**Internal & External Vulnerability Scanning**

**External**

**The router is the gateway between devices and the internet, so it is imperative to harden its security**

**Shodan**

* Google of IoT
* Continually scans the internet and adds vulnerable devices to their database

A search for something like ‘NetGear’ will bring up all the NetGear devices on the database

It will show what ports that are open on the device

You DO NOT want your router admin interface to be accessible via the internet

* If it is necessary to access it then it must be hardened in a way that you must VPN into your network to access it or only be bale to access it locally

Searching for ‘default password’ searches for devices that respond to that string

* Meaning the device has a default user and password displayed to everyone on the internet, which is exploitable

Routers also have vulnerable code that haven been patched, just like computers

* Known router exploits can be found on exploit-db as well

Search for your own router vulnerabilities using your IPv4 address and search it in Shodan

To see what Ports and Services are running on your router, you can use the router web admin interface - <https://ipaddr>

* Port (range) forwarding
* DMZ
* Port triggering
* UPnP (Universal Plug’n’Play port forwarding)
  + Port forwarding without your knowledge
  + Manufacturer vulnerabilities as well
  + What ever you are port forwarding to MUST be a secure and hardened network/device as this is giving that device full access to your network and devices
* Available patches

Other methods:

* SSH to router with ip
* Telnet to router with ip
* PuTTY (Windows)

Route -n get default

* Gives ip

SSH root@192.168.1.1

* Paste password and login is complete

Once on router, you can scan ports

* Netstat -tuln

Make sure that the ports that are open are only listening to your local network and not the internet

How to check what ports are listening to the internet:

* Nmap
* Zenmap
* Pentest-tools.com / tcp port scanner
* Mxtoolbox.com port scan
* GRC Shields up

Hacked router check (like dark web personal details or password search)

* Techmonkeys.co.uk

**Qualys**

Free online **vulnerability** scanner (more than a port scanner)

Provides guidance on how to fix vulnerabilities

**Internal**

Dynamic Host Configuration Protocol (DHCP) – automatically assigned IP

Statically assigned – by you or whoever runs local network

The router usually assigns ips to the local devices by DHCP

How to determine if you’re using DHCP

* Ipconfig /all (Windows)
* Cat /var/log/syslog ¦ rep DHCP (Linux, Debian)
* Or through network manager
* Network 🡪 network adapter 🡪 advanced (MacOS)

If they haven’t been assigned using DHCP, then they have been statically assigned

**When using Kali on a VM, make sure the network card is in bridge mode**

After port scanning, the next step is to do a vulnerability scan

Baseline Security Analyzer MBSA (Windows)

OpenVAS (Linux)

* Provides you with an ip and a port number
* You then enter this in the search bar on a browser and login to the network
* Set up user and password to login
  + --create-user=admin --role=Admin
  + --user=Admin1 --new-password=admin
  + User and password created: admin, admin
* Login to the greenbone UI with this
* Can enter target host ip for vulnerability scan
* Vulnerability report generated with links to CVEs

**Nessus home**

Scan home network (up to 16 ips) with free version

Perhaps the leading vulnerability scanner

Authenticated scans vs Unauthenticated scam

Unauthenticated scan

* Scanner acts like a hacker, no access to device and looks for vulnerabilities is running services

Authenticated scan

* Provide the scanner with a password and it’ll login to the machine and scan for further vulnerabilities
* This mimics what an attacker might be looking for once he already has access to the device
* More conclusive
* Giving a scanner passwords and access to your device however could mess up the config on the device, it shouldn’t but the risk is there
* Nessus and Qualys shouldn’t have this problem as they are mature services but OpenVAS is free