Top 3 Undiscovered Vulnerabilities IPsonar Finds on a First Scan

A publication of Lumeta Corporation
www.lumeta.com

Introduction

Large enterprises function in an ever-expanding IP space and often have difficulty getting a handle on every network connection, host, and active IP on their networks. It is in this gray area where connected devices can fall outside the watchful eye of security management. Consequently, this is where serious threats can (and often do) manifest themselves. The remedy lies with Network Discovery; the simple idea being: you can't secure what you can't manage, and you can't manage what you don't know about.

However, all network discovery products are not the same. Lumeta IPsonar uniquely fills a gap in situational awareness – by discovering and providing data on the entire network including all assets and connections, both known and previously "unknown." Finding, identifying, and cataloging several hundred thousand devices across a global, secure infrastructure extremely rapidly and without disruption or triggering alarms on security tools is what IPsonar does best.

Unlike most discovery products, IPsonar performs active probes of the address space, empirically discovering everything that's on the network – not just the IP range that is supplied for scanning. Network connections that are discovered and mapped are proven through these active probes, rather than inferred based on requested routing information.

These are the methods IPsonar's Network Discovery uses to look for unknown networks:

- Apply multi-protocol discovery to penetrate deep into the network, identifying forwarding and filtering devices.
- Trace data paths through a network to visualize how connectivity flows.
- Flag "stealth" assets that do not respond to direct queries, pinpointing resources that may not be under management.
- Validate that firewalls and router access control lists (ACLs) are operating in compliance to policy.

Further, the patented leak detection in IPsonar reveals unauthorized connections between a network and another network or sub-network, (e.g., unsecured routers exposed to the Internet or open links to former business partners). This is crucial in the proactive fight against leaks, revealing all unauthorized connections by protocol, and identifying whether access is outbound, inbound, or both.

IPsonar provides a route-based network topology based on the true state of enterprise network connectivity.

Top 3 Undiscovered Vulnerabilities IPsonar Finds on a First Scan

1. IDS/IPS deployment isn't enough

Intrusion Detection & Prevention Systems (IDS/IPS) providers typically recommend that a company place an IDS/IPS on every segment where there is critical data to protect or a set of users that should be monitored. As a result, large companies often need to deploy hundreds of IDS/IPS within their networks.

In practice, IPsonar frequently discovers unprotected areas of the network, where an IDS/IPS deployment could be more effective.

Using IPsonar as part of a comprehensive security strategy to guide IDS/IPS deployment and maintenance, our clients are able to proactively identify candidate areas for placement of IDS/IPS and other security monitoring tools.

IPsonar has capabilities that IDS/IPS solutions do not have:

- Find the unknown parts of the network, identify devices, subnets, and networks
- Show the boundaries between autonomous systems
- Map how actual connectivity flows across the network

These hidden parts of the network, which often pose an even greater threat than the well-managed and protected areas of the network, are brought into visibility through the unique network discovery capabilities of IPsonar.

Our clients recognize the need for security tools such as IDS/IPS, but are also quick to realize that in order to truly secure the network, and for the IDS/IPS to realize its potential, they need to know what parts of the network pose the greatest threat.

2. Vulnerability Management isn't enough

Vulnerability Management (VM) tools identify vulnerabilities specific to each network device (e.g., routers, servers) in known portions of the network.

VM will identify the IP addresses available via the external domain name servers for a given domain and conduct tests on those devices. Users can also input IP addresses directly. They do not, however, discover what else is connected to the network. IPsonar empirically discovers all devices and connectivity across the network, including previously unidentified areas.

By the nature of the detailed vulnerability analysis that VM tools perform, scalability is not their highest priority. Generally, these tools will take approximately 30 minutes to scan a Class C network (256 addresses). In contract, IPsonar, which was built on the technology originally developed to discover and map the Internet, routinely scans networks consisting of multiple Class A networks (tens of millions of IP addresses) within hours.

In addition to these limitations, VM tools focus on vulnerabilities at the device level. They do not focus on vulnerabilities at the level of the network itself. For example, VM tools do not identify the network perimeter or analyze connectivity to other networks. IPsonar does discover all devices and connectivity in the address space, including issues like legacy partner connections or remote offices with a rogue Internet connection – issues that often quietly avert the security a VM tool can provide.

Our clients understand the value of VM tools. The detailed vulnerability analysis they perform on devices is important. However, in order to fully secure a network, this analysis needs to be carried out on all devices. IPsonar can identify network connections, and the endpoint devices on those connections, to feed the VM tools with complete network information.

3. Non-traditional IP-enabled devices aren't being properly secured

Over the last decade-plus, the proliferation of Internet Protocol (IP) has grown at a tremendous rate. IP-enabled devices are not just the traditional computing devices of the past, but the IP network is also home to a number of consumer devices, industrial control systems/SCADA, ATMs, POS machines, healthcare devices, IP phones, and more. These non-traditional network endpoints are not always managed or monitored by IT tools, and so they often pose a security hole, even in some of the best managed infrastructures.

The adversaries of today are simply seeking to gain entry into the network. Once they are in, they're in. And they will traverse the connections within the network until they find the sensitive data they are seeking. They don't look for the high-profile targets, they're searching for targets of opportunity and often non-traditional IP-attached devices provide them with that opportunity.

IPsonar operates with tremendous speed and ease to discover all connected devices and connections across the network, providing IT with the information needed to ensure that every connected IP-enabled device, regardless of its manufacturer or function, is secured. IPsonar's discovery looks for default configurations/credentials, open ports, and much more. When most network operations or security managers see for the first time the connections that ATMs, healthcare devices, infrastructure controls, and other non-traditional IP-enabled devices leave open on their otherwise well protected network, they understand the power of global network visibility.