA        0xC0, 0x17 ECDH    None    3DES-CBC (168)  SHA1
DES-CBC3-SHA              0x00, 0x0A RSA     RSA     3DES-CBC (168)  SHA1
more...

```

To see debug logs, please visit individual host

Port	Hosts
21 / tcp / ftp	162.241.216.11

```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name                      Code      KEX      Auth    Encryption      MAC
-----
DES-CBC3-SHA              0x00, 0x0A RSA     RSA     3DES-CBC (168)  SHA1

The fields above are :

```

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.1
Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date: August 24, 2016
In the news: true

Reference Information

CVE: [CVE-2016-2183](#)

and i will upload the report too in form of html and nessus file

[certified hacker__oopvna.html](#)

[certified hacker_q0g3na.nessus](#)

and in similar way i have performed the same for VIT website so this is the final report of the scan

tenable Nessus Essentials Scans Settings

vit

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 23 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
136.233.9.13	1 1 32

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 5 at 9:21 AM
End: September 5 at 9:43 AM
Elapsed: 22 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Tenable News

PaperCut NG
Unauthenticated
XMLRPC Functionality

Read More

tenable Nessus Essentials Scans Settings

vit

Configure Audit Trail

Back to My Scans

Hosts 1 Vulnerabilities 23 History 1

Filter Search Vulnerabilities 23 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
MEDIUM	6.1	5.7	jQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1		
LOW	3.1	2.2	Web Server HTTP Header Internal I...	Web Servers	1		
INFO	SSL (Multiple Issues)	General	4		
INFO	HTTP (Multiple Issues)	Web Servers	3		
INFO	Web Server (Multiple Issues)	Web Servers	3		
INFO	TLS (Multiple Issues)	General	2		
INFO	Service Detection	Service detection	3		
INFO	Nessus SYN scanner	Port scanners	2		
INFO	Additional DNS Hostnames	General	1		
INFO	Apache HTTP Server Version	Web Servers	1		

Tenable News

PaperCut NG
Unauthenticated
XMLRPC Functionality

Read More

tenable Nessus Essentials Scans Settings

vit / Plugin #136929
← Back to Vulnerabilities

Hosts 1 Vulnerabilities 23 History 1

MEDIUM JQuery 1.2 < 3.5.0 Multiple XSS

Description
According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

Solution
Upgrade to JQuery version 3.5.0 or later.

See Also
<https://blog.jquery.com/2020/04/10/jquery-3.5.0-released/>
<https://security.paloaltonetworks.com/PAN-SA-2020-0007>

Output
URL : https://136.233.9.13/sites/all/themes/vittheme/js/jquery-2.1.1.min.js?rdiaip4
Installed version : 2.1.1
Fixed version : 3.5.0

To see debug logs, please visit individual host

Plugin Details

Severity:	Medium
ID:	136929
Version:	1.11
Type:	remote
Family:	CGI abuses : XSS
Published:	May 28, 2020
Modified:	December 5, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuln: 730 days +
Product Coverage: Very High
CVSS3 Impact Score: 2.7
Threat Sources: No recorded events

Risk Information
Vulnerability Priority Rating (VPR): 5.7

vit_iwmt3r

vit_6nlfph.nessus

vit_iwmt3r.html