Tripwire IP360 Scan Progression

When you start a Tripwire® IP360™ scan, there are 11 tasks that run in background, and many of these tasks are influenced by other information.

The 11 tasks of a Tripwire IP360 scan are:

1. Name Resolution
2. Ping
3. Host Discovery
4. NetBIOS Name Resolution
5. Credential Set Creation
6. CIFS Share Enumeration
7. Port Scan
8. Application Scan
9. OS Fingerprint Scan
10. OS Computation
11. Vulnerability Scan

Details for each scan task

Name Resolution

During Name Resolution, the IP Addresses provided during Network Configuration are resolved to host names that are displayed during scanning and in scan reports. This is done using the DNS Servers configured for the appliance performing the scan.

Ping

Pinging hosts is a portion of host discovery; however, it is separated into its own task. There are database specific configurations that can be applied to the product around ICMP timeout and max requests.

Host Discovery

The actions that occur during the Host Discovery phase are dictated by the configured Scan Profile. During this task, specific TCP and UDP ports are contacted in an attempt to determine if a host is up and responsive.

NetBIOS Name Resolution

NetBIOS Name Resolution uses a very specific NetBIOS packet to attempt to determine the NetBIOS Name of a host. If the name is discovered, it is reported in a scan report.

Credential Set Creation

During Credential Set Creation, the credentials that were provided via the Tripwire IP360 user interface are turned into specific credential sets that can be provided to rules when requested.

CIFS Share Enumeration

Independent of any ASPL rules, enumeration of available shares on the host is done during the CIFS Share Enumeration task. This is reported on the main page of a scan report.

Port Scan

When the Port Scan task is initiated, the ports are scanned based on the known port list in ASPL. There are settings related to retry attempts and timeouts that can be configured in the database to tweak the port scan.

Application Scan

The Application Scan task is the first task that fully leverages Tripwire's Advanced Security Profiling Language (ASPL). ASPL is the heart of the info-gathering portion of the scan.

During the Application Scan task, application rules are executed against ports that are discovered to be open. Tripwire IP360 associates various protocols to specific ports and will only scan for those protocol to port pairings.

Tripwire IP360 also leverages extensive research to execute protocols, applications, and rules in a specific order to limit the intrusiveness of a scan. Should you wish to scan for protocols and applications on non-standard ports, the Scan Profile contains the Enhanced App Scan option. While this option provides a more in-depth scan, it also increases the likelihood of a negative application interaction occurring.

Also during the Application Scan, "votes" are also gathered for applications that can only exist on specific operating systems for later use in the OS Computation portion of the scan.

Tripwire IP360 leverages a unique tree based scanning structure, which allows the product to identify protocols, specific applications running on that protocol, and, finally, specific versions of that application.

OS Fingerprint Scan

The OS Fingerprint Scan task allows Tripwire IP360 to apply traditional Stack Fingerprinting techniques to assist in determining the operating system.

There are eight stack fingerprint rules that are executed against a host and then compared with a database of known operating system responses. The result of each successful response match is a single "vote" for an operating system, meaning a full Stack Fingerprint match could provide eight votes for a host.

This portion of the scan can be disabled in the Scan Profile.

OS Computation

When all of the operating system votes have been determined, Tripwire IP360 determines the most likely operating system. This is done during the OS Computation task.

All votes that were cast during the Application Scan are combined with votes from the OS Fingerprint Scan to determine the total votes for each operating system. The operating system with the highest number of votes is reported in the scan report. If more than two or more operating systems get the same number of votes, the parent OS of the operating systems will be reported in the scan report.

Vulnerability Scan

The Vulnerability Scan task is the most crucial task that is performed during each scan. This is where all the information gathered to this point is used to determine the vulnerable state of a system.

Due to the Tripwire IP360 Application Tree, only vulnerabilities rules associated with applications discovered on the system are executed. Additionally, the results of OS Computation are used to further pare down the number of vulnerability rules that are run.

As with the Application Scan, rules executed during the Vulnerability Scan can be ordered to limit the intrusiveness of a scan. Additionally, the specific vulnerabilities rules executed in a scan can be controlled using a Scan Profile's Fine Tune tab.

There are several types of rules that can be run during a Vulnerability Scan. These can be configured using in the scan profile.

- **Verified Rules:** Rules that have been confirmed and are in a verified state (i.e. shipping rules from your ASPL package, plus custom rules that have been marked verified).
- **Intrusive Rules:** Rules that may result in product crashes. Customers are advised not to run these rules unless they are in a test environment, where negative application interactions are acceptable.
- **Custom Rules:** These are rules inserted directly into the VnE, written by the customer or Tripwire's Professional Services team.
- **Authentication Attempted Rules:** Certain rules in the system are used to look for weak or known bad passwords. These rules could, potentially, cause an account lockout. If that is a concern on the network being scanned, this setting allows you to disable those rules.