5. Vulnerability Analysis

HACKER SCHOOL™

ETHICAL HACKING

Designed by Freepik

Theory

designed by freepik

Vulnerability

A bug or flaw or a state of being exposed which leads to a critical hacking attack from the Hacker is called Vulnerability.

Vulnerability Research

It is the process by which security flaws in technology are identified. Vulnerability research does not always involve reverse engineering, code analysis, etc. Performing vulnerability research against technology pre-release enables technology vendors to provide their customers with higher quality products and higher levels of trust and security.

List of vulnerability research websites

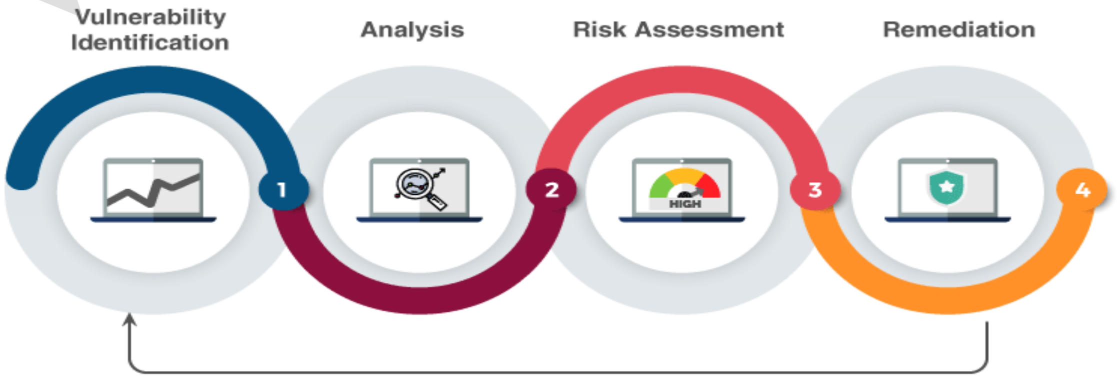
- securityfocus.com
- vulnerability-lab.com
- us-cert.gov
- packetstormsecurity.com
- nvd.nist.gov
- cvedetails.com

Vulnerability Analysis

Vulnerability analysis is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications or network infrastructure. This phase allows the organization to perform security assessment with the necessary knowledge, awareness and risk background to understand the threats and react appropriately.

Attackers perform vulnerability analysis to identify security loopholes in the target organization's network or communication infrastructure. Attackers take advantage of identified vulnerabilities to perform further exploitation of that target network.

The vulnerability scanner (software) compares details about the target attack surface to a database of information about known security vulnerabilities in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts.



Objectives

- Identify vulnerabilities ranging from critical design flaws to simple misconfigurations.
- Document the vulnerabilities so that the developers and networks administrators can easily identify and reproduce the findings.
- Create guidance to assist network administrators and developers with remediating the identified vulnerabilities

Types of vulnerability Assessments

- External Scans
- Internal Scans
- Environment Scans
- Host assessment
- Network assessment
- Database assessment

Common types of Vulnerabilities

- Missing data encryption
- SQL injection
- Buffer-overflow
- Missing authentication for critical functions
- Missing authorization
- Unrestricted upload of dangerous file types
- Cross-site request forgery
- Download of codes without integrity checks
- Weak passwords
- Path/Directory traversal

List of network vulnerability scanners

- Nessus
- GFI LanGuard - Scans both Hardware & Software Vulnerabilities.
- Qualys guard - Works both on LAN & WAN
- Saint
- Nexpose - Paid and free solution available from Offensive security
- Core impact - Scanner and Exploit framework
- OpenVAS

Types of Vulnerability Assessment Reports

- Technical Report - Includes detailed description related to vulnerabilities found on the target computer(s)
- Non-Technical Report - Brief report on vulnerabilities found on the target computer(s). This report includes graphs and charts that are easy to understand the risk.

CVE (Common Vulnerabilities and Exposures)

CVE is a dictionary of standardized identifiers for common software vulnerabilities and exposures. CVE IDs, i.e., CVE-2018-1002100 which are assigned by CVE Numbering Authorities from around the world, ensures confidence when used to share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange. CVE IDs act as a benchmark for evaluating security services

CVSS (Common Vulnerability Scoring System)

CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities. CVSS assessment consists of three metrics for measuring vulnerabilities

1. **Base Metrics:** It represents the inherent qualities of a vulnerability
2. **Temporal Metrics:** It represents the features that keep on changing during the lifetime of a vulnerability.
3. **Environmental Metrics:** It represents the vulnerabilities that are based on a particular environment or implementation.

Each metrics sets a score from 1-10, ten being the most severe. CVSS score is calculated and generated by a vector string, which represents the numerical score for each group in the form of a block of text. CVSS calculator is developed to rank the security vulnerabilities and provide the user with overall severity and risk related to the vulnerability.

Ddos-attack
BOOM
PC
Password Hacking
Protection
Hacking Mail
PC
PETYA A
Virus Attack

Practicals

INDEX

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

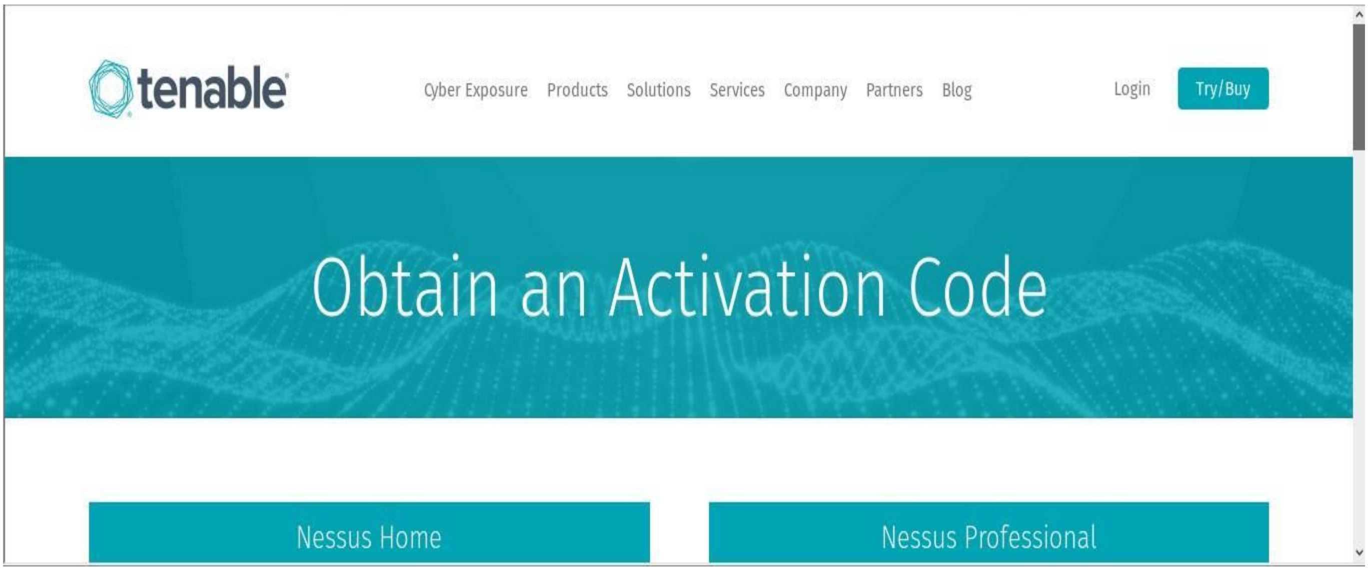
Practical 1: Performing vulnerability assessment using the Nessus Vulnerability Scanner.

Description: In this practical we will learn how to get a Nessus activation key, downloading, installing and setting up Nessus to perform vulnerability assessment on the target system. And also learn, after performing the assessment, how to generate vulnerability assessment reports in different formats.

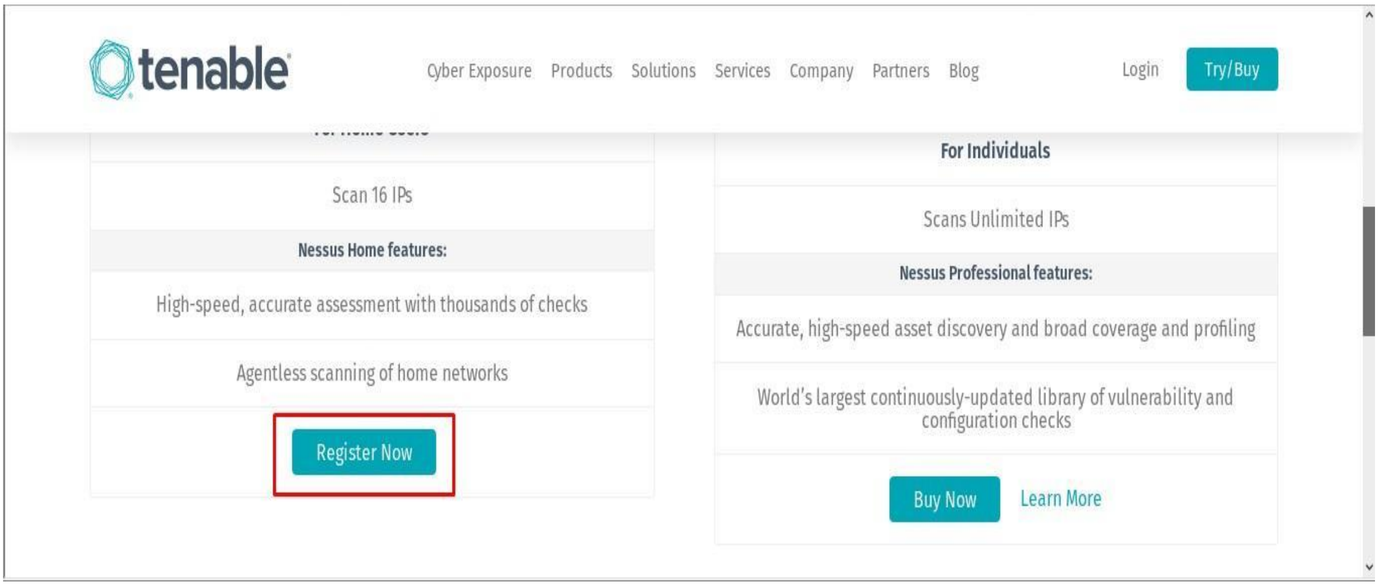
Part1: Download and Install Nessus Vulnerability Scanner

Step 1: Perform a simple google search to download Nessus Vulnerability Scanner or click on the following link

- https://www.tenable.com/products/nessus/activation-code
- Choose **Nessus Home** edition and click on register now.



Obtain an Activation Code



For Individuals

Scan 16 IPs

Nessus Home features:

High-speed, accurate assessment with thousands of checks

Agentless scanning of home networks

Scans Unlimited IPs

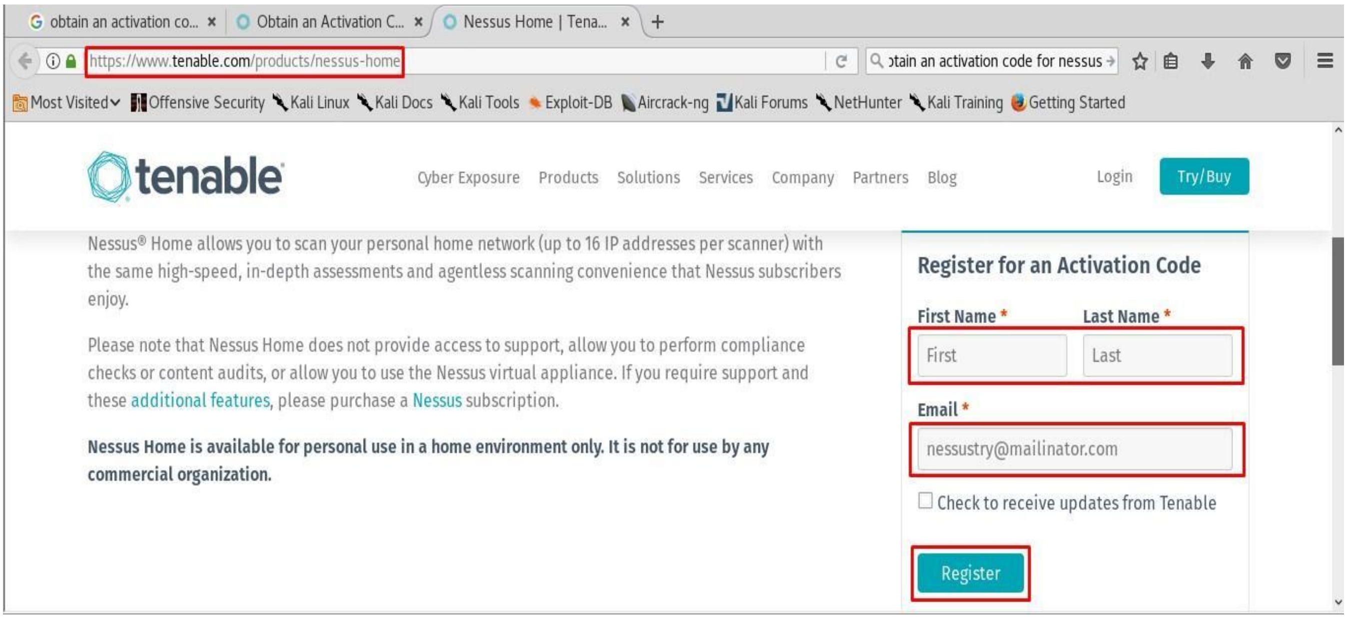
Nessus Professional features:

Accurate, high-speed asset discovery and broad coverage and profiling

World's largest continuously-updated library of vulnerability and configuration checks

Step 2: We will be redirected to the registration page, complete user registration and click **Register**.

- **Note: Provide a valid email address (you will receive Nessus Activation Code).**



Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these additional features, please purchase a Nessus subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

Register for an Activation Code

First Name * First

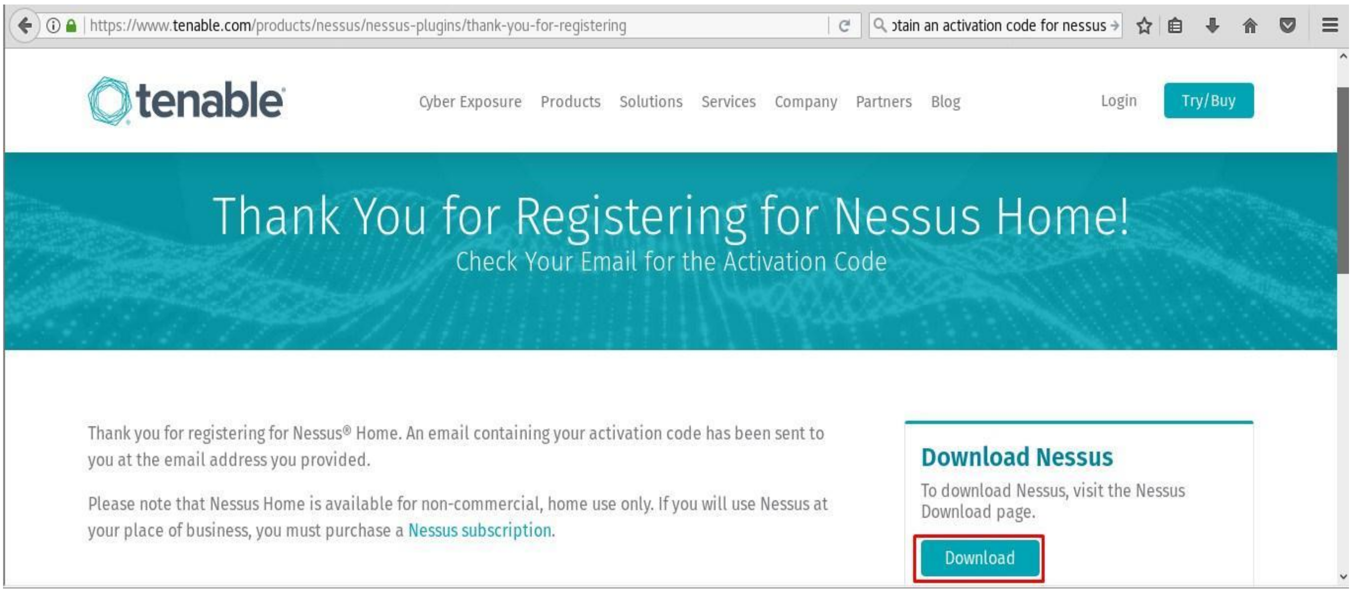
Last Name * Last

Email * nessustry@mailinator.com

☐ Check to receive updates from Tenable

Register

Step 3: After registration, click on download.


https://www.tenable.com/products/nessus/nessus-plugins/thank-you-for-registering
otain an activation code for nessus
tenable
Cyber Exposure
Products
Solutions
Services
Company
Partners
Blog
Login
Try/Buy

Thank You for Registering for Nessus Home!

Check Your Email for the Activation Code

Thank you for registering for Nessus® Home. An email containing your activation code has been sent to you at the email address you provided.

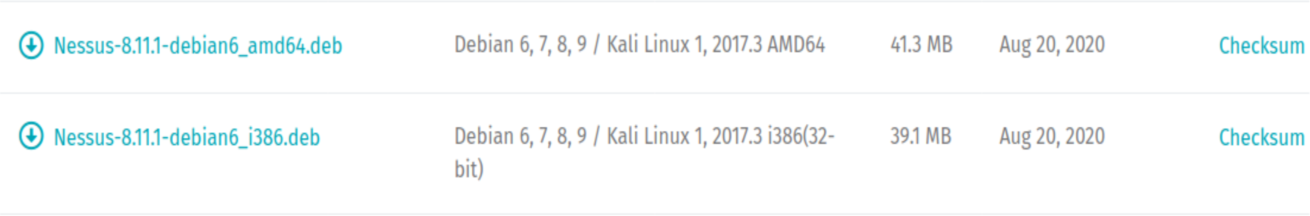
Please note that Nessus Home is available for non-commercial, home use only. If you will use Nessus at your place of business, you must purchase a Nessus subscription.

Download Nessus

To download Nessus, visit the Nessus Download page.

Download

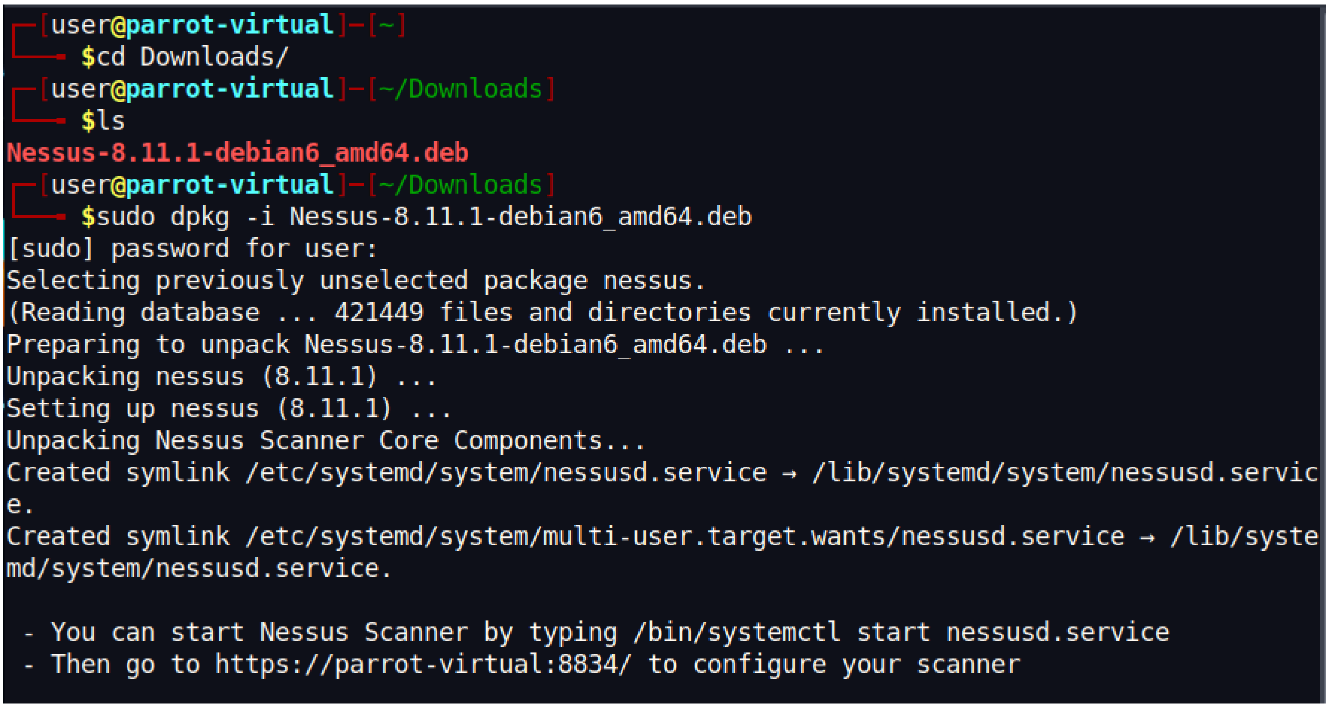
Step 4: Select Linux version **.deb package** (32-bit or 64-bit based on your machine compatibility). Click **Agree** to start the download.



Nessus-8.11.1-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	41.3 MB	Aug 20, 2020	Checksum
Nessus-8.11.1-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	39.1 MB	Aug 20, 2020	Checksum

Step 5: In the terminal, locate the **Downloads** directory and execute the following command.

- **dpkg -i <package name>**



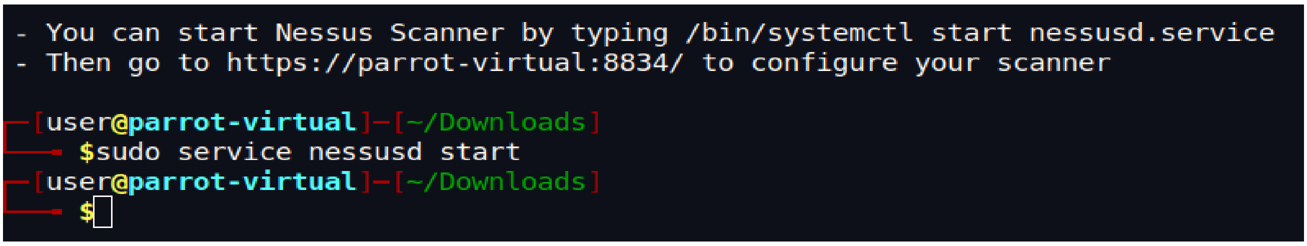
```
┌─[user@parrot-virtual]─[~]
└──╼ $cd Downloads/
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $ls
Nessus-8.11.1-debian6_amd64.deb
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $sudo dpkg -i Nessus-8.11.1-debian6_amd64.deb
[sudo] password for user:
Selecting previously unselected package nessus.
(Reading database ... 421449 files and directories currently installed.)
Preparing to unpack Nessus-8.11.1-debian6_amd64.deb ...
Unpacking nessus (8.11.1) ...
Setting up nessus (8.11.1) ...
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.servic
e.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/syste
md/system/nessusd.service.

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://parrot-virtual:8834/ to configure your scanner
```

Part 2: Nessus Configuration

Step 6: Execute the following command to start Nessus

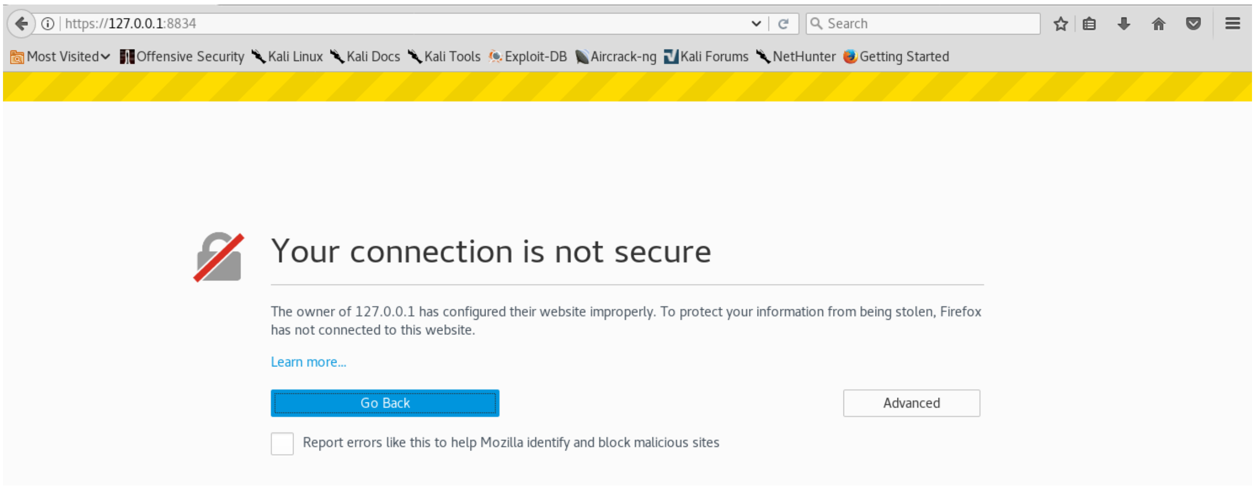
- **/etc/init.d/nessusd start**



```
 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://parrot-virtual:8834/ to configure your scanner

┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $sudo service nessusd start
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $
```

Step 7: On browser open https://127.0.0.1:8834/



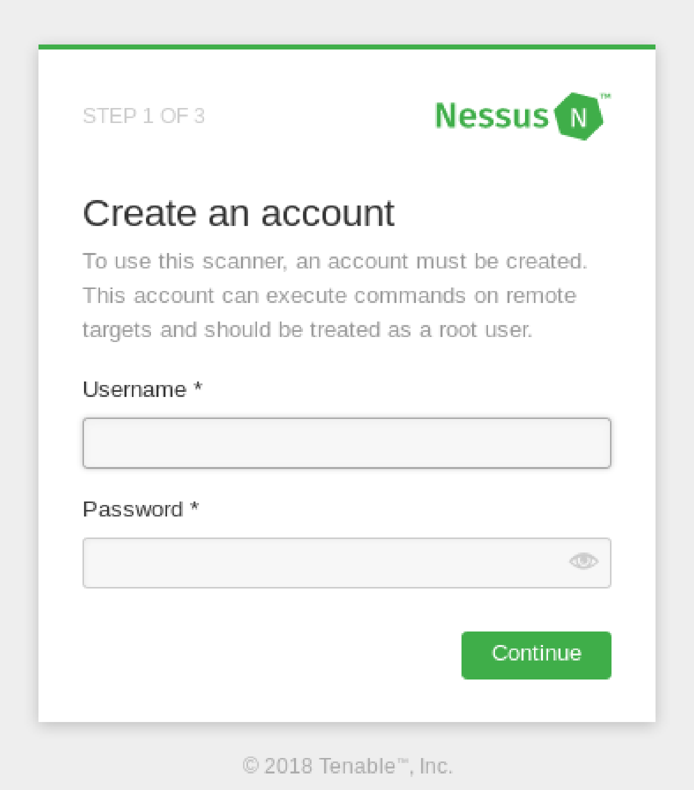
Your connection is not secure

The owner of 127.0.0.1 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

Step 8: Click on **Advanced** and **Add Exceptions** to display Nessus login screen. Provide Username and Password (remember these credentials to Login to Nessus in future).



STEP 1 OF 3

Create an account

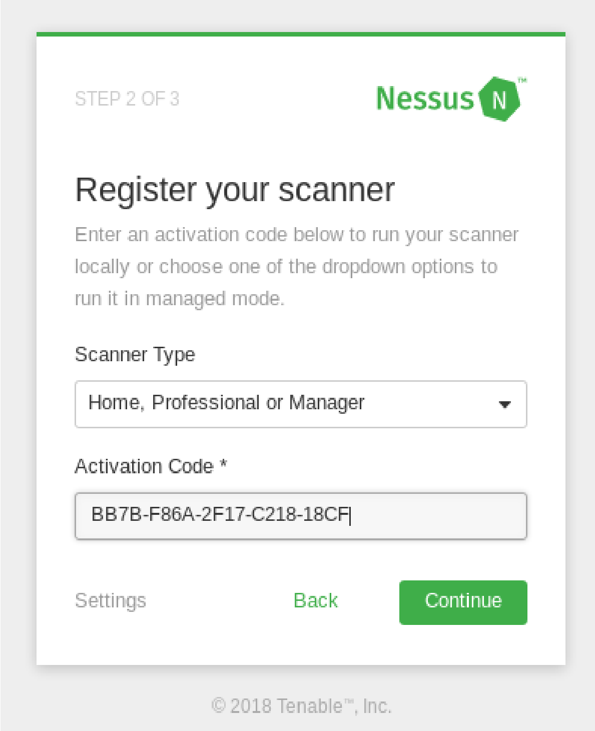
To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.

Username *

Password *

© 2018 Tenable™, Inc.

Step 9: Enter **Activation Code** when prompted. Initialization process starts and takes some time to complete.



STEP 2 OF 3

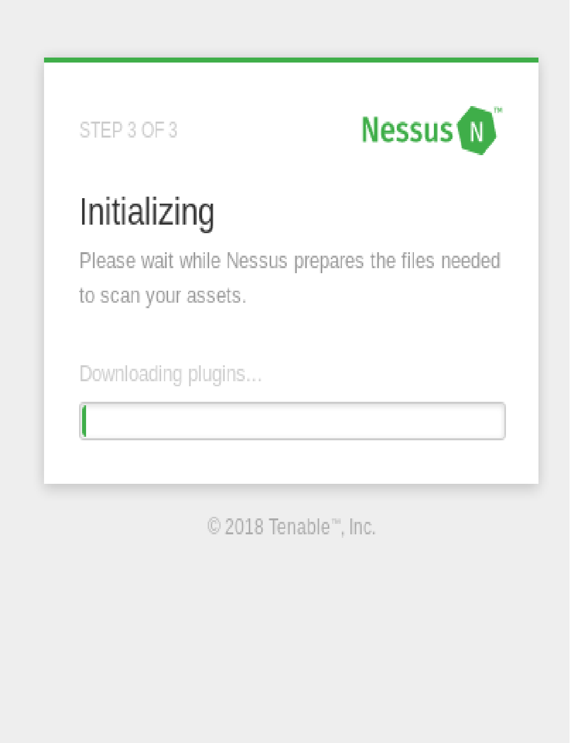
Register your scanner

Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.

Scanner Type: Home, Professional or Manager

Activation Code *: BB7B-F86A-2F17-C218-18CF

© 2018 Tenable™, Inc.



STEP 3 OF 3

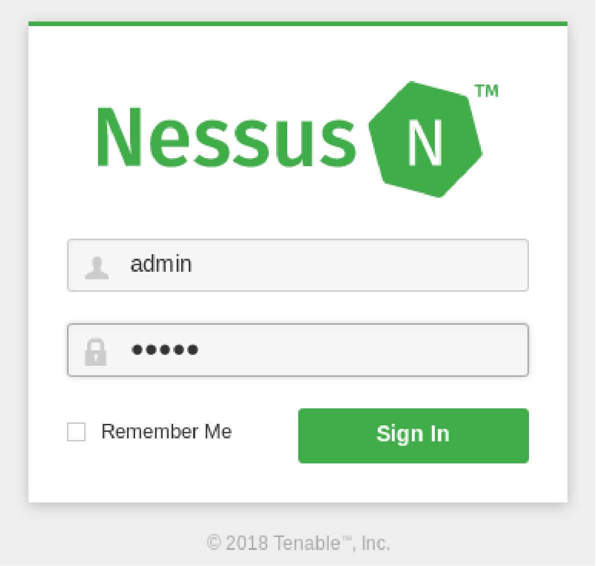
Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2018 Tenable™, Inc.

Step 10: Once registration is done. We can Login to Nessus (using your credentials as created before).

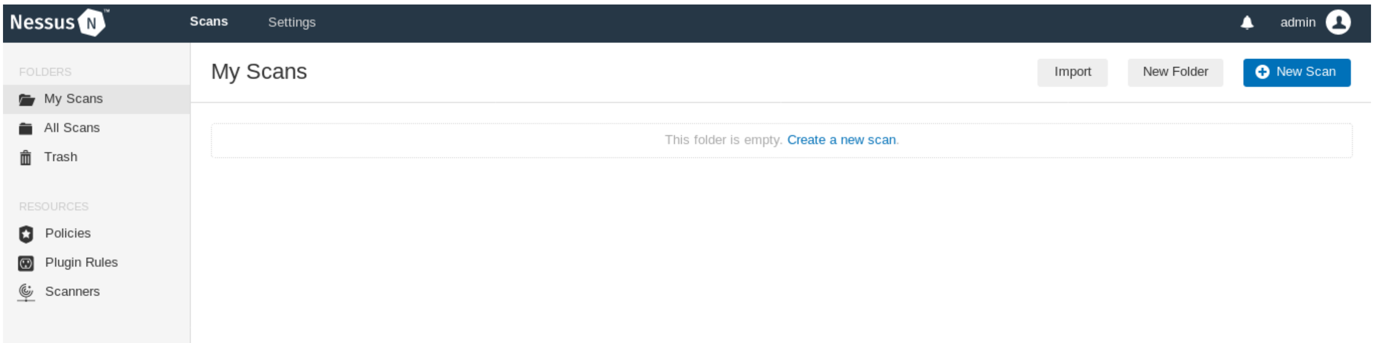


admin

●●●●●

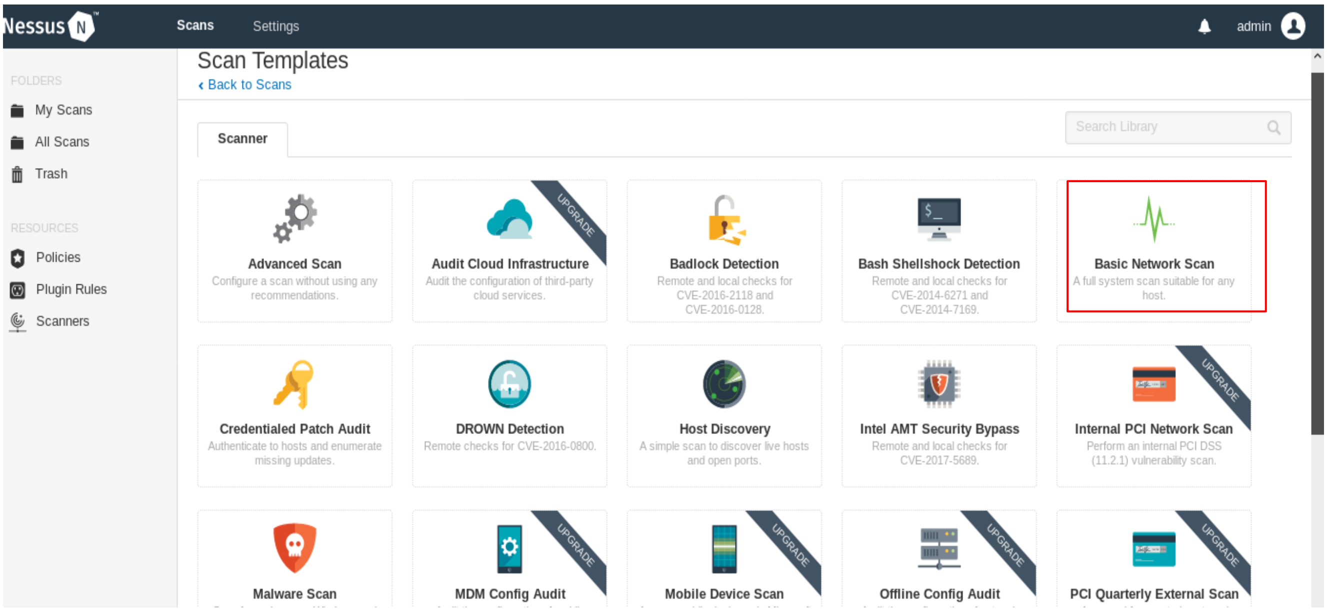
□ Remember Me

Step 11: To perform a vulnerability scan, click on **New Scan** on the top-right corner of the Nessus interface.



This folder is empty. Create a new scan.

Step 12: Select the type of scan that we are intended to perform on the target machine. In this case, let us choose **Basic Network Scan.**



Advanced Scan Configure a scan without using any recommendations.

Audit Cloud Infrastructure Audit the configuration of third-party cloud services.

Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan A full system scan suitable for any host.

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.

DROWN Detection Remote checks for CVE-2016-0800.

Host Discovery A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan

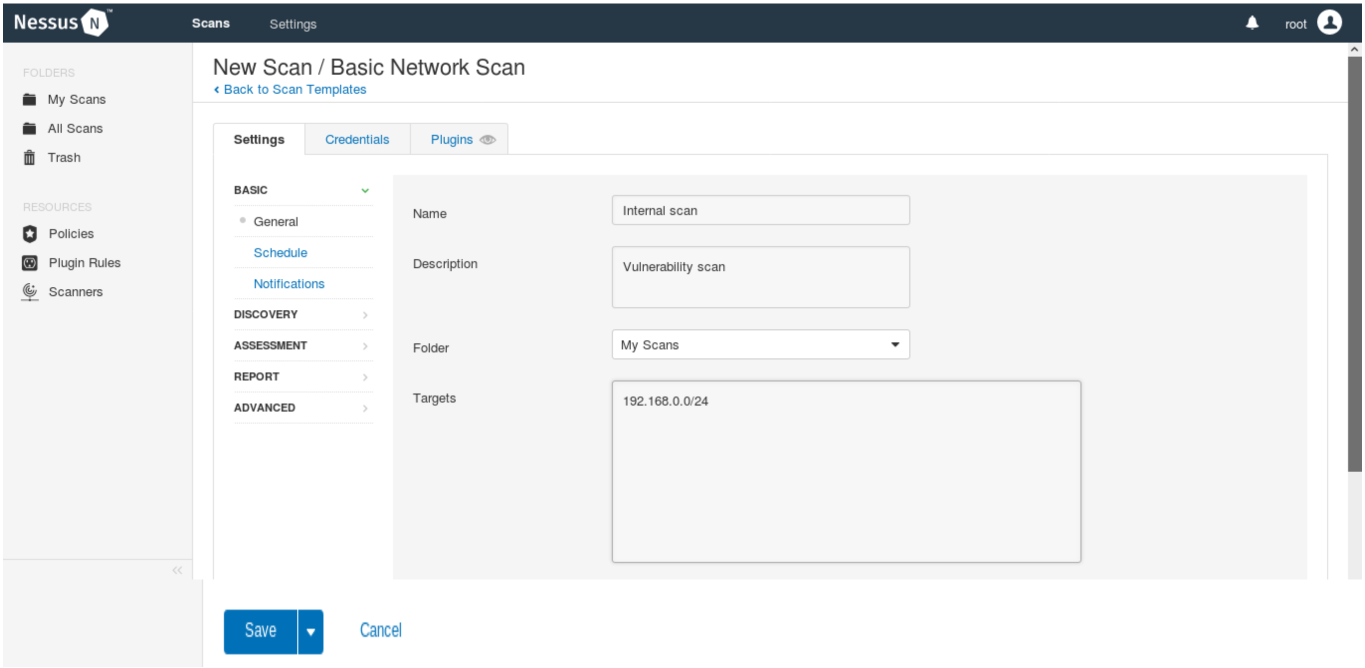
MDM Config Audit

Mobile Device Scan

Offline Config Audit

PCI Quarterly External Scan

Step 13: Provide the necessary details (Name of your scan, IP address of the target are mandatory) and save the profile.s



New Scan / Basic Network Scan

‹ Back to Scan Templates

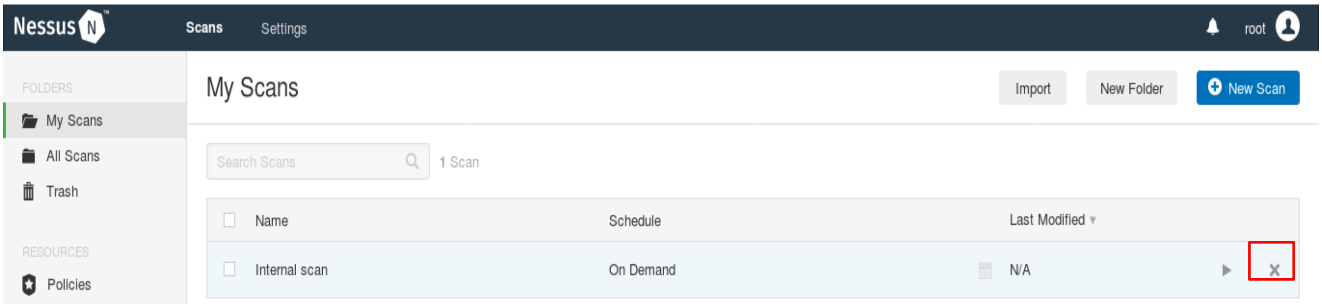
Name: Internal scan

Description: Vulnerability scan

Folder: My Scans

Targets: 192.168.0.0/24

Step 14: We can see that the scan name is listed under **My Scans** tab. Click on the play button to start the scan.

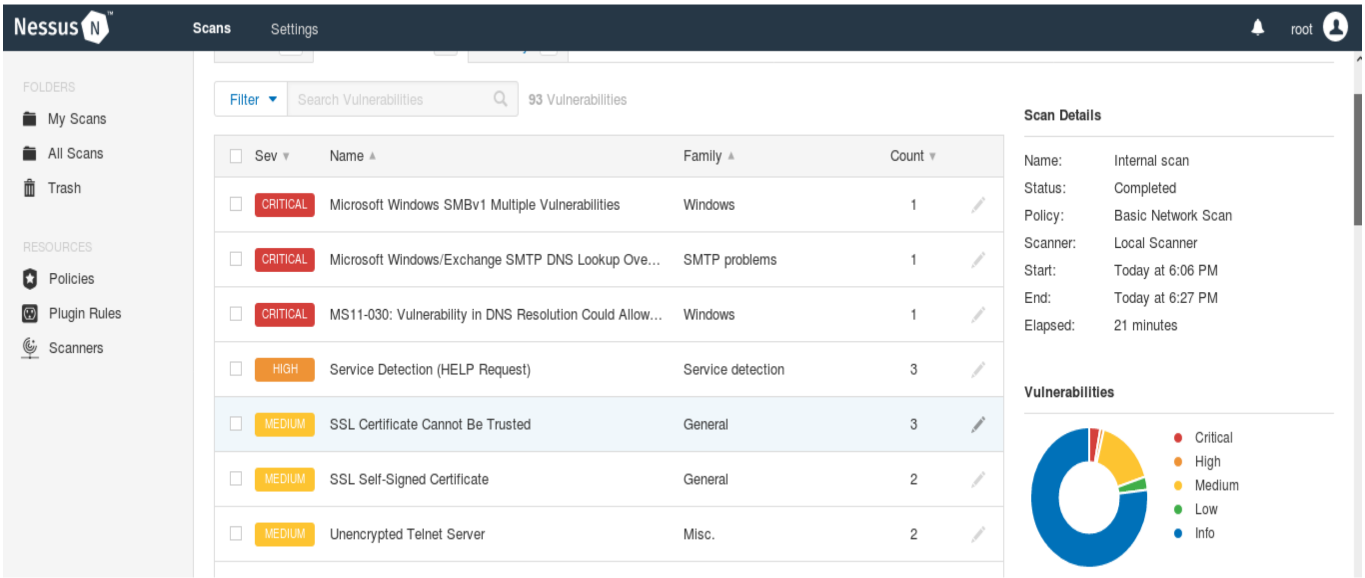


My Scans

1 Scan

Name	Schedule	Last Modified ▾
Internal scan	On Demand	N/A

Step 15: Click on the scan to view identified vulnerabilities



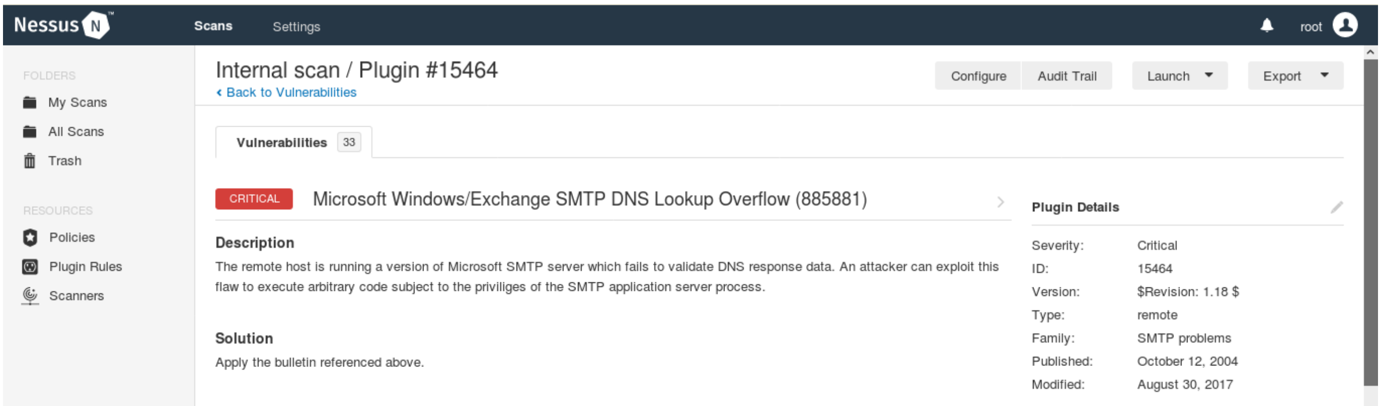
93 Vulnerabilities

Sev ▾	Name ▴	Family ▴	Count ▾
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1
CRITICAL	Microsoft Windows/Exchange SMTP DNS Lookup Ove…	SMTP problems	1
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow…	Windows	1
HIGH	Service Detection (HELP Request)	Service detection	3
MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	Unencrypted Telnet Server	Misc.	2

Scan Details

Name:	Internal scan
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Start:	Today at 6:06 PM
End:	Today at 6:27 PM
Elapsed:	21 minutes

Step 16: Click on those vulnerabilities for detailed information regarding the risk.



Internal scan / Plugin #15464

‹ Back to Vulnerabilities

CRITICAL Microsoft Windows/Exchange SMTP DNS Lookup Overflow (885881)

Description

The remote host is running a version of Microsoft SMTP server which fails to validate DNS response data. An attacker can exploit this flaw to execute arbitrary code subject to the priviliges of the SMTP application server process.

Solution

Apply the bulletin referenced above.

Plugin Details

Severity:	Critical
ID:	15464
Version:	$Revision: 1.18 $
Type:	remote
Family:	SMTP problems
Published:	October 12, 2004
Modified:	August 30, 2017

- To document the results, click on the **export** button located on the top right corner.

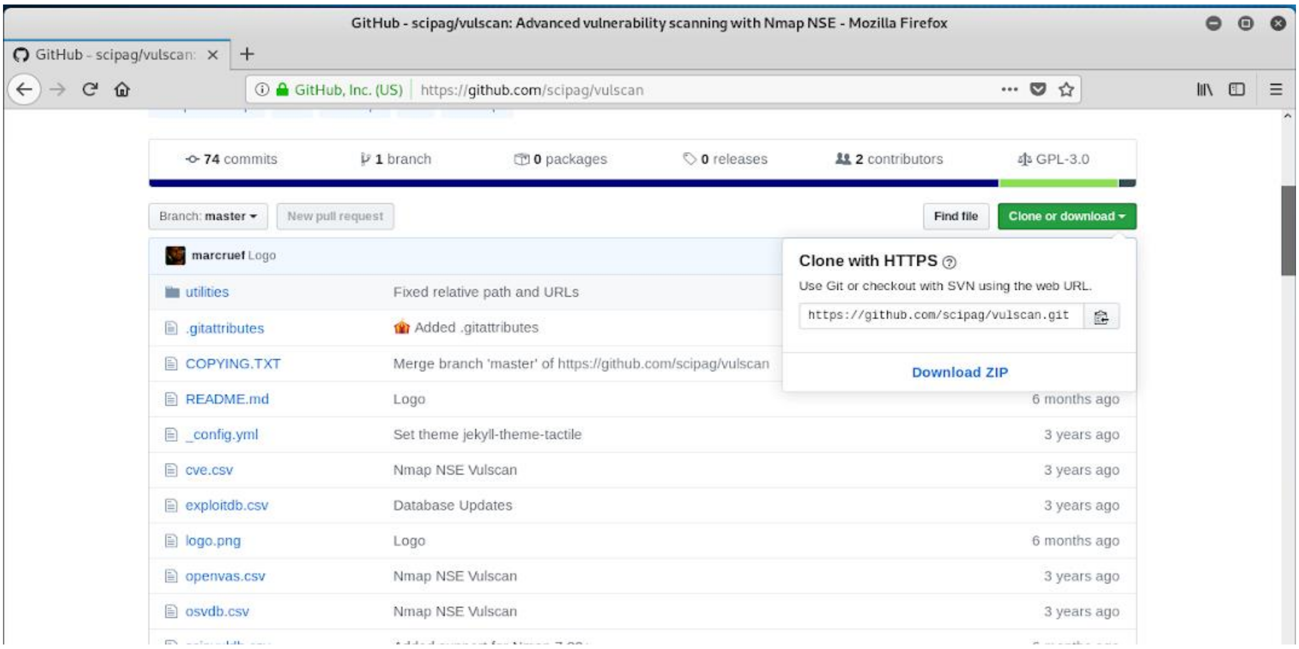
Practical 2: Performing vulnerability assessment using the Nmap-vulners.

Description: In this practical we will learn how to clone **nmap-vulners** and **vulscan** scripts from GitHub and perform vulnerability scanning using **nmap** tool with the cloned scripts nmap-vulners and vulscan.

Prerequisites: git tool should be installed to clone tools from GitHub.

Step 1: This is one type of vulnerability identification scanning with nmap scripts. In this scanning we download vulnerability data from online and add it to nmap tool to identify vulnerabilities on target system. This will only give you possible vulnerability details based on the version of software it identifies in the scanning.

- Let’s get into the practical, clone the vulnerability data and related nmap scripts from the GitHub to your attacker machine by executing below steps.
- **git clone https://github.com/scipag/vulscan.git**



GitHub - scipag/vulscan: Advanced vulnerability scanning with Nmap NSE - Mozilla Firefox

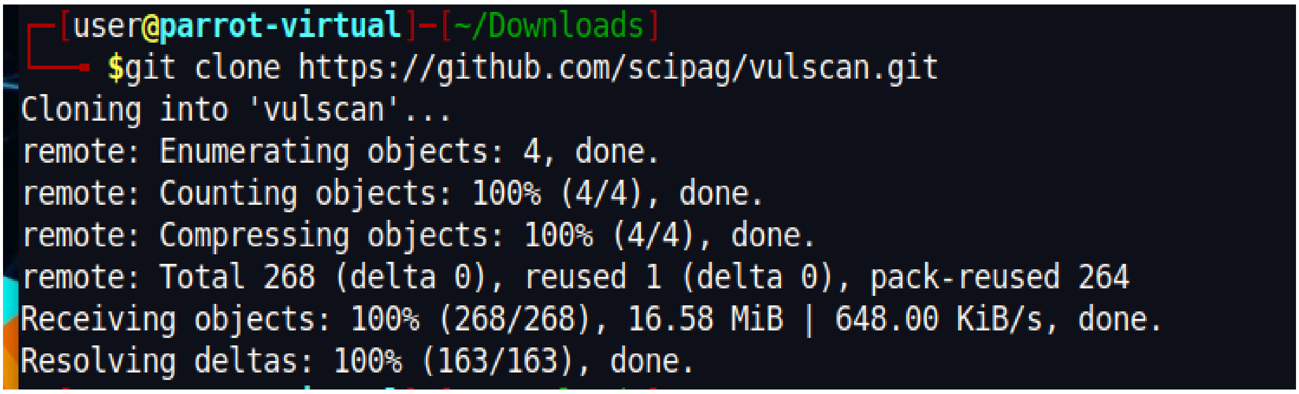
GitHub, Inc. (US) https://github.com/scipag/vulscan

74 commits · 1 branch · 0 packages · 0 releases · 2 contributors · GPL-3.0

Branch: master · New pull request · Find file · Clone or download

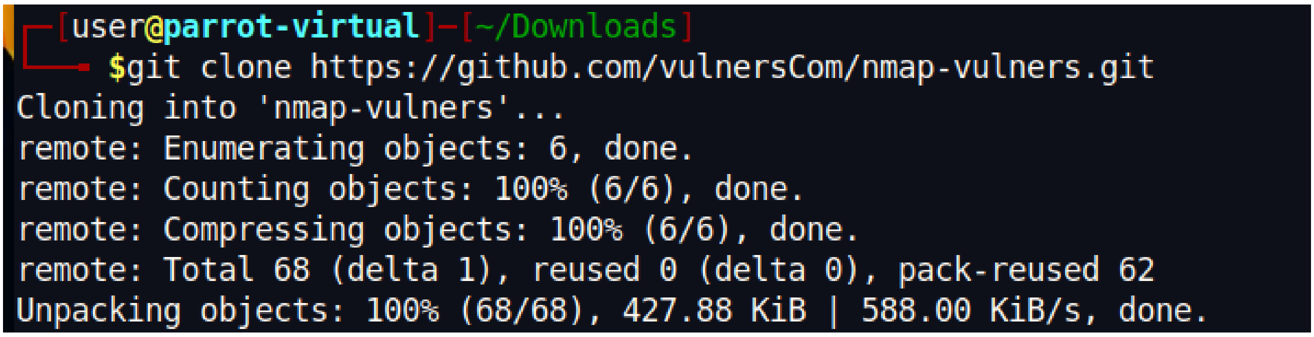
Clone with HTTPS
Use Git or checkout with SVN using the web URL.
https://github.com/scipag/vulscan.git
Download ZIP

marcruef Logo		
utilities	Fixed relative path and URLs	
.gitattributes	Added .gitattributes	
COPYING.TXT	Merge branch 'master' of https://github.com/scipag/vulscan	
README.md	Logo	6 months ago
_config.yml	Set theme jekyll-theme-tactile	3 years ago
cve.csv	Nmap NSE Vulscan	3 years ago
exploitdb.csv	Database Updates	3 years ago
logo.png	Logo	6 months ago
openvas.csv	Nmap NSE Vulscan	3 years ago
osvdb.csv	Nmap NSE Vulscan	3 years ago



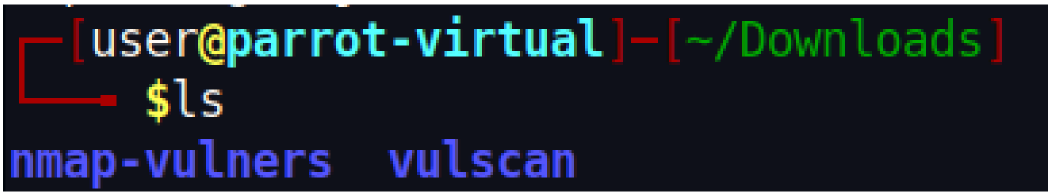
```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $git clone https://github.com/scipag/vulscan.git
Cloning into 'vulscan'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 268 (delta 0), reused 1 (delta 0), pack-reused 264
Receiving objects: 100% (268/268), 16.58 MiB | 648.00 KiB/s, done.
Resolving deltas: 100% (163/163), done.
```

- **git clone https://github.com/vulnersCom/nmap-vulners.git**



```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $git clone https://github.com/vulnersCom/nmap-vulners.git
Cloning into 'nmap-vulners'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 68 (delta 1), reused 0 (delta 0), pack-reused 62
Unpacking objects: 100% (68/68), 427.88 KiB | 588.00 KiB/s, done.
```

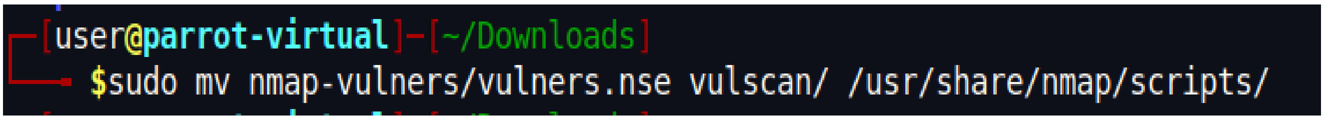
Step 2: we can see two directories with names vulscan and nmap-vulners created in your system.



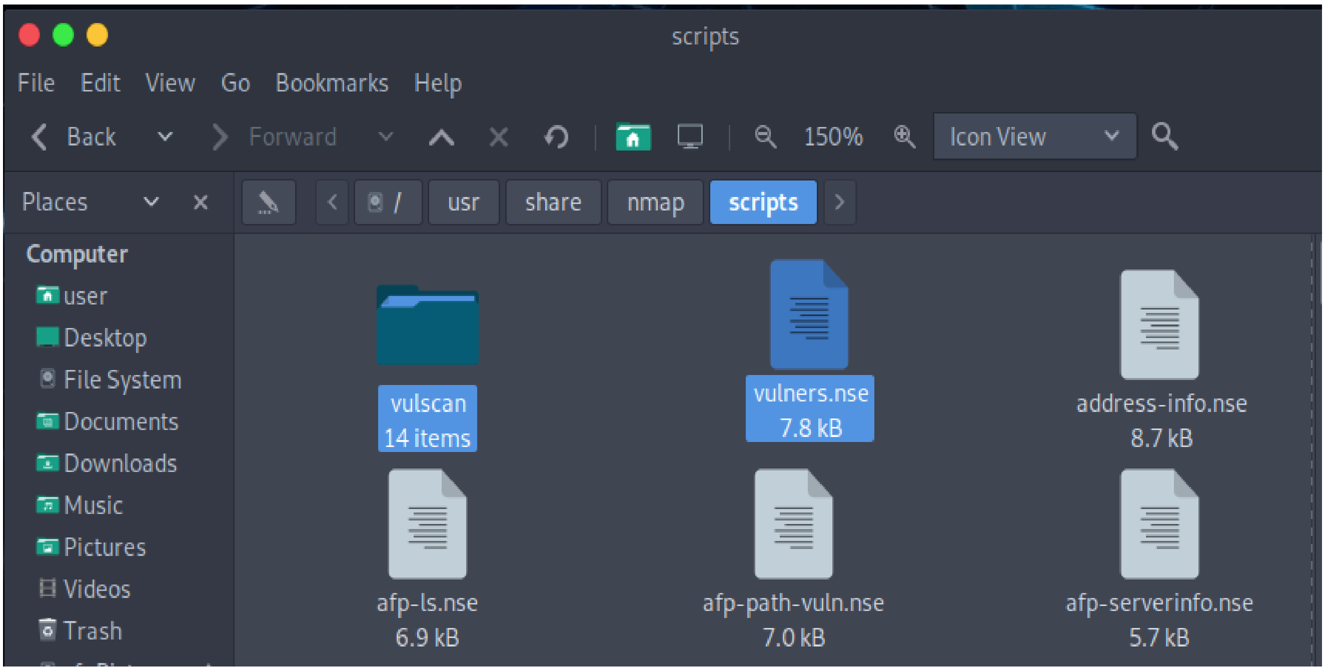
```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $ls
nmap-vulners  vulscan
```

Step 3: Copy vulners.nse in nmap-vulners directory and complete vulscan directory to **/usr/share/nmap/scripts/** location, because while performing nmap script scan nmap by default it will take scripts from the above path, so to make our work simple we move the downloaded scripts to that path. Execute the below command on terminal to move files.

- **mv nmap-vulners/vulners.nse vulscan/ /usr/share/nmap/scripts/**

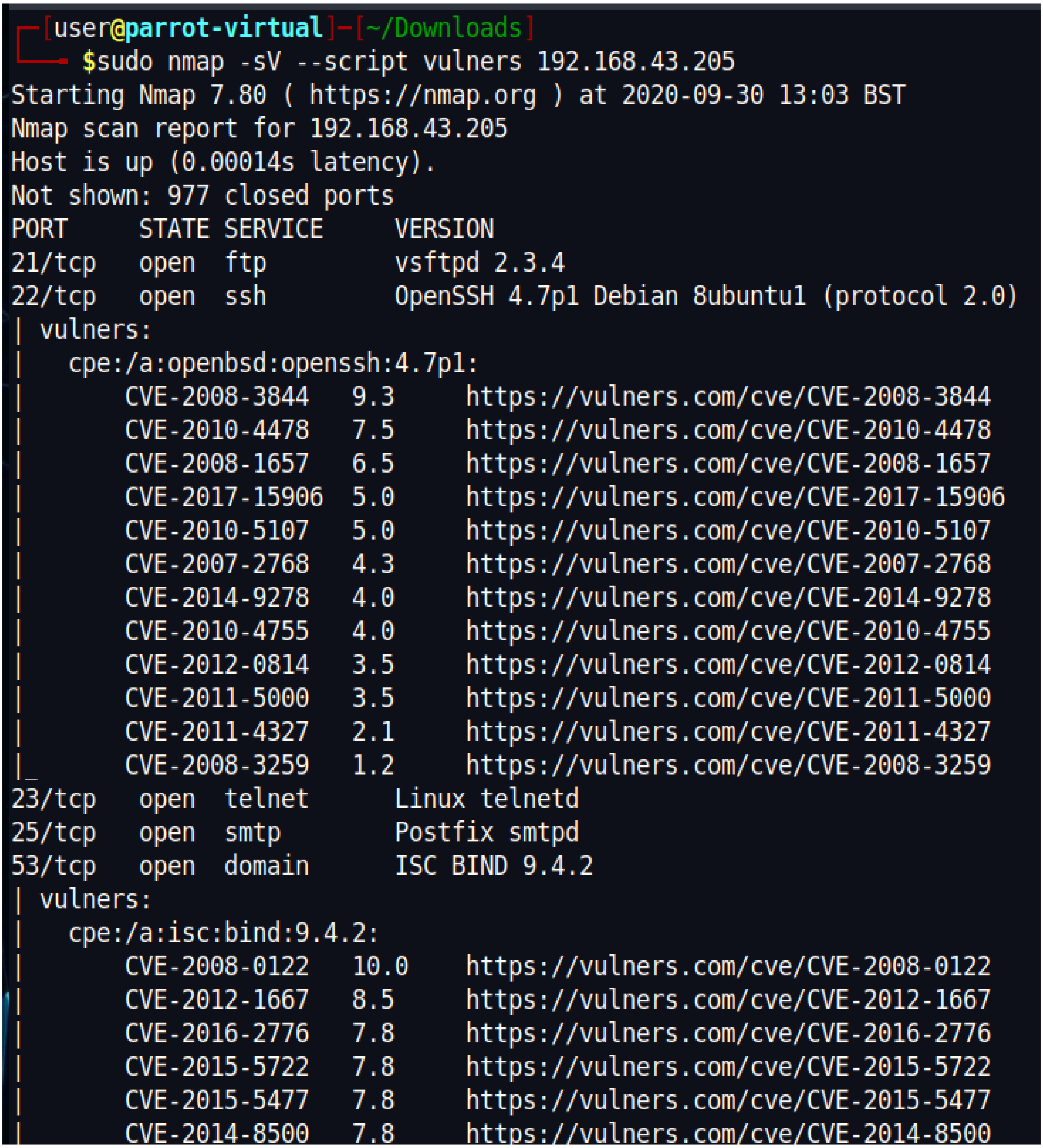


```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $sudo mv nmap-vulners/vulners.nse vulscan/ /usr/share/nmap/scripts/
```



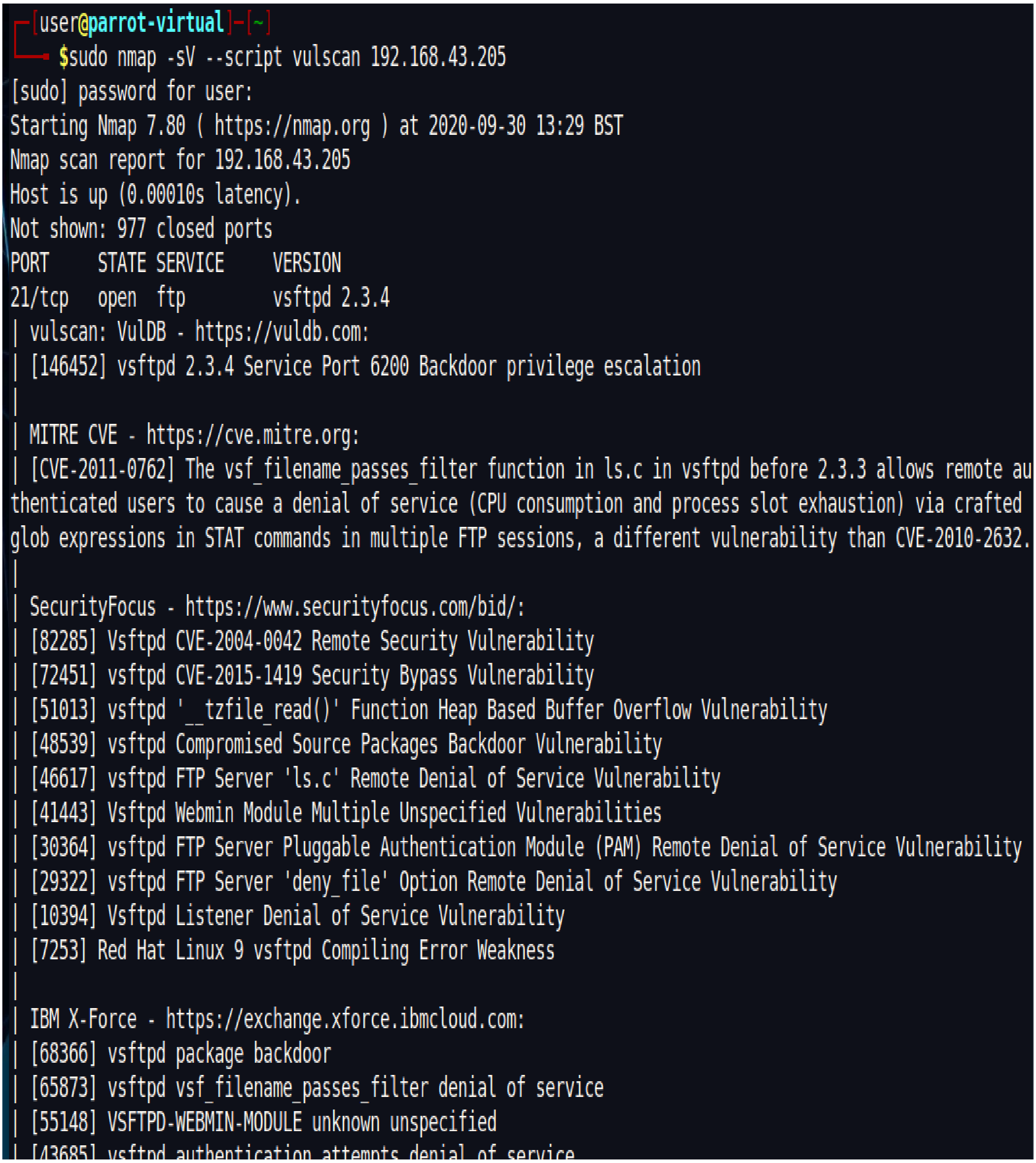
Step 4: To perform vulnerability scanning by using the scripts, execute below steps.

- **nmap -sV --script vulners <targetIP>**



```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $sudo nmap -sV --script vulners 192.168.43.205
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-30 13:03 BST
Nmap scan report for 192.168.43.205
Host is up (0.00014s 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)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       CVE-2008-3844   9.3     https://vulners.com/cve/CVE-2008-3844
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       CVE-2007-2768   4.3     https://vulners.com/cve/CVE-2007-2768
|       CVE-2014-9278   4.0     https://vulners.com/cve/CVE-2014-9278
|       CVE-2010-4755   4.0     https://vulners.com/cve/CVE-2010-4755
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
|_      CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       CVE-2008-0122   10.0    https://vulners.com/cve/CVE-2008-0122
|       CVE-2012-1667   8.5     https://vulners.com/cve/CVE-2012-1667
|       CVE-2016-2776   7.8     https://vulners.com/cve/CVE-2016-2776
|       CVE-2015-5722   7.8     https://vulners.com/cve/CVE-2015-5722
|       CVE-2015-5477   7.8     https://vulners.com/cve/CVE-2015-5477
|       CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
```

- **nmap -sV --script vulscan <targetIP>**



```
┌─[user@parrot-virtual]─[~]
└──╼ $sudo nmap -sV --script vulscan 192.168.43.205
[sudo] password for user:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-30 13:29 BST
Nmap scan report for 192.168.43.205
Host is up (0.00010s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulscan: VulDB - https://vuldb.com:
| [146452] vsftpd 2.3.4 Service Port 6200 Backdoor privilege escalation
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote au
thenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted
glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [82285] Vsftpd CVE-2004-0042 Remote Security Vulnerability
| [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability
| [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
| [48539] vsftpd Compromised Source Packages Backdoor Vulnerability
| [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability
| [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities
| [30364] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability
| [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability
| [10394] Vsftpd Listener Denial of Service Vulnerability
| [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [68366] vsftpd package backdoor
| [65873] vsftpd vsf_filename_passes_filter denial of service
| [55148] VSFTPD-WEBMIN-MODULE unknown unspecified
| [43685] vsftpd authentication attempts denial of service
```

- These scans will give vulnerability details, CVE details, reference link and vulnerability severity rating etc.