**Module 12 Assignment**

Tylor Underwood

Penetration Testing

Professor Nicholas Oles

June 4, 2022

**Executive Summary**

The Happy Accident Labs penetration began with some simple reconnaissance. The internet can be used to find a lot of information about HAL that is publicly available. This includes email addresses, the location of the offices, and more. From there the next step was to infiltrate the network which was done by cracking the WiFi password. The WPA connection was unencrypted making it easy to get a hash of the password which was then cracked using Aircrack-ng with a dictionary attack. From there, the network was scanned for possible vulnerabilities and a very severe one was discovered. SMB vulnerability MS17-010 was open for exploitation on an unpatched system. This is an extremely severe vulnerability that essentially allows the tester to have full control over the system. With this control, the penetration tester was able to install a backdoor into the system for later use. Unfortunately, the test concludes that the network is vulnerable to cyber-attacks.

**Findings**

**Week 2: Open-Source Intelligence**

**Definition of vulnerability:** Using Open-Source Intelligence it is easy to scroll through publicly available webpages to find information on the company that can be used in an attack

**Root cause of vulnerability:** The posting of unnecessary information on publicly available websites

**Proof of concept, description of method used, screenshot, data gathered:**

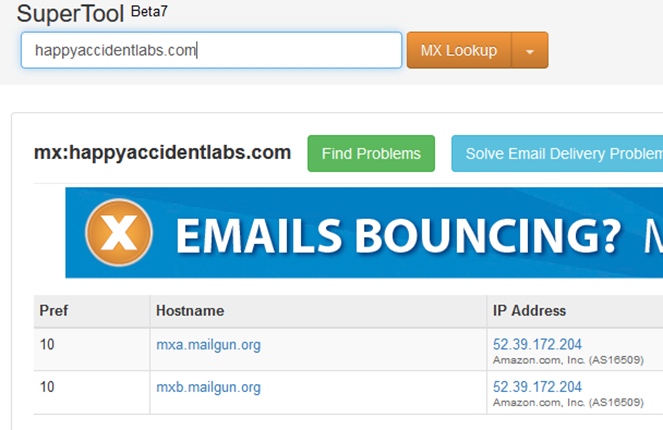
The information gathered was gathered using the internet and is publicly available

Domain Name Information

Graphical user interface, text, application, chat or text message

Description automatically generated

Email Provider



Point of contact

* Sarah Russel
* [russells@happyaccidentlabs.com](mailto:russells@happyaccidentlabs.com)

Address

* 222 S. 15th St, Omaha NE

Other Information

In need of a systems administrator

* Use PFSense Firewalls
* Website developed using Wordpress
* Use of Filesharing

**Likelihood, how easy to exploit vulnerability, the exploit publicly available, does it require physical/WAN/LAN:** very likely, very easy to exploit, publicly available, only requires an internet connection

**Access, is it repeatable:** easy to access and very repeatable (only need internet connection and basic knowledge on browsing the internet)

**Resultant risk:** An attacker can gather data using information gathering to use in the creation of an advanced and targeted attack

**Recommendation for mitigation:** Go through all of the web servers and other associated sites that have information on the company that is publicly available and remove the information that is not necessary

**Week 3: Cracking the WiFi Password**

**Definition of vulnerability:** Is possible to capture WPA information and crack using a password crackers such as aircrack-ng

**Root cause of vulnerability:** The handshake is unencrypted and the password used is not strong enough

**Proof of concept, description of method used, screenshot, data gathered:**

Wireshark was used to capture the traffic that was used to initiate a successful connection to the access point. Since this was unencrypted, a hashed version of the password was found. From there a dictionary attack using Aircrack-ng software was used to uncover the password.

Graphical user interface, table

Description automatically generatedText

Description automatically generatedGraphical user interface, text, application

Description automatically generatedRectangle

Description automatically generated with low confidenceA screenshot of a computer

Description automatically generated with medium confidenceA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**Impact of a successful exploit of vulnerability:** An attacker would be able to connect to the network and carry out more attacks from there. This basically opens the flood gates.

**Likelihood, how easy to exploit vulnerability, the exploit publicly available, does it require physical/WAN/LAN:** Not hard to exploit, likely to happen, publicly available, required to be within range of an access point.

**Access, is it repeatable:** Yes.

**Resultant risk:** Very possible for an attacker to connect to the WiFi and the possibility for a large-scale breach or attack is good. Once again, basically opens the flood gates.

**Recommendation for mitigation:** Use encryption to make sure that the WPA connection is secure. Also, make sure to implement a strong password policy, making sure the WiFi password is secure.

**Week 7: Unpatched SMB Vulnerability MS17-010**

Definition of vulnerability: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

**Root cause of vulnerability:** unpatched systems, use of SMB

**Proof of concept, description of method used, screenshot, data gathered:**

On the target host it was discovered that the MS17-010 vulnerability exists. The vulnerability was successfully executed allowing for remote control of that computer. After that, hash dump was run giving access to a list of users and their hashed passwords which were then cracked using the John the Ripper application.

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

***Text

Description automatically generated***

Graphical user interface, text, application

Description automatically generated

**A screenshot of a computer

Description automatically generated**

**Impact of a successful exploit of vulnerability:** remote code execution along with complete compromise of the affected system. Can be remotely controlled by the hacker allowing for easy installation of a backdoor.

**Likelihood, how easy to exploit vulnerability, the exploit publicly available, does it require physical/WAN/LAN:** Very likely if an attacker can gain access to the network, is publicly available, requires connection to the network

**Access, is it repeatable:** Yes

**Resultant risk:** Leaves open the possibility for complete server and network compromise.

**Recommendation for mitigation:** Systems need to be patched immediately when they are released. Systems should also be audited on a regular basis.

**Appendix**

* Aircrack-ng: Aircrack-ng is a suite of tools that can be used to assess network security. Can be used to monitor, attack, test, and crack (*Aircrack-Ng*, n.d.). The tool can be downloaded here: <https://www.aircrack-ng.org/>
* Backdoor: A backdoor is an undocumented way of gaining access to a computer system and is a potential security risk (NIST, n.d.)
* John the Ripper: John the Ripper is an Open-Source password security, auditing, and password recovery tool that can be used to crack passwords (*John the Ripper Password Cracker*, n.d.).
* MS17-101 Eternal Blue: This vulnerability (also known as CVE-2017-0144) affects specific Windows Servers allowing complete confidentiality, integrity, and availability loss and compromise. This is an execute code vulnerability (CVE Details, n.d.)

**Sources**

*Aircrack-ng*. (n.d.). Aircrack-Ng.Org. https://www.aircrack-ng.org/

CVE Details. (n.d.). *CVE-2017-0144 : The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows*. CVEDetails.Com. https://www.cvedetails.com/cve/CVE-2017-0144/

*John the Ripper password cracker*. (n.d.). Openwall.Com. https://www.openwall.com/john/

NIST. (n.d.). *backdoor - Glossary | CSRC*. NIST.Gov. https://csrc.nist.gov/glossary/term/backdoor