Отчет

# Задание:

Выбрать подсеть с маской 24 и просканировать ее по tcp по всем портам (65535) с детектированием версий сервисов и ОС. Желательно использовать скрипты NSE. Можно взять четыре любых октета в глобальной сети.

# Выполнение:

1. **Произведено сканирование подсети 45.33.32.0/24 (подсеть тестового узла разработчиков nmap) командой nmap –sV –n 45.33.32.0/24;**

Обнаружен один хост с открытыми tcp-портами и возможностью определения служб.

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.0068s latency).

Not shown: 993 filtered ports

PORT STATE SERVICE VERSION

22/tcp open tcpwrapped

135/tcp closed msrpc

256/tcp closed fw1-secureremote

443/tcp closed https

445/tcp closed microsoft-ds

8080/tcp closed http-proxy

8888/tcp closed sun-answerbook

1. **Произведено сканирование локальной сети с хостом, с образом Metasploitable.**

Обнаружен один хост с открытыми tcp-портами и возможностью определения служб.

Nmap scan report for 192.168.119.131

Host is up (0.014s latency).

Not shown: 975 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?

513/tcp open login?

514/tcp open shell?

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ccproxy-ftp?

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)

6004/tcp filtered X11:4

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

10180/tcp filtered unknown

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.119.132

Host is up (0.030s latency).

All 1000 scanned ports on 192.168.119.132 are filtered

1. **Проведено сканирование узла с использованием скрипта vulners.nse (nmap -sV 192.168.119.131 --script=/usr/share/nmap/scripts/vulners.nse)**

Выявлены потенциальные уязвимости:

Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-18 02:15 EDT

Nmap scan report for 192.168.119.131

Host is up (0.0095s latency).

Not shown: 977 filtered 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-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478

| CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478

| CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778

| CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778

| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906

| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906

| CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708

| CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708

| 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-2010-4755 4.0 https://vulners.com/cve/CVE-2010-4755

|\_ CVE-2008-5161 2.6 https://vulners.com/cve/CVE-2008-5161

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)

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

| vulners:

| cpe:/a:apache:http\_server:2.2.8:

| CVE-2010-0425 10.0 https://vulners.com/cve/CVE-2010-0425

| CVE-2010-0425 10.0 https://vulners.com/cve/CVE-2010-0425

| CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192

| CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2013-2249 7.5 https://vulners.com/cve/CVE-2013-2249

| CVE-2013-2249 7.5 https://vulners.com/cve/CVE-2013-2249

| CVE-2009-1891 7.1 https://vulners.com/cve/CVE-2009-1891

| CVE-2009-1891 7.1 https://vulners.com/cve/CVE-2009-1891

| CVE-2009-1890 7.1 https://vulners.com/cve/CVE-2009-1890

| CVE-2009-1890 7.1 https://vulners.com/cve/CVE-2009-1890

| CVE-2012-0883 6.9 https://vulners.com/cve/CVE-2012-0883

| CVE-2012-0883 6.9 https://vulners.com/cve/CVE-2012-0883

| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

| CVE-2013-1862 5.1 https://vulners.com/cve/CVE-2013-1862

| CVE-2013-1862 5.1 https://vulners.com/cve/CVE-2013-1862

| CVE-2014-0231 5.0 https://vulners.com/cve/CVE-2014-0231

| CVE-2014-0231 5.0 https://vulners.com/cve/CVE-2014-0231

| CVE-2014-0098 5.0 https://vulners.com/cve/CVE-2014-0098

| CVE-2014-0098 5.0 https://vulners.com/cve/CVE-2014-0098

| CVE-2013-6438 5.0 https://vulners.com/cve/CVE-2013-6438

| CVE-2013-6438 5.0 https://vulners.com/cve/CVE-2013-6438

| CVE-2011-3368 5.0 https://vulners.com/cve/CVE-2011-3368

| CVE-2011-3368 5.0 https://vulners.com/cve/CVE-2011-3368

| CVE-2010-1452 5.0 https://vulners.com/cve/CVE-2010-1452

| CVE-2010-0408 5.0 https://vulners.com/cve/CVE-2010-0408

| CVE-2010-0408 5.0 https://vulners.com/cve/CVE-2010-0408

| CVE-2009-2699 5.0 https://vulners.com/cve/CVE-2009-2699

| CVE-2009-2699 5.0 https://vulners.com/cve/CVE-2009-2699

| CVE-2008-2364 5.0 https://vulners.com/cve/CVE-2008-2364

| CVE-2007-6750 5.0 https://vulners.com/cve/CVE-2007-6750

| CVE-2007-6750 5.0 https://vulners.com/cve/CVE-2007-6750

| CVE-2009-1195 4.9 https://vulners.com/cve/CVE-2009-1195

| CVE-2012-0031 4.6 https://vulners.com/cve/CVE-2012-0031

| CVE-2012-0031 4.6 https://vulners.com/cve/CVE-2012-0031

| CVE-2011-3607 4.4 https://vulners.com/cve/CVE-2011-3607

| CVE-2011-3607 4.4 https://vulners.com/cve/CVE-2011-3607

| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

| CVE-2013-1896 4.3 https://vulners.com/cve/CVE-2013-1896

| CVE-2013-1896 4.3 https://vulners.com/cve/CVE-2013-1896

| CVE-2012-4558 4.3 https://vulners.com/cve/CVE-2012-4558

| CVE-2012-4558 4.3 https://vulners.com/cve/CVE-2012-4558

| CVE-2012-3499 4.3 https://vulners.com/cve/CVE-2012-3499

| CVE-2012-3499 4.3 https://vulners.com/cve/CVE-2012-3499

| CVE-2012-0053 4.3 https://vulners.com/cve/CVE-2012-0053

| CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317

| CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317

| CVE-2011-3639 4.3 https://vulners.com/cve/CVE-2011-3639

| CVE-2011-3639 4.3 https://vulners.com/cve/CVE-2011-3639

| CVE-2011-3348 4.3 https://vulners.com/cve/CVE-2011-3348

| CVE-2011-3348 4.3 https://vulners.com/cve/CVE-2011-3348

| CVE-2011-0419 4.3 https://vulners.com/cve/CVE-2011-0419

| CVE-2011-0419 4.3 https://vulners.com/cve/CVE-2011-0419

| CVE-2010-0434 4.3 https://vulners.com/cve/CVE-2010-0434

| CVE-2008-2939 4.3 https://vulners.com/cve/CVE-2008-2939

| CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

| CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

| CVE-2012-2687 2.6 https://vulners.com/cve/CVE-2012-2687

| CVE-2012-2687 2.6 https://vulners.com/cve/CVE-2012-2687

| CVE-2011-4415 1.2 https://vulners.com/cve/CVE-2011-4415

|\_ CVE-2011-4415 1.2 https://vulners.com/cve/CVE-2011-4415

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 tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

| vulners:

| cpe:/a:proftpd:proftpd:1.3.1:

| CVE-2011-4130 9.0 https://vulners.com/cve/CVE-2011-4130

| CVE-2011-4130 9.0 https://vulners.com/cve/CVE-2011-4130

| CVE-2010-3867 7.1 https://vulners.com/cve/CVE-2010-3867

| CVE-2010-3867 7.1 https://vulners.com/cve/CVE-2010-3867

| CVE-2010-4652 6.8 https://vulners.com/cve/CVE-2010-4652

| CVE-2010-4652 6.8 https://vulners.com/cve/CVE-2010-4652

| CVE-2009-0543 6.8 https://vulners.com/cve/CVE-2009-0543

| CVE-2009-0543 6.8 https://vulners.com/cve/CVE-2009-0543

| CVE-2009-3639 5.8 https://vulners.com/cve/CVE-2009-3639

| CVE-2009-3639 5.8 https://vulners.com/cve/CVE-2009-3639

| CVE-2019-19272 5.0 https://vulners.com/cve/CVE-2019-19272

| CVE-2019-19272 5.0 https://vulners.com/cve/CVE-2019-19272

| CVE-2019-19271 5.0 https://vulners.com/cve/CVE-2019-19271

| CVE-2019-19271 5.0 https://vulners.com/cve/CVE-2019-19271

| CVE-2011-1137 5.0 https://vulners.com/cve/CVE-2011-1137

| CVE-2011-1137 5.0 https://vulners.com/cve/CVE-2011-1137

| CVE-2008-7265 4.0 https://vulners.com/cve/CVE-2008-7265

| CVE-2008-7265 4.0 https://vulners.com/cve/CVE-2008-7265

| CVE-2012-6095 1.2 https://vulners.com/cve/CVE-2012-6095

|\_ CVE-2012-6095 1.2 https://vulners.com/cve/CVE-2012-6095

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| vulners:

| cpe:/a:postgresql:postgresql:8.3:

| CVE-2016-7048 9.3 https://vulners.com/cve/CVE-2016-7048

| CVE-2016-7048 9.3 https://vulners.com/cve/CVE-2016-7048

| CVE-2019-10211 7.5 https://vulners.com/cve/CVE-2019-10211

| CVE-2019-10211 7.5 https://vulners.com/cve/CVE-2019-10211

| CVE-2015-3166 7.5 https://vulners.com/cve/CVE-2015-3166

| CVE-2015-3166 7.5 https://vulners.com/cve/CVE-2015-3166

| CVE-2015-0244 7.5 https://vulners.com/cve/CVE-2015-0244

| CVE-2015-0244 7.5 https://vulners.com/cve/CVE-2015-0244

| CVE-2017-14798 6.9 https://vulners.com/cve/CVE-2017-14798

| CVE-2017-14798 6.9 https://vulners.com/cve/CVE-2017-14798

| CVE-2015-0243 6.5 https://vulners.com/cve/CVE-2015-0243

| CVE-2015-0243 6.5 https://vulners.com/cve/CVE-2015-0243

| CVE-2015-0242 6.5 https://vulners.com/cve/CVE-2015-0242

| CVE-2015-0242 6.5 https://vulners.com/cve/CVE-2015-0242

| CVE-2015-0241 6.5 https://vulners.com/cve/CVE-2015-0241

| CVE-2015-0241 6.5 https://vulners.com/cve/CVE-2015-0241

| CVE-2018-1115 6.4 https://vulners.com/cve/CVE-2018-1115

| CVE-2018-1115 6.4 https://vulners.com/cve/CVE-2018-1115

| CVE-2015-3167 5.0 https://vulners.com/cve/CVE-2015-3167

| CVE-2015-3167 5.0 https://vulners.com/cve/CVE-2015-3167

| CVE-2012-2143 4.3 https://vulners.com/cve/CVE-2012-2143

| CVE-2014-8161 4.0 https://vulners.com/cve/CVE-2014-8161

| CVE-2014-8161 4.0 https://vulners.com/cve/CVE-2014-8161

| CVE-2010-0733 3.5 https://vulners.com/cve/CVE-2010-0733

| CVE-2010-0733 3.5 https://vulners.com/cve/CVE-2010-0733

| CVE-2019-10210 1.9 https://vulners.com/cve/CVE-2019-10210

|\_ CVE-2019-10210 1.9 https://vulners.com/cve/CVE-2019-10210

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

|\_http-server-header: Apache-Coyote/1.1

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel