EE379K Enterprise Network Security Lab 3 Report

Student: Brian Cheung bc32427
Professor: Mohit Tiwari
TA: Antonio Espinoza
Department of Electrical & Computer Engineering
The University of Texas at Austin

October 27, 2019

Part 1 - APT Campaign Questions

Exercise Set 1

1. Dwell time is the number of days from when an attacker first compromises the victim to when the attacker is finally detected. The decrease in median dwell time over the past year can be attributed to the improvement of "internal hunting capabilities" and "enhanced network, endpoint and cloud-service provider visibility." [1]

2. Advanced Persistent Threat (APT) groups are "generally focused on espionage activities."

    - APT37 ("Reaper") - Active since 2012, APT37 primarily targets organizations in South Korea, but have recently started targeting Japan, Vietnam, and the Middle East in order to gain intelligence for North Korea's military, political, and economic interests.
    - APT38 - APT38 uses destructive malware to steal hundreds of millions of dollars from financial institutions. This group is linked to North Korean espionage operators.
    - APT39 - APT 39 is an Iranian cyber espionage group primarily targeting the Middle East. It targets the telecommunications sector, travel industry and supporting IT firms, and the high-tech industry in order to monitor and track specific individuals and collect customer data for strategic purposes related to national priorities.
    - APT40 ("Periscope") - APT40 is a Chinese espionage group that targets Southeast Asian countries that are important to China's "Belt and Road Initiative". The group takes large amounts of information from organizations in the engineering, transportation, and defense sectors related to maritime technologies.

3. The known methods of initial compromise for APT37 include phishing operations and strategic web compromise. Specifically, APT37 sent a reunification-themed email that contained a weaponized HWP attachment. This spearphishing attachment is a form of social engineering that relies on the victim to execute the attachment which compromises the victim's system. "Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments." [2] APT37 also used social networking and cloud platforms like Twitter, AOL, and Dropbox to relay commands to compromise

the victim's systems. Analyzing network data for abnormal data flows and unexpected protocol behaviors may be useful in detecting such attacks. [3]

4. A lack of investigation on infected systems may cause the victim to overlook the the possibility of a larger breach. After detection of malware on a system, it is important to understand that the piece of malware may have stemmed from a lateral movement from another system in the environment, and not just a new isolated attack. This understanding would encourage the victim to run a more thorough investigation to detect the breach. A poorly timed remediation may actually hurt the victim even further. If an attacker has had long term access to the victim, the attacker may likely have many different ways to evade eradication methods. As a result of a poorly time remediation, the victim could fail to eradicate the attacker and even complicate the investigation further prolonging the investigation and remediation process. This mistake can be avoided by conducting regular reviews of incident response plans, use cases, and playbooks in addition to properly handling and storing evidence in incident respons plans. Organizations should also develop guidelines and procedures for analyzing threats ion addition to erradication and remediation plans.

Exercise Set 2

5. According to MITRE [3], the Web Service attack is a Command and Control and Defense Evasion tactic. Since this attack often uses common services that the victim is already using and web service providers often us SSL/TSL encryption, attackers can easily hide under the "expected noise" and extra level of protection.

6. Web services commonly used in a Web Service attack: 1

7. Social networking platforms like Twitter, cloud storage services like Dropbox, and Github are often used in a Web Service attack. These services allow attackers to post content embedded with malicious domains or IP addresses that infect victims. A victim may be able to detect the malicious intent through abnormal data flows and suspicious activity when accessing content on these services.

Web Service	Examples
Social Networking	10
Cloud Storage	9
Github	7
Google Services	7
Pastebin	5
Blogs	3
Downloader	1

Table 1: Table of web services commonly used in a Web Service attack.

Exercise Set 3

8. APT41 targets the video game industry by "stealing source code and digital certificates, virtual currency manipulation, and attempting to deploy ransomware." [4] An APT group like APT41 could be interested in targeting the video game industry for financial gains.

9. APT29 is a Russian cyber threat group that has a very sophisticated way of communicating with the malware, Hammertoss. [5]

   (a) The malware generates a Twitter handle (user ID) based on the specific day. This tells the malware which Twitter account to check for a tweet that contains instructions for the next stage in the process. If the Twitter account isn't registered, then Hammertoss will wait for the next day to begin the process again.

   (b) If APT29 registered the specific Twitter account for that day, the group will tweet a URL that directs Hammertoss to a webpage that contains images along with a hashtag that specifies the offset of the hidden data and the characters for decryption.

   (c) For example, the URL can link to a Github page where APT29 has uploaded an image appended with encrypted data. Hammertoss will visit this page and download the image.

   (d) Hammertoss then decrypts the data with the instructions specified in the tweet.

   (e) The data may include commands or login credentials that instructs Hammertoss to upload a victim's data to a cloud storage service. Once uploaded, APT29 can retrieve the information.

   APT29 makes the process difficult to detect by using Twitter as an extra layer of obfuscation. Additionally, APT29 registers only a small

number of accounts and only communicates at certain times keeping their footprint small and indistinguishable from normal traffic.

10. Sudo prompts the user for the password and allows the user to run commands with root privelages. It can also cache the credentials by storing the timestamp of when `sudo` was last run. This allows the user to have root privelages for a certain period of time. This caching is isolated to a specific terminal session with the `tty_tickets` variable. However, this can be abused to allow malware to execute commands with elevated privelages without the user's password by seeing if timestamps fall within the timeout range. If `tty_tickets` are disables, the malware can do this from any terminal session for the user. This can be detected by monitoring the I/O logs from the `/etc/sudoers` file. To stop such acttacks, the user needs to ensure the `tty_tickets` setting is enabled to prevent any leakage across terminal sessions. Users can also set the `timestamp_timeout` to 0 which would require the user to input their password each time `sudo` is executed. [6]

11. MimiPenguin uses a technique called Credential Dumping. [7] This technique is a form of Credential Access that involves dumping process memory and extracting clear-text credentials. [8]

Part 2 - Fuzzing

1. The Vulnserver expects a command followed by an argument. If an invalid command is sent or no argument is provided, then the server responds with "UNKOWN COMMAND". The fuzzer (part-2/fuzzer.py) generates a random string for a random command and keeps increasing the length of the string until it observes unexpected behavior. Then it changes to a different command and repeats until the Vulnserver crashes. The fuzzer also creates two output files in the output directory (part-2/output/). The `success.txt` file logs all of the successful commands that didn't cause any unexpected behavior. The `failure.txt` file logs all of the commands that caused unexpected behavior. After running the fuzzer and analyzing the output files, the `failure.txt` file shows that a string length of at least 4110 caused unexpected behavior. Sometimes the server crashes and sometimes the server responded with "UNKOWN COMMAND" followed by some additional responses even for a known command. After causing buffer overflow, sending a different command seems to crash the Vulnserver as well.

2. The extremely long string caused the buffer to overflow which caused unexpected behavior. The buffer overflow could be exploited to execute shellcode.

Part 3 - Exploitation

1. The exploit uses HTTP to communicate with the application as shown in Figure 1.

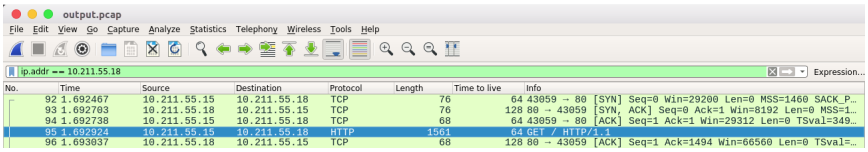

Figure 1: Screenshot of Wireshark displaying the HTTP request made by exploit to the Windows server

2. In the GET request in Figure 2, the Authorization header contains the payload.
3. The payload is encoded to Base64 and excludes the bad characters so that Metasploit can determine the suitable payloads given the space available and OS of the victim. [9] After decoding the payload, Figure 2 shows that the payload contains random letters.
4. 1012 bytes are required before overwriting the EIP. The EIP is overwritten with the target return address in little endian format.
5. The target address is `0x0040ae0f` in little endian format.
6. The `Space` variable specifies that theres is 600 bytes of space for the payload to reside in. If the payload is larger, it may cause corruption or truncation of the exploit.
7. The exit function for the exploit is "thread". This affects the stability of the program after the exploit.
8. CVE number: 2009-0183
9. CVSS base score: 10.0 HIGH The score is high because the Free Download Manager is remotely exploitable, the access complexity is low, it does not require authentication, all system files are revealable, any file is modifiable, and the attacker can render the system unavailable. [10]

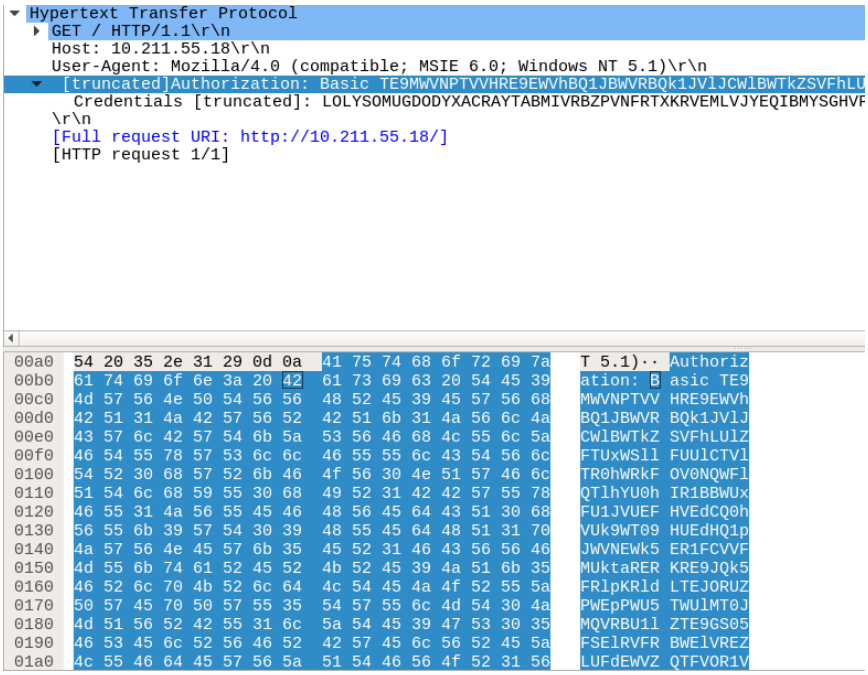

Figure 2: Screenshot of Wireshark displaying the GET request and decoded payload

10. User: `victimbox\class`
11. Current Directory: `C:\Program Files\Free Download Manager`
12. OS: `Windows 7 (6.1 Build 7601, Service Pack 1).`
13. Current Process Name: `fdmwi.exe`; Current PID: `1096`
14. Network Interfaces: 3; MAC Address of current connected interface: 00:1c:42:a9:26:bb
15. Trying to acces the `C:\Users\admin` directory, gives the following error message:

    ```
    [-] stdapi_fs_chdir: Operation failed: Access is denied.
    ```

16. Trying the `getsystem` command gives the following error message. This is because the Meterpreter is not a SYSTEM user.

    ```
    [-] priv_elevate_getsystem: Operation failed: Access is denied. The following wa
    [-] Named Pipe Impersonation (In Memory/Admin)
    [-] Named Pipe Impersonation (Dropper/Admin)
    [-] Token Duplication (In Memory/Admin)
    ```

17. User: `NT AUTHORITY\SYSTEM`
18. Exploit used: `exploit/windows/local/ms13_081_track_popup_menu`
19. Current Process Name: `notepad.exe`; Current PID: 2100; Yes, it makes sense to stay in this process to have elevated privelages.
20. The hash for the admin user is: `admin:1001:aad3b435b51404eeaad3b435b51404ee:7c098297bf99` The website CrackStation was used to decrypt the hashed password. [11]
21. Admin Password: `iloveponies`
22. Admin's Secret: `i love lutefisk`

Conclusion

References

[1] FireEye, "M-Trends 2019 Report," 2019.

[2] MITRE, "Spearphishing Attachment."

[3] MITRE, "Web Service."

[4] FireEye, "APT41."

[5] FireEye, "APT29."

[6] MITRE, "Sudo Caching."

[7] MITRE, "MimiPenguin."

[8] MITRE, "Credential Dumping."

[9] Peleus, "Converting Metasploit Module to Stand Alone."

[10] NIST, "Common Vulnerability Scoring System Calculator - CVE-2009-0183."

[11] "Free Password Hash Cracker."