Using Nessus To Discover Rogue Access Points

www.tenable.com/blog/using-nessus-to-discover-rogue-access-points

A "Rogue" Access Point

Detecting and preventing rogue wireless access points is a major concern for many organizations. It is important to ensure that all wireless networks are established and configured in compliance with the organization's policies and standards for wireless networks. The problem is that it is very easy for a user to establish a rogue wireless access point either inadvertently or deliberately. A wireless access point plugged into your network will typically have an Ethernet connection tied into some part of your LAN, and provide wireless access to an attacker that bridges the connections. Users could put one on the network for convenience, or a company provisioned access point could be misconfigured by the IT department. Recently the PCI standards council has produced a document called "The Information Supplement: PCI DSS Wireless Guideline", that outlines the recommendations for securing wireless networks for PCI DSS compliance. This is a good reminder of the importance for organizations to continually seek out rogue access points in their environments and remove them.

Types of Rogue Access Points

A rogue access point can take many forms. Popular examples include using a SOHO wireless router or reconfiguring an existing wireless client/device. However, there are typically multiple configurations for the rogue access point:

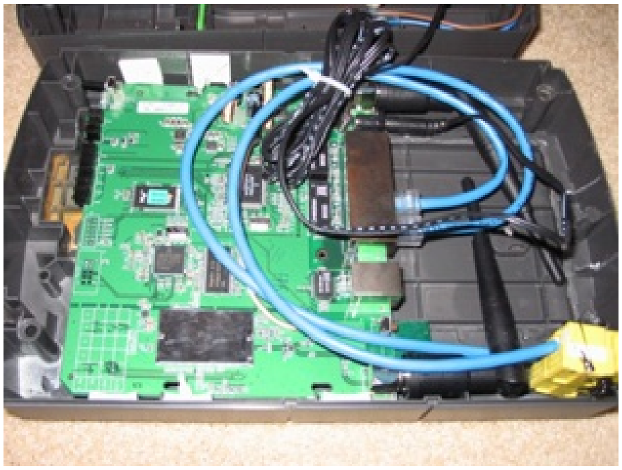
- **Wireless router connected via the "trusted" interface** - In this configuration the wireless access point connects the "trusted" side of the router to your internal network. A DHCP server is typically enabled and can conflict with your own internal DHCP server. Usually all management ports and services are configured as well, such as HTTP or SNMP.

- **Wireless router connected via the "untrusted" interface** - In this case the external, or firewalled side, is plugged into your internal LAN. Typically, very few services, if any, are available on this interface, making it difficult to detect across the network.

- **Installing a wireless card into a device already on the trusted LAN** - While this requires physical access, an attacker or user could install a wireless card into a system on the trusted LAN. The system could then be configured as an access point, which is a function supported by most wireless chipsets, drivers and popular operating systems such as Windows, Linux and Mac OS X.

- **Enabling wireless on a device already on the trusted LAN** - This is the same as the above, except the attacker or user utilizes the hardware and drivers that are already present.

Rogue Access Point Inside UPS



> *The picture above shows a rogue wireless access point installed into a desktop APC UPS. The device is a Linksys WRT54G router with 802.11b/g wireless capability. The Ethernet ports on the UPS are connected to the Ethernet ports on the Linksys router, providing the ability to collect traffic in addition to providing the attacker or user remote access. In this case, the trusted side of the rogue access point is connected to the internal network making it easier to detect (depending on the configuration). More information about this project can be found at http://www.renderlab.net/projects/sneaky/.*

Wired Side Scanning vs. Wireless Scanning

The PCI DSS Wireless Guideline clearly states, and re-enforces PCI requirement 11.1, the need to perform wireless rogue access point detection using a wireless sensor. This requirement describes the limitations of wired side scanning, first limiting it to *"tools that scan suspicious hardware MAC addresses on switches"* and also states:

- *"...tend to have high false positive/negative detection rates."*
- *"Often miss cleverly hidden and disguised rogue wireless devices or devices that are connected to isolated network segments..."*
- *"Wired scanning also fails to detect many instances of rogue wireless clients. A rogue wireless client is any device that has a wireless interface that is not intended to be present in the environment."*

However, they fail to list the limitations with wireless analyzers, which include:

- Many do not listen on all 2.4 GHz channels, for example channels 12-14
- Many do not monitor on all frequencies and technologies, such as 802.11a/n, Bluetooth or 900Mhz
- On congested networks, how do you tell the difference between access point providing access to the office upstairs or a rogue access point on your network?

It is interesting that both wired and wireless detection methods for rogue access points tend to have high false positive/negative detection rates, and can miss cleverly hidden devices. As for the notion that wired scanning can miss rogue wireless clients, this is simply not true with regards to Nessus as configuration checking can be used to detect wireless adapters in use by wired clients, and even detect their state.

Ubiquiti SR9 900 Mhz Wireless MiniPCI

> *The wireless card above uses the unlicensed 900 MHz frequency to transmit wireless data. This card is supported under Linux using the MadWiFi drivers. Since many organizations do not monitor for 900 MHz, it could be used in a rogue wireless access point to provide an attacker or user a backdoor into the network. However, the device providing wireless access needs to be plugged into the Ethernet network to gain access to your internal network.*

To overcome all of these limitations, use both wired-side and wireless rogue AP detection. It is useful to have some form of wireless intrusion detection, even if you are working with a limited budget. Using open-source projects such as Kismet can provide good results. Wireless security researcher Joshua Wright, author of several popular wireless attack and defense tools, put together a great presentation on using Kismet to monitor your wireless network. Kismet is a free and open-source wireless analysis tool that can be integrated with other tools, such as Microsoft Excel, to produce reports and analyze data. There are also several commercial tools available to monitor the wireless network and most major wireless vendors include features to detect rogue access points in their systems.

Detecting Rogue Access Points on the Network

Nessus contains a plugin called Wireless Access Point Detection, which enables you to discover rogue access points on the network. It goes through several steps to determine if a device is in fact a wireless access point:

1. The OS fingerprint plugins build the database to determine the operating system type and function of the device. The sophisticated operating system fingerprinting functionality in Nessus uses different tactics that extend beyond the popular TCP/IP fingerprinting method, including analyzing several protocols such as HTTP, FTP and SNMP. More documentation on how Nessus detects the operating system can be found in the post titled "Enhanced Operating System Identification with Nessus"

2. Checks the OS fingerprint database to see if anything has been flagged as a WAP, or "Wireless Access" point, and if so writes it to the report.

3. Takes Nmap's list of OS fingerprints that relate to wireless access points and compares it against the list of found OS fingerprints.

4. Looks at the Realm of the web authentication of the device, compares it against a list unique to Nessus. Additionally checks against a generic list of Realms, e.g., "Wireless", " AP ".

5. Performs an FTP and Telnet banner match to determine if it is an AP.

6. Performs SNMP queries, using the "public" community string to identify the device as a WAP, checking the "sysDesc" MIB for evidence of a WAP.

Nessus also has several plugins that detect Wireless access points and associated vulnerabilities that have been published. In addition, if the device is using NAT and port forwarding, Nessus will detect that there are multiple hosts behind it of different operating systems with plugin id 31422, Reverse NAT/Intercepting Proxy Detection. This functionality is commonly found in Wireless Access Points to allow services from the Internet to different hosts behind the firewall.

Passively Detecting Wireless Access Points

The Passive Vulnerability Scanner (PVS) contains functionality to find APs using several plugins. The plugins look at many different types of network traffic for the presence of wireless access points, including:

- HTTP - Several devices are managed via HTTP, and PVE can examine the traffic to detect many devices and flag them as wireless access points.
- SNMP - Nessus will try to query the SNMP service on the device, but will only be effective in the default configuration by trying the community string "public". If the SNMP traffic is going in clear-text, PVS can see the SNMP information without knowledge of the community string and use this information to determine if the device is a wireless access point.

PVS also contains several plugins that inspect network traffic and look for evidence they are behind a NAT device. These plugins are great for detecting the rogue access point that has been plugged in with the "untrusted" side connected to your internal LAN. Traffic leaving the "untrusted" interface and traversing your LAN will typically be NAT'd. PVS will look for specific patterns in the traffic to identify this, including:

- Looking for the X-Forwarded-For field and User-Agent strings associated with proxies
- Detecting when one IP address is presenting itself as multiple operating systems

Conclusion

Rogue access points can be established either by attackers or authorized users to gain access to your internal network. Whether an attacker installs such a device, or a user reconfigures a device already connected to the network, the risk is equally high. Use a two-step approach to detect rogue access points, incorporating both wireless and wired-side information about such devices. Make certain that you maintain a "whitelist" of access points in your environment, including the IP address, MAC address and the wireless MAC address to be certain that one of your own access points is not flagged as "rogue".