How-to Guide:
Stuff Off Shodan

As technology advances and society becomes more interconnected, the chances of your digital device being located on full spectrum search engines has increased dramatically. Asset and device owners may choose to intentionally expose their devices to the public Internet, but some are unaware of this potential and unknowingly face a higher risk of cyberattack. The ability to query for Internet-connected assets is vital to managing attack surface, and Shodan.io can support those efforts.

WHAT IS SHODAN[1]

Shodan (www.shodan.io) is a web-based search platform for Internet connected devices. This tool can be used not only to identify Internet connected computers and Internet of Things/Industrial Internet of Things (IoT/IIoT), but also Internet connected Industrial Control Systems (ICS) and platforms. Further, potential exploits, default passwords and other attack elements can be harvested from search results. Integrations with vulnerability tools, logging aggregators and ticketing systems allow Shodan to be seamlessly incorporated into an organization's infrastructure.

POTENTIAL USE CASES FOR SHODAN

A key capability of Shodan is its use as an attack surface reduction tool, with the ability to read any number of Internet connected targets, including ICS and IIoT. By pulling back banners of Internet connected devices, Shodan can find any combination of search filters to narrow search results to specifically target potentially vulnerable devices. Below are some common use case searches for reducing attack surface.

ASSESS PUBLIC ASSET RISK PROFILE

Each finding represents a distinct system, and each system may have many entries for services running on different ports. For each system, service, and port that is exposed, ask the following questions:

- Why does this system and service need to be running? Equipment often enables capabilities by default that are not necessary in normal operations.
- What is the business need requiring this system, service, and port to be exposed to the Internet? Administrative tools may be inadvertently configured to connect on an Internet-accessible interface.
- Can this system, service, or port reside behind a VPN? VPNs add strong authentication mechanisms and remove a direct link to potential adversaries.
- Can the service offer strong, multi-factor authentication? Contact your vendor to explore options.
- When was the last time this system or service was fully updated? There may be a valid business justification for why a system was not updated; otherwise, follow your change management process and update your systems on schedule.
- When was the last time this system or service was hardened? Contact your vendor for best practices and support.

USEFUL SHODAN SEARCHES

- Locate Internet accessible SQL servers: **product:"SQL" port:"1433"**
- Locate Internet accessible Windows machines with SMB exposed to the Internet: **os:"windows" port:"445"**
- Locate Internet accessible Windows XP devices: **os:"windows xp"**
- Locate Internet accessible OPC UA Discovery Server: **product:"OPC" port:"4840"**
- Locate default passwords: **"password is" OR "default is" -"required"**

[1] The United States Government does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government.

MORE INFORMATION

Shodan is an extremely powerful tool with searching capabilities that are extensive. There are several licensing options that are available depending on the type of usage required. For more information about Shodan.io or to get further searching guidance, visit https://www.shodan.io.