CLOUD ENABLED ATTACK VECTORS

In partial fulfillment of the requirements for the
Degree of Master of Science in Technology

A Directed Project Report

By

Ryan Jasper

4/8/2015

Committee Member
Phil Rawles, Chair
Jeff Whitten
Raymond Hansen
Anthony Smith

Approval Signature

Date
4/8/15
4/8/15
4/8/15
4/8/15
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>LIST OF FIGURES</th>
<th>v</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>vi</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>viii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>xi</td>
</tr>
<tr>
<td>CHAPTER 1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Statement of Problem</td>
<td>2</td>
</tr>
<tr>
<td>1.2 Research Questions</td>
<td>2</td>
</tr>
<tr>
<td>1.2.1 Primary</td>
<td>2</td>
</tr>
<tr>
<td>1.2.2 Secondary</td>
<td>3</td>
</tr>
<tr>
<td>1.3 Scope</td>
<td>3</td>
</tr>
<tr>
<td>1.4 Significance</td>
<td>3</td>
</tr>
<tr>
<td>1.5 Assumptions</td>
<td>4</td>
</tr>
<tr>
<td>1.6 Limitations</td>
<td>4</td>
</tr>
<tr>
<td>1.7 Delimitations</td>
<td>5</td>
</tr>
<tr>
<td>CHAPTER 2. Literature Review</td>
<td>6</td>
</tr>
<tr>
<td>2.1 Anatomy of a Malicious Attack</td>
<td>6</td>
</tr>
<tr>
<td>2.1.1 Reconnaissance</td>
<td>7</td>
</tr>
<tr>
<td>2.1.2 Delivery</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Common Attack Methodologies</td>
<td>8</td>
</tr>
<tr>
<td>2.2.1 Eavesdropping</td>
<td>8</td>
</tr>
<tr>
<td>2.2.2 Social Engineering (SE)</td>
<td>11</td>
</tr>
<tr>
<td>2.2.3 Command and Control (C2)</td>
<td>12</td>
</tr>
<tr>
<td>2.3 Meraki: Cloud Managed Infrastructure</td>
<td>12</td>
</tr>
<tr>
<td>2.3.1 History</td>
<td>13</td>
</tr>
<tr>
<td>2.3.2 Meraki Functionality</td>
<td>14</td>
</tr>
<tr>
<td>2.4 Summary</td>
<td>17</td>
</tr>
<tr>
<td>CHAPTER 3. Procedure</td>
<td>18</td>
</tr>
</tbody>
</table>
3.1 Reconnaissance .................................................................................. 19
3.2 Weaponization .................................................................................. 21
3.3 Delivery ............................................................................................ 22
3.4 Compromise ...................................................................................... 23
3.5 C2 .................................................................................................... 23
3.6 Exfiltration ....................................................................................... 24
CHAPTER 4. Results ............................................................................. 25
4.1 Findings ........................................................................................... 25
  4.1.1 Reconnaissance ........................................................................... 26
    4.1.1.1 Telnet Communications .................................................... 27
    4.1.1.2 FTP Communications ..................................................... 29
    4.1.1.3 HTTP Communications .................................................. 30
  4.1.2 Weaponization ........................................................................... 32
  4.1.3 Delivery ...................................................................................... 33
  4.1.4 Compromise ............................................................................... 33
  4.1.5 C2 .............................................................................................. 34
  4.1.6 Exfiltration .................................................................................. 34
4.2 Caveats ............................................................................................. 35
  4.2.1 Successful Reconnaissance Phase ............................................. 35
    4.2.1.1 Attack AP Location ........................................................... 36
    4.2.1.2 Mitigating Failure .............................................................. 37
CHAPTER 5. Conclusion ......................................................................... 38
5.1 Impact on Taxonomy ......................................................................... 38
5.2 Mitigation Techniques ...................................................................... 39
  5.2.1 NAC .......................................................................................... 40
  5.2.2 Best Practices ............................................................................ 40
  5.2.3 Block Communications ............................................................. 41
5.3 Future Work .................................................................................... 41
REFERENCES ....................................................................................... 44
APPENDICIES

Appendix A  Cisco 1841 Router Configuration .........................................................47
Appendix B  Meraki Dashboard: Attacker Configurations and Packet Capture .50
Appendix C  Meraki Dashboard: Lab Configurations ..............................................52
VITA ..........................................................................................................................54
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2-1</td>
<td>Management and Data Plane Flows (Meraki, 2015)</td>
<td>17</td>
</tr>
<tr>
<td>Figure 4-1</td>
<td>Lab Architecture</td>
<td>26</td>
</tr>
<tr>
<td>Figure 4-2</td>
<td>Simulated Telnet Traffic</td>
<td>28</td>
</tr>
<tr>
<td>Figure 4-3</td>
<td>WireShark Telnet Data Extraction</td>
<td>28</td>
</tr>
<tr>
<td>Figure 4-4</td>
<td>Simulated FTP Traffic</td>
<td>29</td>
</tr>
<tr>
<td>Figure 4-5</td>
<td>WireShark FTP Data Extraction</td>
<td>30</td>
</tr>
<tr>
<td>Figure 4-6</td>
<td>Simulated HTTP Traffic</td>
<td>31</td>
</tr>
<tr>
<td>Figure 4-7</td>
<td>WireShark HTTP Data Extraction</td>
<td>31</td>
</tr>
<tr>
<td>Figure 4-8</td>
<td>Visual Representation of HTML Code</td>
<td>32</td>
</tr>
<tr>
<td>Appendix Figure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Figure B-1</td>
<td>Attack AP WLAN Availability in Reconnaissance Phase</td>
<td>50</td>
</tr>
<tr>
<td>Figure B-2</td>
<td>Attack AP WLAN Configuration in Reconnaissance Phase</td>
<td>50</td>
</tr>
<tr>
<td>Figure B-3</td>
<td>Wired PCAP From Attack AP in Reconnaissance Phase</td>
<td>51</td>
</tr>
<tr>
<td>Figure C-1</td>
<td>Meraki MS220 Layer 2 Switch Switchport Configuration</td>
<td>52</td>
</tr>
<tr>
<td>Figure C-2</td>
<td>Meraki MX64 VLAN, routing and Switchport Configuration</td>
<td>52</td>
</tr>
</tbody>
</table>
## LIST OF ABBREVIATIONS

This section contains abbreviations of terms used throughout the research.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CDP</td>
<td>Cisco Discovery Protocol</td>
</tr>
<tr>
<td>C2</td>
<td>Command and Control</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Control Protocol</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper Text Transfer Protocol Secure</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Media Access Control Address</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>PCAP</td>
<td>Packet Capture</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>SE</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
GLOSSARY

This section contains definitions of terms used throughout the research.

Access point – Network infrastructure device capable of transmitting and receiving 802.11 radio frequencies to facilitate wireless network access

Address Resolution Protocol – Translates Layer 3 IP addresses to Layer 2 MAC address, facilitating communication between Layer 2 and 3.

Attack – Also malicious activities, cyber-attack, hack – Any kind / multitude of exploits launched by a malicious user

Attack surface – The collection of attack vectors a given device or service is susceptible to.

Attack vector – This is a high level term to cover all kinds of attacks, methodologies and delivery methods

Bring your own device – A trend in organizations, where employees are allowed to use their personal devices to access corporate resources.

Cisco Discovery Protocol – A proprietary protocol that exchanges device information with other Cisco devices.

Cloud enabled attack vector – An attack vector that utilizes cloud computing functionality to perform the attack or phases of an attack

Cloud managed infrastructure – Physical infrastructure hardware (AP, switch, router, or firewall) that is controlled and managed through a cloud service. This term within the paper refers mainly to Meraki devices.

Command and control – Remotely controlling devices / software whether this functionality is built-in or gained through an exploit

Controls – also security controls, physical controls, logical controls – any technology / solution that enforces an organizations written policies

Domain Name Service – Translates named domains (i.e., google.com) to the corresponding Layer 3 IP address.
Dynamic Host Control Protocol – A protocol used to manage and assign IP addressing to hosts. When a host connects to a network it sends out DHCP requests at layer 2, the DHCP server then assigns a layer 3 IP address in the appropriate LAN / VLAN. The host automatically configures its network adapters to gain network access.

Eavesdropping – A passive attack where network traffic is monitored or collected for the purpose of extracting unencrypted data or traffic analysis.

Exploit – An exploit is an attack that takes advantage of a specific vulnerability on target device / software.

File Transfer Protocol – A protocol that facilitates file transfers between two hosts.

Hypertext transfer protocol – A protocol that facilitate communications, commonly used to transfer data.

Hypertext Transfer Protocol secure – A protocol that facilitate secure communications, encrypted HTTP protocol.

Layer 2 – Refers to the data link layer of the OSI model. In this layer of the model data is switched in the form of frames and every communication is broadcast to all devices in the broadcast domain – or LAN segment. Without a router no communication can leave the layer 2 broadcast domain.

Layer 3 – Refers to the network layer of the OSI model. In this layer of the model data is routed in the form of a packet. Routing allows communications between multiple LAN segments

Local Area Network – The network infrastructure and devices that facilitate communications between devices owned or trusted by an organization, at a given site. Traditionally referred to when discussing wired infrastructure.

Malicious user – also malicious attacker, attacker – An individual, internal or external, that has nefarious intentions. Commonly the individual performing an attack.

Media Access Control address – A unique hardware identification number, in the form of six groups of two hexadecimal numbers, assigned at the time of manufacture. The MAC address facilitates layer 2 communications.

Network Access Control – Any technology / solution that provides authentication and authorization functions for users / devices as they attempt to gain network connectivity

Packet capture – refers to the act of recording and creating a file containing network traffic during and eavesdropping attack.

Power over Ethernet – Transmission of electrical current through Ethernet cable to provide power for devices, such as phones or access points.
Social engineering – Social engineering is a type of non-technical attack that focuses on exploiting unknowing individuals into providing sensitive data or perform an activity.

Switch port – A layer 2 port on a switch. For the purpose of this research, switch ports are used to connect RJ45 Ethernet cables between host and switch.

Telnet – A protocol used to manage and administrate infrastructure devices.

Trunk port – An operation mode of a switchport that allows all VLANs to transit. The native VLAN on a trunk does not assign a VLAN identifier, or tag, so the native VLAN is deemed untagged traffic. Any traffic sent without a VLAN tag will be placed on the configured native VLAN.

Virtual Local Area Network – A logical, virtual LAN that resides on a physical LAN. This techniques allows for multiple VLANs to share the same physical resources while maintaining logical separation and segmentation.

Wide Area Network – Traditionally the external, public facing aspect of the network. This includes internet, voice and private line circuits.

Wireless Local Area Network – The network infrastructure that facilitates wireless communications between hosts.
ABSTRACT


The purpose of this directed project and related research was to demonstrate and catalog a new attack vector that utilizes cloud managed infrastructure. Cloud computing is a recent trend that is creating significant hype in the IT sector. Being that cloud computing is a new theme in the computing world, there are many security concerns that remain unknown and unexplored. The product of this directed project provides a documented taxonomy of the new attack vector and how to mitigate risk from this kind of attack.

The new attack vector creates efficiencies throughout the lifecycle of an attack and greatly reduces time and effort for the malicious user; however, efficiencies in time and effort are not the only characteristics of the demonstrated attack vector. This type of attack greatly increases the chance of success and reduces the odds of detection. All of these characteristics culminate to create a tool for the malicious user that is dangerous to every organization in existence.
CHAPTER 1. INTRODUCTION

As new technologies / methodologies are becoming available, security is in a continuous state of evolution. This progression is not always a groundbreaking new exploit. In fact, it can enable a well-versed exploit with a new delivery mechanism, (as is the case for this research). The concepts of command and control and eavesdropping are by no means new to the information security community; however, they are proven and effective. Providing these concepts with a new / innovative delivery method, which places them in the targeted network, and facilitates access to the network is a serious security concern. The ability to perform information gathering from within the target network is the key concept to this attack vector. This research will prove that using cloud managed infrastructure, as a delivery method, is effective and more efficient than the accepted taxonomy of a cyber-attack.

This chapter introduces much of the background information for this directed project and related research by presenting the problem statement and associated research questions. A review of the constraints of the study and defining terms used throughout the study will also be provided within.
1.1 Statement of Problem

With this new attack vector, a malicious user can rapidly perform information gathering to prepare for attack. Once the attacker has gathered the information required, they can gain access to the target network – via cloud managed infrastructure - to launch any number of exploits.

There are many solutions and technologies that can prevent unauthorized devices from accessing a network, such as Network Access Control (NAC). These technologies are scarcely implemented due to cost and complexity. A study of IT professionals indicates two of their biggest concerns regarding Bring Your Own Device (BYOD) is insufficient security controls, management, and visibility. This implies that these organizations currently do not have a means to manage what devices should have access to their network (SANS Institute, 2014).

1.2 Research Questions

This paper is intended to answer the primary research question, as well as additional secondary questions relevant to the study.

1.2.1 Primary

- Can cloud managed infrastructure be used as a hacking tool?
What types of malicious activity can be performed using cloud managed infrastructure?

1.2.2 Secondary

- How does this technology impact the accepted taxonomy of a cyber-attack?
- What can be done to mitigate this newly identified attack vector?

1.3 Scope

The scope of this research was limited to Meraki Access Points (APs), cloud managed infrastructure, which will facilitate the new attack vector. All data sent, received or collected was simulated by the researcher to represent real world traffic - as it would be seen in production environments - as it travels through the network between two hosts. No advanced techniques, analysis, exploits or encryption levels were used for this research as the objective is to prove feasibility of the new attack vector.

1.4 Significance

The significance of this research was to identify a new cloud enabled attack vector and document its taxonomy. This research will be used by security professionals to bolster their organization’s security / risk profile. Additional understanding of how
cloud technologies can be used maliciously will progress the maturity of cloud security as a whole.

1.5 Assumptions

The assumptions for this directed project and surrounding research were as follows:

- Cloud managed infrastructure has already been attached to the target network.
- AP is connected to a Power over Ethernet (PoE) port on Layer 3 switch performing minimal routing.
- The uplink port between switch and AP is enabled and is configured as a Layer 2 trunk.
- No NAC solution is in place.
- Organization’s firewall allows all connections from trusted segments to untrusted segments. At a minimum, port 443 will be allowed outbound from internal network segments.

1.6 Limitations

The following limitations were placed upon the research:

- Research would not have been possible if target organization has sufficient physical / logical security controls in place.
• All results were based off of research performed in a laboratory environment and are assumed to accurately simulate production environments.

• Due to state and federal law, no research was performed on any private, public or commercial entities.

1.7 Delimitations

Several delimiters were placed upon the research, which are as follows:

• Research was limited to proving attack vector utilizing Meraki hardware only.

• Research ceased at the point of launching targeted exploits.

• The research did not attempt breaking encryptions or any other advanced techniques.

• A Meraki MR24 AP, Cisco 1841 router, laptop running Microsoft Windows 8, desktop running Microsoft Windows 7 and a laptop running Kali Linux were used to emulate network traffic and to perform information gathering activities.

• No Social attacks will be performed due to previous assumption that cloud managed infrastructure is already attached to network.
CHAPTER 2. LITERATURE REVIEW

As cloud computing continues to gain in popularity and prevalence, the potential attack surface increases with every service utilized. Cloud security and best practices are still in their infancy and pose a moving target for security professionals. Not only are their security considerations inherent to cloud computing itself, there are also considerations regarding how cloud technologies enable other attack vectors; by increasing the attack surface. No organization is immune to cloud enabled attack vectors, even organizations that do not subscribe to any cloud services.

This chapter provides context to the research throughout this paper. The content of this section was derived either through research / the researcher’s personal experience, work experience or training, which includes access to confidential materials. Specifically, we will discuss the anatomy of malicious attacks, delivery methodologies, several proven attacks, history and functionality of Meraki hardware.

2.1 Anatomy of a Malicious Attack

The SANS Institute defines the anatomy of an attack as summarized below (Cloppert, 2009):
1. Reconnaissance: Performing information gathering to understand architecture and find vulnerabilities.

2. Weaponization: Planning the attack, choosing specific exploits for specific targets

3. Delivery: Delivers packaged exploits created / identified in the Weaponization phase.

4. Compromise: Delivered exploits are executed on targets.

5. C2: Command and Control phase of the attack. Exploit has been executed and infected devices are now communicating with / controlled by malicious individual. Collection and staging of objective for extraction

6. Exfiltration: Extract of target data / information and reducing footprint of exploit to avoid detection.

With regards to the purpose of this research, the two primary phases that will be discussed are reconnaissance and delivery.

2.1.1 Reconnaissance

The reconnaissance phase of the anatomy is the most time consuming aspect of the attack. In the phase significant amounts of time accumulate due to the malicious user having to find and identify vulnerabilities / lack of controls that will allow them to gain technical, non-technical or organizational knowledge on the target. The attacker is looking for anything that will provide insight into architecture, network, host, security policies or human information (USNA, 2015).
2.1.2 Delivery

The delivery phase is characterized by positioning of exploits in desired location. Several common delivery methods currently in use include: Hyper Text Transfer Protocol (HTTP) tampering, drive-by download, code injection, thumb drives and emails containing malicious hyperlinks. Regardless of delivery method, the object is the same, to transport packaged exploits to targets (Cloppert, 2009).

2.2 Common Attack Methodologies

This section will further discuss common attack methodologies that were used as part of this research; eavesdropping, Social Engineering (SE) and Command and Control (C2). These techniques have been in the attacker’s repertoire and have been proven effective time and again. The delivery method used in this research breathes new life into these attacks and ensures their continued longevity.

2.2.1 Eavesdropping

Eavesdropping is a type of passive attack where the malicious user will observe / capture data as it flows through a network. To perform eavesdropping in the most efficient manner, the attacker would ideally have a device attached to the target network. Once that is in place the attacker can perform traffic analysis to gain knowledge about any of the objectives of the reconnaissance phase; architecture, network, host, security
policies or human information. According to The National Institute of Standards and Technology’s (NIST) Special Publication 800-120, through eavesdropping, an adversary can intercept a communication and, thus, access all unprotected information (Hoeper, 2009).

The interception of communications is facilitated by performing a Packet Capture (PCAP), which is a known resource to everyday IT staff and malicious users alike. This is a mature tool / technology with a number of software providers that can perform PCAP and replay the information in the communication. A successful and quick eavesdropping attack can achieve the entirety of the reconnaissance phase goals and limit chance of detection to a marginal amount.

The information gathered will aid the weaponization phase of the attack as the potential targets have been identified and likely profiled. In Special Publication 800-120 NIST details certain attacks that can immediately follow traffic analysis; these are itemized below (Hoeper, 2009).

“Impersonation Attacks, in which an attacker assumes the identity of a legitimate party and attempts to convince a verifier that he is that party. Impersonation attacks are conducted through, but are not limited to, the following methods:

- Masquerading Attacks, in which a party directly claims to be somebody else
• Man-in-the-Middle Attacks, in which an adversary may replay, relay, reflect, interleaving and/or modify messages in one or more protocol executions between two parties to fool at least one of those parties about the identity of the other party;

• Replay Attacks, in which an adversary replays messages from a previously-observed protocol execution;

    Extraction of Authentication Credentials, in which an adversary tries to get information about the long-term authentication credentials.

This can be done through:

• Dictionary Attacks, in which an adversary breaks a weak password and uses it in subsequent sessions;

• Chosen-Text Attacks, in which an adversary strategically chooses challenges in an attempt to extract information about the claimant’s long-term credentials.

    It can be observed that impersonation attacks can be conducted at the protocol level (e.g. man-in-the-middle attacks) and/or at the cryptographic level (e.g. extraction of authentication credentials).

• Key Extraction Attacks, in which an adversary obtains secret keying material by manipulating or breaking the employed key establishment scheme.”
2.2.2 Social Engineering (SE)

SE is an attack that is aimed at the people aspect of an organization's security policy. The definition of SE is put quite eloquently in the SANS Institute’s SE white paper; Social Engineering: A Means To Violate A Computer System (Allen, 2006).

“Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible.”

SE attacks are hugely successful in comparison to other techniques used to acquire sensitive / critical information. So successful in fact that SE has been coined ‘the largest threat to organizations’ (PRWeb, 2014). Additionally, researchers indicate there is a 100% success rate in penetration testing when SE techniques are employed (Lambert, 2013).
2.2.3 Command and Control (C2)

Not only is C2 a phase in the accepted taxonomy of a cyber-attack, it is also a form of attack as well. C2 attacks allow a malicious user to operate devices / software remotely. This method gives the attacker the ability to perform any activities the device / software is capable of within the target network, at their discretion. With regard to the research at hand, the researcher will be using C2 functionality – via cloud managed infrastructure and Meraki’s cloud based controller.

Traditionally, C2 attacks were performed utilizing Internet relay chat protocol however, this method allowed for easy detection and identification of infected hosts and attacker information. Several new methods are becoming popular including HTTP, HTTPS, peer to peer and social networking. These new methods add a layer of obfuscation to the attack that makes the communication streams between command source and infected host indistinguishable from normal traffic on the network (Stephens, 2010).

2.3 Meraki: Cloud Managed Infrastructure

Meraki is the leader in cloud managed networks, with wireless, switching, security, and mobile device management products built from the ground up, to be managed via the cloud. The company grew out of an MIT project called Roofnet, which
was started by two students; Sanjit Biswas and John Bicket. Roofnet was intended to provide a scalable, cloud managed wireless solution to the city of Cambridge.

2.3.1 History

Meraki, as a company, was founded in 2006 by the original two MIT students in collaboration with Hans Robertson. Google and Sequoia Capital funded the company’s creation. Meraki, from its inception has boasted significant levels of growth, at two to three percent per year. It didn’t take long for them to get noticed, and in 2012 Meraki was acquired by Cisco. Meraki, while maintaining its name and product has additionally become the Cisco Cloud Network Group (Meraki, 2015).

Meraki is known for their simple and easy to use out of band cloud management architecture that lets you monitor, configure and control your network from anywhere in the world. Management of your networks is done through the ‘dashboard.’ The dashboard is Meraki’s representation of the controller, which is accessed through the cloud portal: dashboard.meraki.com.

Meraki has gone through many changes as the company has matured. Up until February 2008, when they updated their End User License Agreement (EULA), Meraki was a hacker friendly company. The product was built using open source technologies and they had no issue with end users putting their own software / firmware on the
hardware. With the updated EULA, Meraki forbid using any software other than Meraki’s OS and locked down the hardware to prevent such actions (Gearhart, 2008).

2.3.2 Meraki Functionality

Meraki has custom built their hardware and software with one driving principal, simplicity. They boiled down all of their advanced configuration details and feature sets to a couple checkboxes and radio buttons, all without any loss of major functionality. This section will reveal how the Meraki hardware operates and will perform in the laboratory.

When you receive a Meraki AP, switch or firewall the first thing to do is to connect it to the internet. Plug the AP into a Power over Ethernet (PoE) switch, the AP gets an IP address from Dynamic Host Control Protocol (DHCP). At this point the cloud managed infrastructure attempts to reach the cloud based controller. Once communications with the cloud based controller is established, the hardware then checks for any updates that are available. If an update is available, it will be downloaded, installed and rebooted. If no update is needed, or after the reboot, the AP connects to the cloud controller and downloads the current configuration. From that point forward, the device is able to be remotely controlled through cloud management feature. The dashboard comes standard with live troubleshooting tools and 1-2 minutes delay in configuration changes.
The device communicates with the dashboard through HTTPS. This traffic is rarely blocked by firewalls or access-lists due to the prevalence of the protocol. Nearly every networked device uses HTTPS to communicate with the Internet, so the traffic is deemed safe and generally does not draw much attention. Many firewalls permit traffic from more secure zones (internal networks) to less secure zones (external networks) as default out of the box behavior. However, in the scenario where an organization has very tight access controls and locks down outbound traffic, there is a chance that the communications would not be permitted.

Meraki’s out of the box AP functionality level is, compared to competitors, in a class of its own. Once logged into the dashboard, and administrator would immediately have access to live troubleshooting tools such as PCAP, ping, trace route, throughput and wired VLAN monitoring – DNS, ARP, and DHCP – as well as location analytics, layer 3 / 7 firewall, traffic analytics, host identification, topology and RF spectrum monitoring. All of these features are present in the dashboard. The dashboard is also what facilitates the C2 component of cloud enabled infrastructure, being that commands / configurations are given to the commander - dashboard - and those commands are propagated to the infrastructure under its control.

Meraki makes configuration of APs relatively simple, and in that simplicity lies an unintended source of obfuscation for the attacker. Default behavior of the APs are such that the AP is placed into the VLAN of the connected switch port. The AP receives and IP address from a DHCP server, but provides DHCP services out to clients
associating to the device; this is called Meraki DHCP. The address an associated client will receive is a random IP address in a unique 10.0.0.0 /8 network. When the associated client communicates through the AP, the client’s IP address is NAT’d to the IP address of the Meraki AP. With this configuration all associated clients’ communications appear to be coming from the Meraki device itself. This can limit an IT staff’s visibility into specific client’s activity. Again, this is out of the box functionality, different parameters exist to suit the needs of an organization.

It is also important to understand how the different types of traffic flow through the LAN / WAN. The two types of traffic being referred to are the control / management plane and the data plane. The control and management plane will carry configurations, statistics and monitoring information. The data plane carries all user traffic. In the Meraki model, the control and management plane data is sent encrypted to the cloud while the data plane is forwarded out to its intended destination. Figure 1 below represents this graphically (Meraki, 2015).
2.4 Summary

This chapter has discussed the critical concepts and methodologies used throughout this research. The accepted taxonomy of a cyber-attack was detailed to provide a reference point of how this taxonomy changes using the cloud enabled attack vector discussed later in the paper. Background information on the various types of proven attack methods that will be utilized in the research was provided. Finally, insight into the history of Meraki and how their cloud managed infrastructure operates was touched upon. This section lays the foundation of knowledge used throughout the rest of this paper.
CHAPTER 3. PROCEDURE

This section details the methodology, phases and steps used to perform the research for this directed project. To fully understand the impact to the SANS Institutes’ anatomy of an attack, each step of the procedure followed the six phases as identified in Chapter 2. The objective of each phase was relative to its given function. The actions that were taken in each phase of the new cloud enabled attack vector will be revealed as it is discussed through this chapter. Any process or function of a phase that was not performed, with regard to assumptions and scope will be discussed. The phases of this experiment were:

1. Phase 1 reconnaissance: Gain physical access or perform SE to get Meraki hardware attached to target network. Use Meraki’s cloud managed infrastructure, C2 functionality, to acquire as much data as possible.

2. Phase 2 weaponization: Determine high value targets and prepare packaged exploits such that the exploit lines up with the information from previous phase, such as: operating system, services, patch levels or vulnerabilities.

3. Phase 3 delivery: Enable delivery method. Use Meraki dashboard’s C2 functionality to change AP configuration, enabling an SSID, facilitating direct network access for attacker.
4. Phase 4 compromise: Packaged exploits deployed and targets compromised

5. Phase 5 C2: Either use C2 as in reconnaissance or delivery phases to facilitate staging of attack objective, or use C2 in the traditional sense on infected targets of the compromise phase.

6. Phase 6 exfiltration: Export objective of attack, retrieve Meraki AP and cover / obfuscate evidence of the attack.

3.1 Reconnaissance

In the lab environment there were three VLANs to demonstrate information gathering capabilities across logically separated networks. VLAN assignments were determined at random with no logical foundation. All of devices were connected to a trunk ports with the native VLAN being that of the host; with the exception of layer 3 routed ports. The cloud managed AP was attached to the network with all radios disabled and the Ethernet interface enabled.

Once the Attack AP was communicating with the dashboard the researcher simulated network traffic; Telnet, FTP and HTTP. These communication flows were collected by the attack laptop, using the PCAP functionality of Meraki AP and dashboard. These communications were analyzed using Wireshark to extract unencrypted data.
For the intent and purpose of this research it was assumed that infiltration and placement of Meraki hardware on target network to have already taken place. While the AP was sitting on the target network in stealth, the dashboard’s troubleshooting tools were used to gather information pertaining to the network and its host. Immediately after obtaining a DHCP lease network information such as default gateway, subnet, LAN / WAN IP addressing and CDP information became available to the researcher. Additionally, Meraki APs monitor the status of DHCP, DNS and ARP requests on every VLAN that is visible.

Connecting the cloud managed infrastructure into a trunk port allowed it to obtain and monitor all active VLAN information seen. Additional network information was determined using the built in tools: PCAP, ping, trace route and access to the ARP table. Wireshark was used to capture, extract and playback data collected from PCAPs, providing the researcher with access to any unencrypted data.

Several scenarios exist where a malicious user could potentially attach cloud managed infrastructure on the target network; they are as follows:

- Social engineering
- Insider attack
- Poor facility / physical security
Due to the overwhelming success rate of SE alone, claimed to be 100% effective, it was assumed that almost any external party would be able to attach cloud managed hardware on the target network if they had the resolve. If not through use of SE, an external party can still gain access to a facility through poor physical security controls. These two approaches require very little technical skill and rely on the lack of physical / logical controls.

Nearly all barriers faced by an external party are removed in the inside attacker scenario, as these individuals would be an employee or contractor, and have authorization to the building and network. Additionally, it was assumed that a hardwired Ethernet connection is provided in their workspace. Logical security would be the obstacle for the inside attacker to overcome. We have a great example of the inside attacker in Edward Snowden. Snowden was not an employee of the NSA; rather he consulted for them while with Dell and Booz Allen Hamilton. Despite not being an NSA employee he was given sweeping authorizations to their systems and infrastructure. He did not like what the NSA was doing so he abused those authorizations and went public with many classified documents (Poitras, 2015).

3.2 Weaponization

Weaponization is the next phase in the SANS Institutes’ anatomy. No actions were taken by the researcher in this phase due to scope. It is in this phase that the information gathered from the cloud managed hardware will be put to use. Specific
exploits will be paired and packaged to a specific target. The pairing of the exploit to target and overall success is directly influenced by the quality of information gained in the previous phase.

At this point the AP was still configured with its radio interfaces disabled to maintain anonymity. A mildly skilled attacker should be able to complete the weaponization phase through the use of free, ethical hacking tools. MetaSploit, a software with massive libraries of exploits, could be used to package exploits to specific vulnerabilities, assuming the attacker has identified vulnerabilities on the target.

Now that the malicious user had a strong understanding of the network topology, has identified targets and prepackaged exploits, they can begin the delivery phase.

3.3 Delivery

The delivery methodology will be utilized in this phase to transport packaged exploits to their target. In the case of this research, the delivery method revolves around the C2 functionality of cloud managed infrastructure. The researcher enabled the delivery method by configuring a WLAN that was broadcast by the Meraki AP. The attacker connected to the WLAN which provided direct network access, bypassing hardened perimeter, to deliver exploits.
Depending on the facility and AP location, this does not require physical access to the facility. Through the use of custom antennae the attacker can increase the maximum distance from the facility. Once all payloads were delivered, the researcher disabled the WLAN so as not to draw any unnecessary attention.

3.4 **Compromise**

This phase was not performed by the researcher as it is outside of the established scope. The compromise phase is the point where the targeted exploits and malicious software would be deployed within the target ecosystem. Whether these exploits or software are meant to take down target resource, install malware, infect more hosts for additional C2 resources or steal personal / intellectual property is of no relevance to this research as the goal of each cyber-attack is dependent upon the attacker’s objective.

3.5 **C2**

The researcher took no action during this phase. With regard to the taxonomy, this phase would have require the use of C2 to control hosts infected during the compromise phase. With the proposed cloud enabled attack vector, the C2 phase may be unnecessary if objectives have already been collected.
3.6 Exfiltration

The exfiltration phase was also outside the scope of what was performed in the research. There are still several things that need accomplished in this phase. Extraction of attack objective is the critical component in this phase. In the research scenario this was a data transfer between hosts, utilizing attack AP’s WLAN. The secondary objectives of this phase were to cover the tracks of the attack. Removal of the AP was the primary focus and should likely be able to be performed in the same fashion as attaching it to the network. In general, eliminating the digital fingerprint of the attack would be dependent upon what exploits were used.
CHAPTER 4. RESULTS

This chapter contains the results from research performed using the procedure discussed in Chapter 3. In addition to the findings, this chapter will also discuss several caveats identified with performing research.

4.1 Findings

The findings from the research represent proof of the proposed hypothesis and appropriately answer the posed research questions. Meraki’s cloud managed hardware can be used as an efficient tool in the hacker’s repertoire. Not only does the cloud managed infrastructure enable discrete, advanced information gathering in a fraction of the time, it also facilitates a means to gain access to the target network to launch any exploit desired; all with ease. To add insult to injury, the AP provides some level of obfuscation to the attack and limits chance of detection by extracting data over LAN / WLAN instead of utilizing WAN.

Figure 4-1 below depicts the lab architecture, IP addressing and VLAN infrastructure as used through the research and will be referenced throughout this chapter.
4.1.1 Reconnaissance

For this phase of the attack the Meraki MR24 attack AP was connected to a trunk port on a layer 3 switch. The configuration for the port was left at the factory default; trunk port with VLAN 1 native. Device configurations are attached in the Appendices. Where the AP is attached to the network makes a difference as to the information that could be collected. This will be further discussed in the Caveats section at the end of this chapter. For the sake of the research, the attack AP was connected in the ideal location as depicted in the Figures.
In the reconnaissance phase, the researcher simulated the flow of information across the network and used the Meraki AP / dashboard to perform PCAPs. The researcher triggered telnet, FTP and HTTP communications, all of which were successfully collected by the PCAP. The sensitive data contained in these captures was extracted using WireShark.

4.1.1.1 Telnet Communications

Figure 4-2 below shows telnet communication flows and Figure 4-3 depicts the extracted telnet data in Wireshark. Microsoft’s built in telnet client was used on the Windows 8 laptop to facilitate the telnet session. The blue text is data sent from router to host and red texts is data from host to router. Not only did this passive attack capture administrator credentials to the device, it also collected the configuration of the router in its entirety.
Figure 4-2: Simulated Telnet Traffic

Figure 4-3: WireShark Telnet Data Extraction
4.1.1.2 FTP Communications

Figure 4-4 and 4-5, below, depict the capture of sensitive FTP data. FileZilla FTP server was installed on the Windows 8 laptop and facilitated the file transfer. Figure 4-4 shows the data’s path through the network while Figure 4-5 displays the sensitive data extracted via WireShark. The same router and host that were used to simulate Telnet traffic were again used to simulate FTP traffic. Again, we capture credentials that allow access to the FTP server, specific product, version and files that are being transferred. In this example the transfer fails, but that is irrelevant as the sensitive data was collected.
4.1.1.3 HTTP Communications

The final sensitive information collection performed was HTTP traffic. For this scenario an IIS webserver was enabled on the Windows 8 laptop with directory browsing open to everyone with read / write permissions. This was configured to facilitate file transfers via HTTP protocol. No authentication was configured on the service.

Figure 4-6, 4-7 and 4-8 depict the traffic flow and data extraction for this exercise. The packet capture collected all data transferred, figure 4-7. Copying that data into a notepad and saving with an .html extension allowed the researcher to see the webpage as
the user would have experienced it, figure 4-8. This again enabled the researcher to not only know it was unauthenticated, but also revealed the directory structure of the host.

Figure 4-6: Simulated HTTP Traffic

Figure 4-7: WireShark HTTP Data Extraction
4.1.2 Weaponization

Moving into the weaponization phase of the attack, the researcher has already amassed a very substantial amount actionable intelligence. Despite not having performed any analysis or exploits as a part of this research, it is apparent how the researcher could use this information.

Outside of the sensitive data discussed in the reconnaissance section, the researcher is also aware of what products and versions are offering services. That information by itself is enough for the researcher to line up and narrow exploits to a much smaller selection. Access to several file directories in the network is also available if the attack objective is intellectual property. In addition to the more advanced exploits, the researcher also has a wealth of layer 2 information from the packet captures that would facilitate all of the attacks discussed in Section 2.1.1.
4.1.3 Delivery

Assuming the researcher had the output of the weaponization phase, exploits packaged and ready for distribution, getting the exploits to the target devices would be the result of this phase. Fortunately, the C2 nature of Meraki APs makes this feat very simple. The researcher enabled a WLAN on the attack AP to allow direct network access without having to gain physical access to the facility.

One defining characteristic of this attack vector is bypassing the WAN for delivery, instead delivering via LAN / WLAN. This component further reduces chances of detection as traffic will not be transferred through edge devices. Traditionally, Intrusion Prevention System (IPS) technologies and other monitoring / reporting solutions either live or have a sensor on perimeter devices. Delivery via this method would allow for the use of exploits that might normally be blocked by an IPS due to its attack signature being identified.

4.1.4 Compromise

No actions were performed by the researcher for this phase due to scope. This phase is assumed to be relatively unaffected, in function, by the methodology of the new attack vector.
The compromise phase would take place immediately after delivery phase was completed. At this point, the researcher has unhindered network access and can associate any number of devices to the attack AP. These devices would be implementing the exploits that were identified in the weaponization phase. Once the exploits were completed, the network access was terminated.

4.1.5 C2

This phase was also out of scope to the research. With respect to the new attack vector this phase may not even be necessary. Since this attack vector allows for direct network access, a slave device might not be needed if objectives can be accomplished in delivery / compromise phases. If more advanced techniques were being used, researcher would be controlling newly infected machines to stage objective of the attack for extraction in the next phase.

4.1.6 Exfiltration

To begin this phase, the researcher enabled and connected to the WLAN on the attack AP. Network access was used to extract attack objectives. After successful extraction of data, the next step was to retract the attack AP from the facility. If building security is lax there shouldn’t be an issue returning to collect the device. The company won’t be aware of the exploits for some time, so they will remain blissfully ignorant of the situation with no reason for suspicion. If the SE approach was used, then a follow up
SE attack with the same individual could be used to have the exploited individual remove the AP and ship it back.

4.2 Caveats

There are several caveats that came to light through the research and laboratory exercises that are important to note. First and foremost, attaching an attack AP to a network does not guarantee the results of this research. Secondly, there are some pitfalls in the reconnaissance phase and some precautionary steps that should be executed to increase the chance of a successful infiltration.

4.2.1 Successful Reconnaissance Phase

It is important to note that the overall success of the attack is based upon getting the AP attached to the appropriate device in the infrastructure. This can be a difficult task as a malicious outsider would be connecting the AP to a network drop somewhere in the office space with no knowledge of where the drop is terminated. If the AP is attached directly to a layer 2 device a packet capture will provide only layer 2 level information. While this would still provide a wealth of knowledge, it does not provide any insight into the layer 3 data flows, where truly sensitive / personal data can be obtained.
4.2.1.1 Attack AP Location

Ideally, the AP should be attached to the core layer 3 switch, performing routing. As previously stated, there is no guarantee where the AP is being attached if you do not have access to the networking closet or knowledge of network drop termination. While this seems like a relatively significant pitfall there are several trends and technologies the researcher has observed in the field that will increase the likelihood of attaining an agreeable point of attachment. These enabling trends and technologies revolve around virtual switch stacks, large switch chassis with multiple switch blades and route processors as well the tendency of organizations to put PoE switches in place as the core. Additionally targeting a smaller offices or satellites would likely prove more successful than larger offices.

Switch stacks and large switch chassis increase the likelihood of finding an appropriate place to attach an Attack AP. These large chassis and stacks greatly reduce network administration by having one logical device, in the case of switch stacks, or a multitude of blades in a chassis managed by a supervisor blade. In these types of deployments were each IDF services a large number of clients, it would be beneficial to network performance to route traffic at layer 3 between MDF and IDFs instead of layer 2 switching. This increases the number of broadcast domains and limits the propagation of layer 2 broadcasts to areas in the network where they logically make sense.
4.2.1.2 Mitigating Failure

There are several considerations that can increase the chances of having a successful attack. To mitigate the risk of failure due to attaching to the attack AP to a non-PoE port, the attacker would either have a power adapter on their person - if they were to exploit physical security - or provide it with the AP in the SE approach. This precognition can prevent a scenario where the attacker cannot find a PoE port and avoid drawing unneeded attention to themselves as they wander around the office space looking for one.

Additionally, the researcher believes that smaller offices would make better targets as it is more likely that they would be supported through a single network closet and the equipment would be a PoE capable switch. It is also assumed that this single switch / stack would be layer 3, rather than layer 2, to support future growth and general flexibility.
CHAPTER 5. CONCLUSION

In summation of this research, and answering the primary research questions; yes, a Meraki AP is a very useful, efficient hacking tool capable of passive information gathering attacks and enabling on demand delivery methods. As cloud technologies improve efficiencies and streamline IT as a whole for organizations, it will offer those same benefits to nefarious individuals. With minimal effort and time, massive amounts of relevant information can be gathered in near real time from within a – traditionally - trusted security zone. Collecting information from within the internal network provides a better opportunity for the attacker to collect sensitive data, as there is less security controls in place. This research also provided plentiful insight into the secondary research questions as well which will be discussed in the following sections.

5.1 Impact on Taxonomy

The first secondary research question asks what the impact to the generally accepted taxonomy of a cyber-attack would be. While the taxonomy of the cloud enabled cyber-attack has many similar characteristics there are several glaring differences between the two and some blending of separation between phases. The amount of time and effort a malicious user would expend in the reconnaissance phase and performing
traffic analysis will be reduced significantly as well as provide better results. The researcher predicts the amount of time and effort would be halved, at a minimum. Also, the new delivery methodology increases the likelihood of success.

This reduction of effort / time is a byproduct of the answers to the two primary research questions in addition to relying on SE to facilitate the reconnaissance phase. As discussed previously, SE is incredibly successful and should not take long to get the attack AP attached to the internal network. Once the device is behind the hardened network perimeter the potential for a successful attack increases significantly. This increase is expected for two reasons; the device is in a trusted zone as stated, and there is less of a chance to be detected in one of the early phases. If an organization is only concerned with monitoring their perimeter, this new attack vector would essentially put the attacker in their blind spot; this is especially true regarding delivery / compromise / exfiltration phases.

5.2 Mitigation Techniques

Addressing the final Research Question regarding prevention of this newly identified attack vector, mitigation of this attack vector to a marginal level is entirely possible. However, it would be a costly and time intensive endeavor. The best way to prevent this attack vector, and many others, is through the utilization of a Network Access Control (NAC) solution.
5.2.1 NAC

This type of solution would require authentication and authorization in the form of directory lookup / credential verification, Certificates or MAC address. While these methods are not 100% effective the researcher would argue that the solution is proficient enough to stop all but a truly educated, determined attacker.

Not only would a NAC solution protect from a malicious external party it would also provide protection from a malicious insider. With the prevalence of BYOD and insider attacks it should be argued that every organization implement stringent security policies in addition to NAC. There are still ways to bypass a NAC solution. For example, if a malicious insider was aware of the NAC solution, collecting a MAC address and spoofing that MAC is trivial. Acquiring credentials or certificate fraud would allow you to masquerade as an authorized individual. However, if there is a security policy enforced by NAC to limit access to network resources as required, the impact of this kind of attack can be mitigated.

5.2.2 Best Practices

Outside of a large project to implement a NAC solution, simply following industry best practices can successfully mitigate the risk to a lower level. Several of these concepts include disabling unused switch ports, using an unused VLAN as the
native for trunk ports, disabling plain text communications and services would also be an effective deterrent.

5.2.3 Block Communications

In the case of Meraki there is another method that could be employed. If there is no Meraki equipment in your network, simply blocking traffic destined to the Meraki cloud would be effective. However, this methodology applies only to the specific cloud enabled attack vector identified in this work. This approach would likely not be feasible for larger, more widely used cloud providers such as Amazon or Microsoft’s cloud offering. Blocking traffic to these destinations could have an unintended impact upon your employees and business applications that tie into these clouds.

5.3 Future Work

Through the course of the research we have demonstrated the power and resourcefulness of Meraki’s dashboard. Compromised dashboard credentials should be a serious concern for any organization that currently has Meraki infrastructure deployed in their networks. While Meraki does have two factor authentication, in practice this is poorly adopted. If a malicious user were able to gain access to an organization’s dashboard they would be able to execute the attack vector laid out in this paper. In addition, this would bypass any NAC solution in place, there is even less chance of detection and access to a wealth of additional data not available to the researcher in this
paper. Besides SE, is it possible for an attacker to compromise an organization’s dashboard? Several concepts appear feasible, including: proxy attack, session hijacking, man in the browser or an exploit against Meraki’s infrastructure.

Following a similar procedure for this research, is it possible to run an evil Twin or captive portal type of attack during the reconnaissance phase to gather credentials. Meraki does have captive portal and 802.1x authentication functionality. The ability to implement these types of attacks into the reconnaissance phase would increase the likelihood of achieving objectives of the attack.
REFERENCES
REFERENCES


APPENDICES
HACK-ME#sh run
Building configuration...

Current configuration : 1728 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname HACK-ME
!
boot-start-marker
boot-end-marker
!
! aaa new-model
!
! aaa authentication login LOGIN local
aaa authorization exec default local if-authenticated
!
aaa session-id common
!
resource policy
!
ip cef
!
!
ip dhcp use vrf connected
!
ip dhcp pool LAB-DATA
    network 172.16.0.0 255.255.255.0
dns-server 4.2.2.1 8.8.8.8
default-router 172.16.0.1
!
ip dhcp pool MGMT-NET
    network 10.0.0.0 255.255.255.0
dns-server 4.2.2.1 8.8.8.8
default-router 10.0.0.1
!
ip dhcp pool LAB-VOICE
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 4.2.2.1 8.8.8.8
!
!
ip domain name LAB.LCL
!
!
username rjasper privilege 15 secret 5 $1STKqH$PLTw9/SdQELWBXPxQIWca.
!
!
!
!
interface FastEthernet0/0
  ip address 10.255.255.253 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
  no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.1
  encapsulation dot1Q 1 native
  ip address 10.0.0.1 255.255.255.0
!
interface FastEthernet0/1.2
  encapsulation dot1Q 2
  ip address 172.16.0.1 255.255.255.0
!
interface FastEthernet0/1.3
  encapsulation dot1Q 3
  ip address 192.168.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.255.255.254
!
ip http server
ip http authentication local
no ip http secure-server
!
access-list 1 permit 10.0.0.0 0.0.0.255
access-list 1 deny any
!
!
!
!
control-plane
!
!
!
!
line con 0
line aux 0
line vty 0 4
  access-class 1 in
  transport input all
line vty 5 15
  access-class 1 in
  transport input all
!
scheduler allocate 20000 1000
end
APPENDIX B. MERAKI DASHBOARD: ATTACKER CONFIGURATIONS AND
PACKET CAPTURE

Figure 5.3-1: Attack AP WLAN Availability in Reconnaissance Phase

Table: SSID Availability

<table>
<thead>
<tr>
<th>SSID</th>
<th>Visibility</th>
<th>Per-AP availability</th>
<th>Scheduled availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>HACK-ACCESS (disabled)</td>
<td>Advertise this SSID publicly</td>
<td>This SSID is enabled on some APs...</td>
<td>disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Only enable on APs with any of the following tags:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MALICIOUS X</td>
<td>1 AP matched</td>
</tr>
</tbody>
</table>

Figure 5.3-2: Attack AP WLAN Configuration in Reconnaissance Phase
Figure 5.3-3: Wired PCAP From Attack AP in Reconnaissance Phase
APPENDIX C. MERAKI DASHBOARD: LAB CONFIGURATIONS

Figure 5.3-1: Meraki MS220 Layer 2 Switch Switchport Configuration

Figure 5.3-2: Meraki MX64 VLAN, routing and Switchport Configuration
VITA
VITA

PROFESSIONAL EXPERIENCE

Netrix LLC  Chicago, IL  July 2012 - Current

Senior Security and Wireless Engineer

- Presales engineer: Worked with sales team and clients / prospects to engage / discuss / sell / identify opportunities regarding Meraki hardware; created 30+ BoMs, proposals and SoWs
- Lead engineer: Designed, deployed, assessed and maintained Cisco NGFW with Firepower IPS module and FireSight management console for three separate clients; two medium sized organizations in healthcare and one SMB client in manufacturing
- Lead engineer: Designed, deployed, assessed and maintained Cisco ASA firewall infrastructures for more than 15 separate clients of varying size; high availability, IPsec, SSL, AnyConnect, client VPN, site-to-site VPN, NAT / PAT, DMZ
- Lead engineer: Designed, deployed, assessed and maintained Meraki infrastructure for 11 clients: Meraki APs, L2 / L3 switches, firewalls, system manager enterprise MDM
- Lead engineer: Designed, deployed, assessed and maintained Cisco Identity Service Engine (1.0 – 1.3) for five separate clients; one enterprise holding company, three medium sized organizations – healthcare and banking and one SMB client in manufacturing; 802.1x, authentication, authorization, MAB, profiling and posturing for wired, wireless and VPN
- Lead engineer: Designed, deployed, assessed and maintained Cisco wireless solutions for over 13 separate clients across many verticals including: education, finance, manufacturing, professional services, service providers / resellers, residential, commercial residential and government. Solutions included performing pre / post site survey, creating predictive heatmaps, AireOS controllers, IOS XE controllers, Meraki, Prime Infrastructure (1.0 – 2.1), Mobility Service Engine, Cisco Wireless Control System, standalone APs, outdoors, external antennae, voice, video, 802.11b/g/n/a/ac, WEP / WPA / WPA2 PSK / enterprise, 802.1x integration, PEAP, EAP-TLS, flexconnect, one-to-one, BYOD, captive portal and single SSID
- Lead engineer: Performed risk assessment for one medium sized client in healthcare. Categorized and ranked recommendations from auditors by level of
risk, and created strategic roadmap to for initiatives to address these recommendations

- Performed evaluation and assessment of top SIEM solutions (Splunk, HP Arcsight, Juniper Secure Analytics); designed, implemented and maintained Splunk
- Performed assessment, designed, implemented and maintained new network architecture to provide network segmentation
- Performed assessment, designed, implemented and maintained Cisco Prime LMS (4.2) to monitor, audit, compliance and reporting for network infrastructure
- Performed assessment, generated proposal and executed for staff augmentation to maintain new technologies and perform analysis / tuning of reported data
- Performed maintenance and analysis on Websense Triton DLP, web and email modules

- **Lead engineer:** Performed, analyzed and reported upon internal / external Nessus vulnerability scans for 30+ clients across many verticals – perform at minimum 10 scans quarterly; identification of vulnerabilities, action steps to close vulnerability and identification of day zero exploits (heartbleed, bashbug)

- **Lead engineer:** Designed, deployed, assessed and maintained Cisco routing and switching infrastructure for 40+ clients of varying size and verticals; L2 / L3, IP, routing protocols (BGP, EIGRP, OSPF, RIP), access-lists, route-maps, policy based routing, static routing, IP SLAs, DMVPN, 802.1q, trunking, spanning-tree, switch ports, routed ports, VTP

- **Lead engineer:** Designed, deployed, assessed and maintained circuit migration projects for many clients; planning, NAT, DNS, rDNS, E-mail, test & turnup, sizing, readiness, solution specific projects (O365)

- **Support engineer:** Performed maintenance, operational and provisioning tasks within ISP / SP core network infrastructure that provides fiber, T1, T3, MPLS, SIP, managed VoIP and cloud circuits / services to over 80 clients in 200+ distinct locations
  - Provisioned, deployed and turned-up 50+ PE routers / circuits
  - Migrated ISP client (40+ locations) DMVPN routing from EIGRP to BGP
  - Routine maintenance, upgrades, cross connects

- **Training resources:** Attended manufacturer training events (or used my working knowledge) and in turn performed training within Netrix to other engineers: wireless site survey, predictive heat maps, Cisco on-prem WLC design / deployments, Meraki infrastructure (firewall, switch, AP, SME), CCNA, CCNA Security, CCNA Wireless, Juniper DDoS, Juniper Web App Secure
PROFESSIONAL DEVELOPMENT

Certifications

Cisco

- 300-206 Security CCNA
- 500-265 Advanced Security Architecture System Engineer Representative
- 500-451 Unified Access Representative
- 640-554 IOS Network Security
- 650-621 Advanced Wireless lifecycle
- 642-732 Wireless site survey
- 640-722 Wireless CCNA
- 640-802 CCNA

Meraki

- Cisco Meraki Network Associate
- Cisco Meraki Network Professional

Training

Cisco

- Cisco unified access bootcamp: Three day session covering wireless converged access model, flexconnect mobility anchor, mobility controller, mobility oracle, Prime, ISE, IOS XE / AireOS controllers, 3850 switch / WLC and Catalyst 4500 E
- Network as a sensor: One day session regarding utilizing netflow data and feeding the flows into LANcope, making every host sensor
- Content security bootcamp: Three day session covering ESA, Ironport, CWS, ScanSafe and SourceFire AMP integration
- TrustSec and ASA clustering: Full day hands lab via webex. Configured ASAs in a cluster, configured ISE, ASA and switches to allow for TrustSec protocol to be used; writing ACL by AD membership rather than IP address
- Numerous voice of the engineer hour / two hour Webex sessions discussing new technologies in security, wireless and route / switch

Meraki

- CMNA: Full day hands on lab with Meraki instructors. Configured every product family Meraki offers as well as all the features
CMNP - Meraki Master’s Program #24 10/2014: Five day training at Meraki headquarters. Pilot / test group for Meraki’s developing certification path. Lectures and discussions with every area of their organization from tech support to CEO and everyone in between. Lectures included in detail discussion of how the hardware operates and access to Meraki confidential materials. As a Meraki Master we are also expected to train our organization as well as beta test new Meraki code and hardware. In addition to the technical deep dive, we were also trained on how to perform presales and must attend a monthly Master’s training session.

Juniper

JWAS and JDDoS: Three day training session with Juniper trainer, lecture and hands on lab with Juniper Web App Secure and Juniper DDoS product.

EDUCATION

Master of Science – Information Security
Purdue University West Lafayette, IN May 2015

Bachelor of Science – Network Engineering Technology
Purdue University West Lafayette, IN May 2010