www.inl.gov

Idaho National Laboratory

Auto Discovery of Network Nodes through Passive and Active Methods

Addressing the long standing challenge of automatically discovering network nodes

Owen Parkins
New Mexico Institute of Mining and Technology
Mentor: Jake Gentle (D520)
Technical Leads: Rita Foster and Bryce McClurg (D520)

Overview

Discovering nodes connected to a network has been a long standing challenge for network administrators who want to detect intruders on their networks. Creating an automatic solution is a greater challenge due to the increasing complexities of networking (Foster & McClurg, 2018). A node can be discovered through passive or active methods. A passive method will capture network traffic and determine the node type based on sent and received traffic. Active methods test nodes and use a node's response to the node type. This project is looking at Nmap, Ettercap, and a Commercial Off-The-Shelf (COTS) product. The first tool is an active method, while the other tools are passive.

Objectives

Determine the auto discovery capabilities of Nmap, Ettercap, and COTS contain. Each tool is unique and could identify different fingerprinting information about a substation automation control network nodes that could be used to create a detailed network map.

Observations

Active Method Pros (+) and Cons (-):	Passive Method Pros (+) and Cons (-):
+ Detects responding devices	+ Undetectable via tools
+ More accurate fingerprints	+ Detects ongoing attacks
- Invasive	- Quiet nodes undetectable
- Uses lots of bandwidth	- Requires router configuration

Auto Discovery Results

	Nmap	Ettercap	COTS
Hosts Detected	11	6	10
Host Fingerprint Accuracy	81%	*0%	*20%
Services Detected	29	1	9

* - Passive methods will increase in accuracy the longer the method is used, and the more traffic that is analysed.

Methods

A laptop with all three tools hosted inside a virtual machine with a bridged network adapter was used. Two different network connections to this network were available to the laptop. The first was a standard ethernet connection to the main router, and the second was a ethernet connection in a span configuration. The network used Modbus in addition to normal protocols between the devices. One at a time the tools were ran on the laptop. COTS and Ettercap were ran for an adequate time of at least 30 minutes, though exact timing was not measured.

Significance

The active method was able to determine more about the heterogenous network setup than the passive methods. This is because it uses a brute force technique to determine the network architecture. The passive methods were surprisingly successfully despite the limited time that was given to them and that the network uses report by exception which generates less network traffic. The COTS tool created more refined and useful output than Ettercap.

Future Work

Joining both active and passive discovery methods could prove beneficial to protecting a network. Future work should investigate using an ELK stack, a data analytics tool, to refine Ettercap's output and possibly include Nmap's output. The ELK stack could also be used to join Ettercap and Nmap's output together into a meaningful display. Other tools like BinWalk should be investigated to more accurately identify what services are running on network nodes. This allows network administrators to more accurately protect their networks.

References

Foster, Rita. A. & McClurg, Bryce. L. (2018). Efficacy and Measurement of Automated Response. *POWID ISA. INL/LTD-18-50286*
Foster, Rita. A. & McClurg, Bryce. L. (2018). Machine-to-Machine Automated Threat Response - Core Concepts. INL/LTD-18-50175