



**Romel Cabling** ▾



Home

Home > My courses > Network Attacks: Detection, Analysis & Counter... > 02 External Vulnerability Scanning - Shodan, Qual... > Lesson Proper for Week 2

# Lesson Proper for Week 2

## EXTERNAL VULNERABILITY SCAN



An external vulnerability scan is a scan that is conducted outside of the network you're testing.

An assessment that's performed without access to the network that's being scanned. External scans target external IP addresses in your network, identify vulnerabilities as well as all the ports that can be accessed from the internet.

### BENEFITS OF EXTERNAL SCANS

By looking at your network from this view, you can easily identify what that most pressing issue is within your network. You can also identify any services or new servers that have been set up since the last scan and identify if they present any new threats to your organization.

### VULNERABILITY SCANNING TOOLS

#### 1. SHODAN

(Sentient Hyper-Optimized Data Access Network)



A search engine but instead of searching for websites, it searches for internet-connected devices — from routers and servers.

A search engine scanning the entirety of the internet for connected devices.

- **SHODAN** is similar to more well-known search engines like Google, but instead of indexing websites, **SHODAN** indexes each publicly available device connected to the internet.
- **SHODAN** can tell hackers everything they need to know to break into your network.\_

### SHODAN SEARCH ENGINE



*\*SHODAN is designed with IT professionals in mind.*

-

### BRIEF HISTORY

**SHODAN** started in 2003 as a pet project for a young computer programmer, **JOHN MATHERLY. MATHERLY** figured out a way to map each device connected to the internet by constantly crawling the web for randomly generated IP addresses, and he eventually developed a search engine to search through his growing database of internet-connected devices. Matherly released Shodan to the public in 2009.\_

Matherly's intention was never to create an easy way for hackers to discover devices and infiltrate them, but as soon as Shodan was up and running, it began discovering industrial supervisory control and data acquisition (SCADA) systems, security cameras, traffic lights, and other sensitive devices that shouldn't have been publicly accessible.

-

### USES OF SHODAN

- a. Can be used to find vulnerabilities in your devices' security.
- b. A useful resource for data scientists, law enforcement officials, and cybersecurity professionals researching about the dispersal of internet of things (IoT- Internet of Things) products, operating systems, and server technology.

c. By identifying all of the devices connected to the internet, displaying what information those devices are sharing with the public, and making it clear how easy that information is to access.

## **HOW SHODAN WORKS**

**An IP address is your device's digital signature** — it's what allows Google to tailor searches to your location, and it's what allows all internet-connected devices to communicate with each other.

Internet-connected devices have specific "ports" that are designed to transmit certain kinds of data. Once you've established a device's IP address, you can establish connections to each of its ports. There are ports for email, ports for browser activity, ports for printers and routers — **65,535 ports in all**.

When a port is set to **"open"**, it's available for access — this is what allows your printer to establish a connection with your computer.

*\*Example. The computer "knocks" at the open port, and the printer sends a packet of information called a **"banner"** that contains the information your computer needs to interact with the printer.*

**Banners** can provide all sorts of identifying information:

1. Device name
2. IP address
3. Port #
4. Organization
5. Location

**SHODAN** able to find and connect things like:

- Baby monitors
- Internet routers.
- Security cameras.
- Maritime satellites.
- Water treatment facilities.
- Traffic light systems.
- Prison pay phones.
- Nuclear power plants.

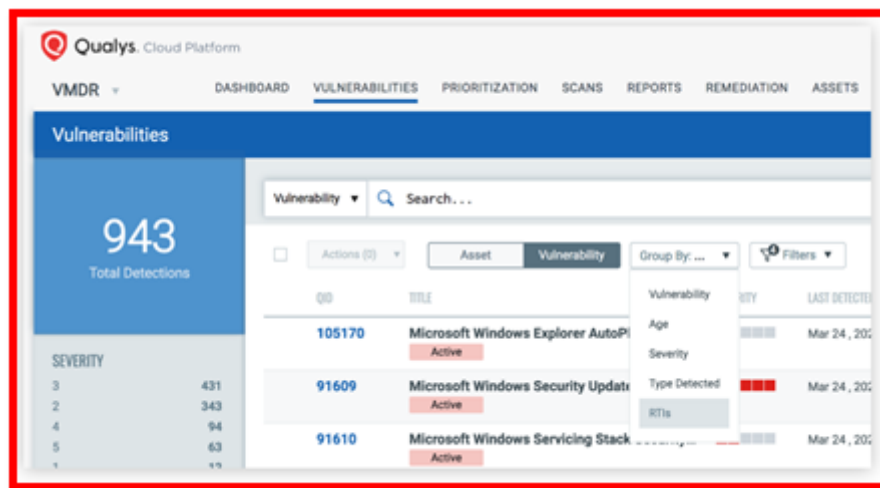
## 2. QUALYS



A cloud-based solution that detects vulnerabilities on all networked assets, including servers, network devices (e.g. routers, switches, firewalls, etc.), peripherals (such as IP-based printers or fax machines) and workstations. Qualys can assess any device that has an IP address.

A commercial vulnerability and web application scanner. It can be used to proactively locate, identify, and assess vulnerabilities so that they can be prioritized and corrected before they are targeted and exploited by attackers

### QUALYS DASHBOARD



### **HOW QUALYS WORKS**

Qualys uses a unique inference-based scan engine to find vulnerabilities. Each scan begins with a pre-scan module which accurately fingerprints a host. The fingerprinting is performed by sending a series of specially crafted packets to the host and by interpreting the results.

Qualys uses a unique inference-based scan engine to find vulnerabilities. Each scan begins with a pre-scan module which accurately fingerprints a host. The fingerprinting is performed by sending a series of specially crafted packets to the host and by interpreting the results.

## 3. NETWORK MAPS

Network Mapping can be defined as understanding the physical connections between various systems/computers in a network.

A visual representation of connections between systems/computers. The visual representation generally includes flowcharts, topographical views, and device inventories.

Network mapping is the process of visualizing all the devices on your network, how they're connected, and how the overall network is structured. The network map generally equips you with information about whether the network is functioning properly or whether any particular device has a problem.

-

### **NETWORK MAP LEVELS**

There are two main levels of maps to consider: *physical and logical*.

**A physical network map** diagrams all the actual components of your network, including cords, plugs, racks, ports, servers, cables, and more. A physical network map gives you a visual representation of all the material elements of your network and the connections between them.

**A logical network map** is more abstract than the physical network map. It shows the type of network topology (bus, ring, etc.), and how the data flows between the physical objects in your network. This includes IP addresses, firewalls, routers, subnets and subnet masks, traffic flow, voice gateways, and other segments of the network.

-

### ***HOW NETWORK MAPPING WORKS***

Networks are set up in different structures, also called topologies. The structure can have a major effect on how your network functions, what happens when a device or server goes down, and how complex it is to manage. When you map your network, you're basically mapping its topology into a visual network diagram.

Here are the main network topologies to be aware of:

1. **Bus** – A bus network is set up in a straight line, allowing data to flow through the network from the server to each node one by one
2. **Ring** – In a ring, network the nodes are arranged in a circle, and data can flow around the circle in one or both directions
3. **Tree** – In a tree topology, a server has multiple branches of nodes coming off it. This is a bit more robust than a bus or ring topology, as with a tree topology, if one of the branches has a problem with a node, the rest of the network will still function. With ring and bus topologies, a problem with one node can cause the whole network to go down
4. **Star** – A star topology has one central node with all others coming off it in a star pattern
5. **Mesh** – A mesh network has connections between all the nodes and servers, like a lattice or mesh. It has high failover protection because if one node goes down, the network can reroute the data to get it where it needs to go
6. **Hybrid** – A hybrid topology is simply a combination of any or all the above network structures and is very common as networks get larger

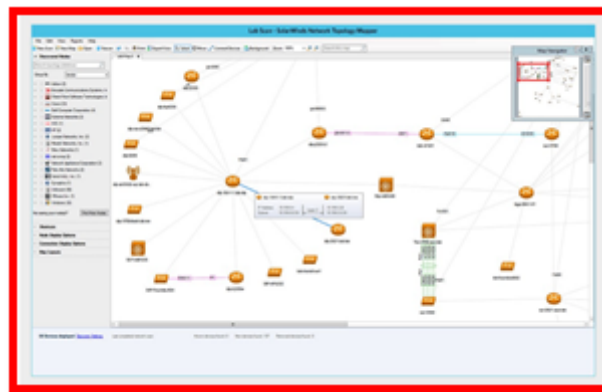
## USES OF NETWORK MAPPING

- a. Used for analysing networks.
- b. checking for connection errors.
- c. to visualize and understand complex network systems by breaking them down into small fragments.

## NETWORK MAPPING TOOLS



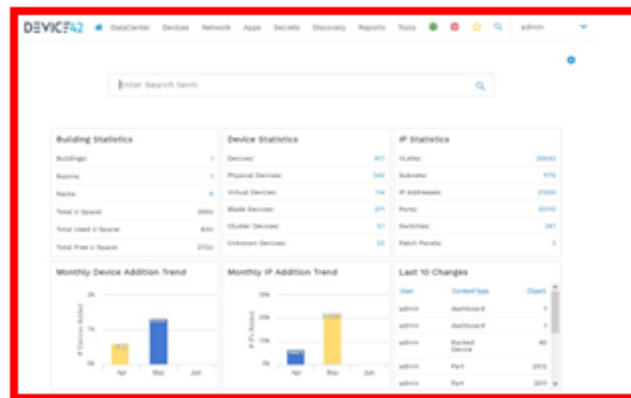
**1. Network Performance Monitor** is extremely useful for both mapping networks and determining how your network is performing. It includes a feature called NetPath, which maps your network and then provides you with information on network performance, traffic, and configuration along the entire service delivery path. You can also see performance metrics with hop-by-hop data between your central servers and your satellite offices.



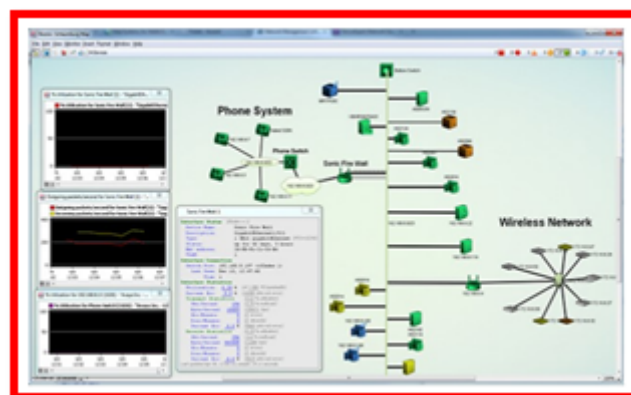
**2. Network topology Mapper** - ability to automatically plot your network to build multiple different kinds of network maps from a single scan.



**3. Paessler PRTG Network Monitor** is a well-known software with monitoring and performance tools as well as reporting features and dashboards. It lets you create maps to show you devices and connections, as well as live status information for your network, so you can detect problems in one glance and troubleshoot effectively using maps as a primary source of information.



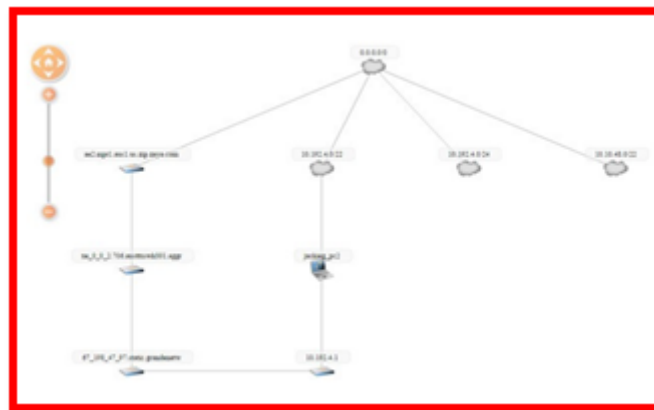
**4. Device42** is a configuration management database with auto-discovery and application mapping tools. You can set up a schedule and Device42 will automatically scan your network and infrastructure and detect any changes as they're made. It can track IP and non-IP based devices and assets, hardware, software, and interdependencies between devices, as well as resource utilization.



**5. Intermapper** allows you to create custom maps quickly and effectively, automatically mapping all the IP-enabled devices in your network. You can customize your maps with colors and different background options, as well as color-coded statuses to show you how the network is performing.



**6. Nmap** is a free and open-source network mapping tool that uses IP packets to determine what hosts are on the network, what services are offered by those hosts, and identify operating systems, firewalls, and other information.



**7. Spiceworks** is a manual network mapping tool that allows you to view an interactive network diagram of how your devices work together and relate to each other. You can add, edit, move, and resize devices on the map to show how your network is structured, as well as using filters and views to show only the most important data. The network map displays lines between each node—the thicker the line, the more bandwidth is being used.

◀ Preliminary Activity for Week 2

Jump to...



Analysis, Application, and Exploration for Week 2 ▶

## Navigation

Home

 Dashboard

Site pages



## My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Participants


General

01 The Home Router

02 External Vulnerability Scanning - Shodan, Qual...

 Preliminary Activity for Week 2

 **Lesson Proper for Week 2**

 Analysis, Application, and Exploration for Week 2

 Generalization for Week 2

 Evaluation for Week 2

 Assignment for Week 2

03 Internal Vulnerability Scanning

04 Open Source Custom Router Firmware

Ojt/Practicum 1

Social And Professional Issues

System Integration And Architecture 2

## Courses



### Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.



### Activities



Assignments



Forums



Quizzes



Resources

---

Bestlink College of the Philippines  
College Department

Powered by [eLearning Commons](#)