**PORT SCANNER USING RASBPERRY PI**

Hackathon :

Team Members:

Uma Rao

Swathi Panneer Selvam

Ekansh Grover

Govind Aswin

Muni Vijaya Sai Kamisetty

Raspberrypi as a wifi acess point:



**Configuring the wireless interface**

root@raspberrypi:~/Desktop# /etc/init.d/networking restart

[....] Running /etc/init.d/networking restart is deprecated because it may not r[warnble some interfaces ... (warning).

[....] Reconfiguring network interfaces...wpa\_supplicant: /sbin/wpa\_supplicant daemon failed to start

run-parts: /etc/network/if-pre-up.d/wpasupplicant exited with return code 1

RTNETLINK answers: Network is unreachable

Failed to bring up wlan0.

wpa\_supplicant: /sbin/wpa\_supplicant daemon failed to start

run-parts: /etc/network/if-pre-up.d/wpasupplicant exited with return code 1

ifup: interface eth0 already configured

done.

**Configuring DHCP server on Rasbperry Pi:**

root@raspberrypi:~/Desktop# service isc-dhcp-server start

[ ok ] Starting ISC DHCP server: dhcpd.

**Configuring Rasbperry pi as wireless Access point:**

root@raspberrypi:~/Desktop# service hostapd start

[ ok ] Starting advanced IEEE 802.11 management: hostapd.

**Created the rasppy.py script which displays all the vulnerable ports on the connected devices:**

root@raspberrypi:~/Desktop# python3 rasppy.py

 /nmap.org ) at 2015-11-14 22:36 UTC\nNmap scan report for 192.168.42.1\nHost is up (0.00014s latency).\nAll 1000 scanned ports on 192.168.42.1 are closed\n\nNmap done: 1 IP address (1 host up) scanned in 1.07 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.19 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.11 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.07 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.14 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.17 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.14 seconds\n'

 **/nmap.org ) at 2015-11-14 22:36 UTC\nNmap scan report for 192.168.42.11\nHost is up (0.0041s latency).\nNot shown: 995 filtered ports\nPORT STATE SERVICE\n135/tcp open msrpc\n139/tcp open netbios-ssn\n445/tcp open microsoft-ds\n5357/tcp open wsdapi\n49155/tcp open unknown\nMAC Address: 84:A6:C8:BC:05:43 (Intel Corporate)\n\nNmap done: 1 IP address (1 host up) scanned in 5.05 seconds\n'**

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.10 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.17 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.15 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.07 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.10 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.14 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.19 seconds\n'

 /nmap.org ) at 2015-11-14 22:36 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.19 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.15 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.23 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.11 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.11 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.14 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.17 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.08 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.18 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.12 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.12 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.07 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.14 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.16 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.08 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.10 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.16 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.22 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.12 seconds\n'

 /nmap.org ) at 2015-11-14 22:37 UTC\nNote: Host seems down. If it is really up, but blocking our ping probes, try -Pn\nNmap done: 1 IP address (0 hosts up) scanned in 1.10 seconds\n'

**Result:**

Vulnerable ports found at 192.168.42.11. The following ports are found at 192.168.42.11 :

**n135/tcp open**

**msrpc\n139/tcp open**

**netbios-ssn\n445/tcp open**

**microsoft-ds\n5357/tcp open**

**wsdapi\n49155**