Why Network Discovery is the Foundation of a Secure Digital Environment

by Devin Jones, Chief Product Officer, UncommonX

Network discovery is foundational to a well-managed and secure digital environment. Unfortunately, most organizations struggle to identify and detail every device, or even most devices, within their environments, whether physical or virtual. There are many purpose-built approaches to network discovery, but, unfortunately, they are often specific to a vendor's primary solution, such as configuration management databases (CMDBs), vulnerability scanners, and security incident and event monitoring systems (SIEMs).

Also, none of them provide a holistic approach that can be leveraged by security organizations and those responsible for network operations. Though there is one solution on the market that does: the patented BOSS (Business Operation Security Suite) platform from UncommonX. To understand why, let's first look at what is required for effective discovery.

Organizations need a complete understanding of assets within the environment so that they can:
Evaluate and assign customized treatment levels for devices based upon business criticality
Identify unmanaged or unknown devices
Identify vulnerabilities, such as outdated or at-risk software and OS version
Evaluate at-risk devices by proximity or communication during an IOC event

Multiple discovery methods are required to achieve discovery's necessary detail and inclusiveness for adequate situational awareness. Each approach has its strengths and weaknesses, but individually they won't provide the fidelity required for sufficient operational understanding. Discovery approaches include passive discovery, authenticated discovery, dark space scans, and agent-based discovery.

Passive discovery has two methods of information gathering to identify the existence of devices and their locations. The first method is to "sniff" traffic live

on the wire using a span/mirrored port or tap to observe packets passing on the network. This method can identify the existence of a device and capture packet metadata that can be fingerprinted. However, probes must be implemented on every monitored network, end-to-end visibility is often not possible, and the depth of data is limited. The second method of passive discovery is to leverage network devices, like firewalls and routers, to gain visibility of devices captured in logs communicating within the environment. This is a good starting point because you know what's "talking" on the network(s) and can leverage other methods for further prosecution for expanded discovery context. Both methods ensure network performance disruption is imperceptible.

Authenticated discovery leverages login credentials of managed devices. This method is typical of vulnerability scanning applications like Nessus or Qualys. Authentication credentials allow for detailed information about devices, such as vendor, OS, service pack versions, registry, file system, processes, memory, and more. In addition, the level of details from managed devices provides asset role and functionality information. Still, it gives no visibility into unmanaged devices, such as unauthorized entities, many IoT endpoints, and guest devices. In the past, penetration testers leveraged authenticated discovery scans to capture credentials from the packet streams of the scanner as it connects to a managed device. Modern access methods have made this vulnerability obsolete, but many remain concerned about this attack vector.

Dark space scans do not leverage credentials but explore a network environment's "dark spaces." They discover the "unknown" and "unmanaged" elements. This approach leverages ping sweeps and TCP/UDP port scans to contact ranges of IP addresses soliciting a response. Once a response is established, the devices are swept for a full range of port numbers to identify active ones. Systems can infer, or "fingerprint," the services running and, subsequently, the device's function from active port identification. Dark space scans will often also query SNMP MIBs using GET NEXT scans to mine as much information as available. ARP caches are also sometimes queried if available. Dark space scans are excellent at discovering that "something" exists on a network and can provide reasonable "guesses" to their function. They don't require endpoint agents or authentication credentials. However, information derived from these scans is limited, and if the traffic generated is not closely metered, it can severely disrupt the connectivity of fragile devices.

Agent-based network discovery requires installing an agent on every device under management. Like authenticated discovery, these scans can uncover detailed information about devices, such as vendor, OS, service pack versions,

registry, file system, processes, and memory and even detect malware. Also, like authenticated discovery, they are only effective on devices under management. Unfortunately, agent-based discovery is cumbersome to deploy. An agent must be deployed on every device under management, which is not trivial in even medium-sized companies. In addition, the agents can slow down endpoint performance and are not available for all types of platforms. This method is typically used in endpoint detection and response (EDR) solutions, SIEMs, and CMDBs.

Detailed asset discovery is crucial for both network and security operations. A practical network discovery approach requires the ability to identify and classify both managed and unmanaged devices on the network, whether they're on-premises, in a colocation facility, physical, virtual, or in the cloud. In addition, it's crucial to have a detailed understanding of the assets under management and identify unknown or unmanaged assets within the environment to evaluate and manage risk.

The UncommonX BOSS platform is unique and effective because it leverages several methods to ensure the highest fidelity asset discovery information without disrupting network performance or device performance or challenging endpoint agent installation. First, it leverages authenticated discovery to collect the necessary details of devices under management. Almost all networks currently deploy EDR solutions, SIEMs, or other solutions that require endpoint agents. BOSS integrates with existing systems to take advantage of existing sources of information in the same manner as authenticated discovery without having to bog down system performance with yet another agent.

The platform also uses passive discovery from existing network devices to identify "talking" entities on the system. This narrows down the IP address ranges that dark space scans prosecute so that network traffic and disruption to device and network performance are minimized. BOSS's powerful detection strategy effectively identifies all devices throughout the environment, captures detailed information gathered through automation, and ensures that performance impact is managed completely. There is no other solution that can provide the same comprehensive picture of what is in your network environment.

About the author

Devin Jones is Chief Product Officer for UncommonX. He is an accomplished executive leader with advanced experience building company infrastructures that define, design, build, and deliver product value and revenue growth. He has excelled at helping companies like Cisco and Juniper Networks establish new markets and identify growth.