WHAT TO EXPECT WHEN YOU FIRST ENABLE SCANNING

Overview

Executing continuous vulnerability scans is one of the cornerstones of a solid cyber security program for your organization. There is a myriad of tools that are "single scan" type tools that give you a single point in time view of your vulnerabilities. RootSecure enables you to have a continuous view into your network vulnerabilities. By constantly being updated with the latest vulnerability scans and automatically detecting when devices enter and leave your network, RootSecure enables complete real-time visibility into your network risk.

The vast majority of hosts on a network have no impact when having a vulnerability scan executed against them. However, some older devices, or consumer grade devices such as printers or network IoT devices, may have denial of service vulnerabilities that are revealed by simply executing a scan against them. This document describes some of these instances and how they can be effectively managed while RootSecure is deployed.

Note: RootSecure has been designed to use the same or similar tools/methods that hackers use. As a result, any issues that may occur simply by scanning a host are equally trivially exploitable by a hacker to cause a Denial of Service (DOS) condition in your network. For these situations, in addition to taking one of the steps below, we also recommend working with the vendor for an appropriate bug fix or other recommended mitigation options.

What Should I Do If I See an Issue?

Generally speaking, when an issue is discovered, there are 4 possible mitigation steps we recommend. Each issue we’ve observed historically is slightly different, so when considering what action to take, consider the following options carefully:
Whitelisting the sensor IP

Various Intrusion Detection (IDS) features exist on some hosts/products, typically around port scan detection and failed login monitoring. The RootSecure sensor regularly conducts port scans to identify open services, and regularly tries known or default username/password on these services. In these situations, the preferred solution is to whitelist the Sensor IP within the IDS feature/product, eliminating any false alerts that are generated.

Port scanning restrictions

Some applications/services which have not had regular vulnerability scan performed before on them, have bugs which can cause memory leaks, or other performance issues after a period of time. Depending on the situation, we can prevent the scanning of the specific port this service is running on. This will ensure that the rest of the host (base OS and other services) are still being scanned for vulnerabilities, while the specific service causing an issue is not. We recommend working with the application vendor to fix the underlying defect and then re-enable scanning on the specific port.

Scheduled scanning of the host IP

The sensor is capable of scanning IPs/networks only within a specific scheduled window. For hosts where the impact of being scanned creates an inconvenience during working hours, we recommend setting scanning to be outside of typical working hours, so the inconvenience is minimized.

Blacklisting the host IP

This is the “hammer” approach, adding an IP to the sensor blacklist will stop the sensor from scanning that host entirely. From the dashboard/sensor perspective, it is as though that host does not exist at all in the network. This option is available as a last resort option, when the impact of scanning the host outweighs the visibility into those host risks.

What Types of Issues Have Been Observed in The Past?

Each situation tends to be unique, but here are some generalizations that we’ve seen in the past and what we recommend for these situations:

Account temporary Lockouts

Some applications are configured by default, or have the feature enabled, to temporarily disable a user account if a number of failed login attempts are observed. This can be an inconvenience if a user needs to connect to this application while the temporary lockout is active. In these situations, whitelisting the sensor IP is the preferred solution, otherwise scheduling the scanning of this host for a time period where the temporary lockout won’t be as inconvenient.
Antivirus endpoint software

Some antivirus endpoint software alerts the user if a port scan is occurring on the host. Since this is a regular activity for the sensor, we recommend whitelisting the sensor IP address in the endpoint software system to prevent any nuisance alerts to end users.

Printers

Some network attached printers accept un-validated data sent to it on specific ports as print data, and subsequently prints out garbage pages on the printer, wasting paper. The scanner attempts to detect specific printers and prevent this from occurring. However, if this issue is observed, we recommend backlisting the printer.

Note: Some specialty industrial printers may have particularly expensive materials which could be inadvertently wasted in such a situation. As such, we recommend blacklisting those printers and, as part of security best practices, mitigating access to them through network segregation techniques.

Consumer grade devices

Many different types of consumer grade network devices: Wi-Fi access points, uPnP devices, IoT Devices, etc. are occasionally prone to issues when being scanned. This is typically due to poor error handling cases in the network stack of these devices when unexpected data is received on an active listening port. If an issue is observed on one of these devices, we generally recommend scheduling the scanning for this device at a time where the nuisance impact will be reduced. Alternatively, if the impact is more severe, then we recommend blacklisting the device IP.

Networking Equipment

Core to the functionality of a network, although very rare, issues have occurred on some networks when a networking switch/router device is scanned. These issues almost exclusively occur only on old and EOL hardware, or low-end versions of higher-end products. Each of these situations is unique. If you believe that you are seeing an issue with a piece of networking equipment, please contact us. If the impact is more than nuisance level, feel free to blacklist the equipment control port IP or temporarily pause scanning while we can help investigate.

Firewalls

Some firewalls have IDS features built in, we recommend whitelisting the sensor IP in those features to ensure that the network is fully scanned, and no unnecessary CPU resources are wasted on the firewall. Please feel free to contact us and we'll assist in investigating any suspected firewall issue.

VPNs

The RootSecure sensor consumes very little bandwidth typically for most scans. As a result, scanning can be effective across VPN’d networks as long as the VPN has high enough bandwidth
capacity with the sensor traffic and regular traffic combined. VPNs which are specifically rate limited to low bandwidth for VOIP or other similarly low bandwidth VPNs should not be used for scanning as the VPN capacity will likely be exceeded. If you have any questions or concerns about your network configuration and how the RootSecure sensor is best deployed, please contact us.

**Special Industry Specific Concerns**

Some specific industry segments have devices on their network not typical of other businesses/industries as a whole. Special thought and consideration should be taken in these industries around cyber security as a whole, as well as network vulnerability scanning specifically. Please feel free to discuss with us network design best practices around device isolation and network segregation for these types of uncommon/special devices.

**Health Care Industry**

The continuous advancement of health care technology has led to more and more health care specific devices being “network attached” in some form. Doing so has many advantages, but also adds additional risk. For example, a dialysis device vendor may create a network attached device so that the device can be remotely monitored. If the vendor has not invested a lot into security and hardening or has never run a vulnerability scan against the device as part of development, then doing so may cause unexpected behavior similar to an IoT device or consumer wifi router when scanned. However, unlike in the case of a consumer device where the impact is nuisance level, the impact of a dialysis machine having unexpected behavior may result in serious health consequences for patients. As a result, we highly recommend that devices critical to health care of a patient are first isolated from the network using network security device isolation and network segregation techniques, and the respective vendor is consulted about their security practices before a vulnerability scan is initiated on that device IP.

**Networked Manufacturing Devices**

Similarly, to the health care industry, more and more manufacturing devices are network connected devices with many advantages at the cost of additional risk. For any system where, unexpected behavior could result in possible harm to an operator, we highly recommend those devices are first isolated from the network using network security device isolation and network segregation techniques, and the respective vendor is consulted about their security practices before a vulnerability scan is initiated on that device IP.

**Utilities and Scada Devices**

Finally, modern utilities heavily use SCADA devices within their network. These devices are usually isolated at a basic level into a separate network and the vendors of these devices usually invest in security and hardening. However, as a general precaution, since the unexpected behavior of these devices may cause serious impact to operations, similar steps as health care devices need to be taken before actively scanning SCADA devices.
What Systems Are Very Likely to Alert When Scanning Is Enabled?

Intrusion Detection Systems

An Intrusion Detection System (IDS) is designed to detect and alert on the same scanning behavior that the sensor executes continuously. A properly deployed IDS will detect and alert on the scanner as soon as scanning commences. We recommend whitelisting the sensor IP in the IDS to prevent false IDS alerts being a nuisance to your IT staff.

Log Data

Many applications log various debug and error output. When the sensor scans an application or OS, it’s very common for the application to log during the scan. Things like failed connections, unexpected data, failed logins are frequently logged. On some applications that log highly verbose, this can generate a lot of log data. If the log data is not properly managed by an automated log rotation/archiving process, then it’s possible that a host’s hard disk can fill up over time. We recommend following best practices around log management in your network if you observe issues due to log data filling up disks.

Where Do I Go for Questions/Support?

At any time, feel free to contact our security analyst team at support@rootsecure.com for any assistance/questions/comments/concerns you may have.