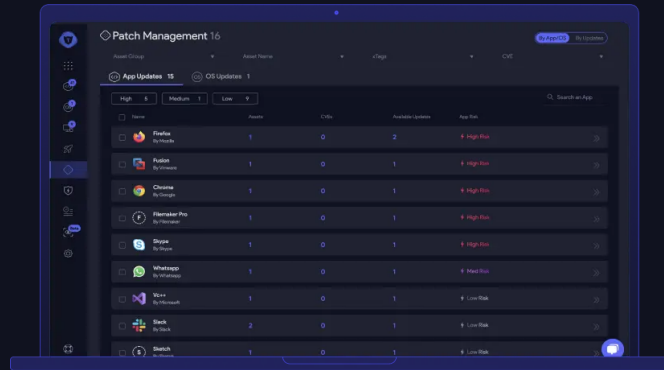


Network Scanner

Get full visibility into your network, visualized in an intuitive vulnerability scanning dashboard.

Perform a network scan with Nmap, the most popular network mapper and vulnerability scanner, and let vRx turn it into a vibrant dashboard of your Nmap XML file results.



Turn Your Nmap XML into a Vibrant Dashboard

vRx makes it easy - just run a scan with Nmap, the most popular vulnerability scanning tool, and import the XML file to vRx. The result is an interactive dashboard that visualizes the scan results in graphs, pie charts, and more.



Network Visibility in 3 Steps

01

Generate Script

02

Import XML

03

Get Visualized Dashboard!

Analyze Your Environment

Visibility

- ✓ Network Insights
- ✓ Port Mapping
- ✓ Services Mapping

Efficiency

- ✓ Share Scan Results
- ✓ Historical Tracking
- ✓ Compliance Reports

Detection

- ✓ OS Detection
- ✓ Systems Inventory
- ✓ Vulnerability Detection

Network Scanner Mapping

Network Visibility

Get full network visibility and monitor the devices, systems, traffic, and applications that utilize your IT infrastructure. Identify unusual traffic or potential upgrades at a glance, protecting against breaches and giving a full-picture view you can use to optimize your network.

Port Mapping

Enable your IT professionals to identify and map all ports and switches, as well as any devices connected to the switch ports, giving them access to essential network information. For each connected port, the platform will list all relevant data for connected devices, such as IP address, OS, and more.

Services Mapping

Service maps give you the ability to keep track of your services and who is using them, allowing you to identify potential problems, optimize services, and track services with extreme accuracy.

Vulnerability Detection

With thorough vulnerability scanning and an advanced alert system, you'll find network vulnerabilities as soon as they're detected. Early identification of vulnerabilities can reduce downtime and give you the tools needed to handle vulnerabilities before they can impact users or lead to breaches.

OS Detection

vRx will remotely identify your scanned host's operating system by analyzing its CP fingerprint, Windows Registry, Unix login, NTP, Windows SRVSVC, and more, giving the information needed to perform TCP Sequence Predictability Classification tests and preventing forged connections from accessing your network.

Compliance Reports

vRx's advanced security capabilities help you stay on top of regulatory compliance needs. Our automatically generated reports can be used to prove compliance and your ability to meet the highest standards of security demanded by regulatory bodies.

Supported Script

</>

Nmap Open Port and Service Detection

```
nmap -sV -sT -O --top-ports 2000 -T4 -oX <output_filename>.xml <target>
```

</>

Nmap Open Port, Service and Vicarius Vulnerability Detection:

```
nmap -sV -sT -O --script=vicarius-vulnerability-scan.nse --top-ports 2000 -T4 -oX <output_filename>.xml <target>
```

</>

Nmap Open Port, Service and Spring4Shell Vulnerability (CVE-2022-22965) Detection:

```
nmap -sT -O --script=spring4shell.nse --top-ports 2000 -T4 -oX <output_filename>.xml <target>
```