ITRI625 - Computer Security II

Metasploit Project Documentation

Affaan Muhammad - 33016763

Joshua Esterhuizen - 30285976

Due: October, 19th 2021

Contents

1 Metasploit **2**
1.1 What is Metasploit? . . . 2

2 Installation and Setup **4**
2.1 Blog . . . 4

3 Scenario 1: Android exploit **5**
3.1 Overview . . . 5
3.2 Carrying out the exploit . . . 5
3.3 Countermeasures . . . 5

4 Scenario 2: Windows exploit **6**
4.1 Overview . . . 6
4.2 Carrying out the exploit . . . 6
4.3 Countermeasures . . . 6

5 Closing remarks **8**
5.1 Reflection . . . 8
5.2 Work Consensus . . . 8

6 Additional readings and miscellaneous information **10**
6.1 News and Opinions . . . 10
6.2 Blogs . . . 11
6.3 Other useful websites . . . 11
6.4 Organisations . . . 11
6.5 Training . . . 12
6.6 Security Groups . . . 12
6.7 Contests and Competitions . . . 12
6.8 Conferences . . . 12

Bibliography **13**

Section 1

Metasploit

The growth and widespread adoption of technology and the internet can be compared to a double-edged sword. While the globe is more interconnected than ever, this almost unanimous adoption of technology has brought with it some issues and problems of its' own. One such major issue is the increased security risk people undertake by participating in the use of technology and the internet. Before the most risk you would be in was if you had dropped important documents while nowadays an attacker could access this information through some nefarious mean without even alerting you or the targeted institution. The simplest was to guard against these on a large scale without sacrificing the comfort of using technology or the internet is to develop and put in place security measures to block these kinds of attacks.

The Metasploit framework was developed to aid in this process by providing a structured and contained way to attempt penetration on a system to test the security measures and their effectiveness. This is helpful for both countering security in the wrong hands as well as aiding in improving the security of organisations.

1.1 What is Metasploit?

Before we can describe the ways that Metasploit can help organisations and how it counters security in the wrong hands, we need to understand what Metasploit is and how it functions. Metasploit and its' framework were originally designed and developed as a tool for security experts in various fields such as network security, security administrators, product vendors and any other security experts to use within their own field according to the specific needs of each.[4]

Other than that, Metasploit is describes as a tool that collectively combines exploits into one central hub for security experts and researchers or alternatively as a project that contains information pertaining to security vulnerabilities and aids in the penetration testing of a system as well as the development of an intrusion detection system.[7, 4]

Penetration testing is a method of identifying certain vulnerabilities within a system be it a computer, network or website. As a process, it includes gathering data on the system to determine where vulnerabilities may lie and then attempt to exploit them to

test the measures put in place.[7]

Section 2

Installation and Setup

For further details have a look at our blog page for the setup that was done. It is located at the following link:
https://ITRI625.github.io/post3.html

2.1 Blog

The blog we created was hosted on GitHub Pages. The link to the blog is:
https://ITRI625.github.io

More information on GitHub Pages can be found at: https://pages.github.com/

The template for the blog was acquired from:
https://startbootstrap.com/theme/clean-blog

GIFs on the Blog were sourced from https://tenor.com/ and https://giphy.com/

Additionally, the screenshots taken were from VMs we implemented in VirtualBox and other images for the headers were sourced from Google Images.

Section 3

Scenario 1: Android exploit

3.1 Overview

The scenario is described as follows:

> *A person (that will be known as the victim in further discussions), opens a SMS received on their mobile device. This SMS has a malicious link embedded in it, or has a link that redirects to a malicious site. The link automatically downloads and runs an Android application package also known in other terms as an APK file. This APK file is what the Android Operating System uses to install applications. This malicious Application, once installed gives the Hacker (known as a perpetrator in an attack) full control over the device to outside parties, including the perpetrator. From here on out, the perpetrator has the victim in the palm of their hands, and can do what every they like to the device as well as carry out further attacks against the victim.*

3.2 Carrying out the exploit

The following resources were cited during this process.[2, 6, 8, 1, 9, 3, 5]

For further details have a look at our blog page for this exploit. It is located at the following link:
https://ITRI625.github.io/post1.html

3.3 Countermeasures

Section 4

Scenario 2: Windows exploit

4.1 Overview

The scenario is described as follows:

> *Windows 7 had all support for the operating system halted in January of 2020. Windows 7 was certainly a user favourite and the end of support saw quite a few users disgruntledly switch to either Windows 8 or 10 to continue to get security focused support and patches. At this point, the support for windows 7 has been defunct for almost 2 years and as such many new exploits have likely surfaced. Nonetheless, even before Windows 7 met its end-of-life there were still many exploits that could be performed on the system that were sequentially fixed in the new versions of Windows. One such vulnerability present in Windows 7 is that the default version of Windows Media Centre will execute any code saved as a ".mcl" file.*

4.2 Carrying out the exploit

For further details have a look at our blog page for this exploit. It is located at the following link:
https://ITRI625.github.io/post2.html

4.3 Countermeasures

The most useful countermeasure to this, and typically, any security related vulnerability is user vigilance. A user should be aware of what files, services, websites, etc. should typically look like in their daily usage a computer system and, as such, should be able to identify when one of these, and in this case a file, looks suspicious and should be scanned via some program before using or opening it. Furthermore, it is also important since this

exploit made use of a .mcl and .exe file that a user makes use of some form of antivirus or antimalware software and in this particular case, ones that are signature based. The reasoning for this is because the executable in this scenario is one that has been created and is typically used in a large scale. It is also vital to understand the exploits you are vulnerable to. In the tutorial we demonstrated that the file could be run and Windows only alerts that it comes from an untrusted, meaning un-certified, source which nowadays is something that happens with most applications as the typically programmer does not have access to particular licencing on their applications. In this case, having a more rigorous firewall or settings for it may have restricted the reverse_tcp from functioning.

Apart from this, the main fix to this particular issue was to install a patch provided by Microsoft on their site, and as such having some sort of patch management system is also vital to users. This could be simply regularly checking each application download page for the newest version or patch. However, there are applications and programs that automate this process and keep all your programs up to date. It should also be noted that most programs tend to offer a "Check for updates" feature when installing the program and likely also in the settings after the fact.

Section 5

Closing remarks

5.1 Reflection

Joshua Esterhuizen had the following to say:

> Working on this project has taught me several different things both within and outside of computer security. The most notable to me personally would be the fact that GitHub allows each user to create and then host a single static website. This is what was used to host the blog section of this project but will also be used by me in a personal capacity for a personal website in future. Apart from this, seeing the sheer amount of exploits that Metasploit has available to use is a bit disconcerting as it covers a wide array of different machines, programs and means of execution and has definitely made me that much more critical of everything I do online. This project also allowed me the chance to learn how to use HTML and CSS when writing the blog, which also forced me to switch up my usual writing style for one that is more colloquial for the general public instead of assuming the people reading the writing are already knowledgeable on the topics.

Affaan Muhammad had the following to say:

> Lorem ipsum

5.2 Work Consensus

All members in the group contributed to this project and a 50/50 balance between work allocation was kept. Below is a table showing how the work was divided in this project amongst the 2 members i.e. Affaan & Joshua

Affaan	Joshua
Scenario 1	Scenario 2
Blog	Blog
Testing	Testing
Bug fixes	Bug fixes
Proofreading	Proofreading
Documentation	Metasploit Literature Review

Section 6

Additional readings and miscellaneous information

CitizenLab located in Toronto, Canada is responsible for actively testing new threats, and exploits. Their site is located at the following url:
https://citizenlab.ca/
You can find additional information and news of current events in the cyber security space.

Heimdal Security headquartered in Denmark are a company which creates different suites for your cyber security needs. They also offer interesting resources such as whitepapers, articles, blogs, data sheets, case studies etc. Their site is located at the following url:
https://heimdalsecurity.com/

Additionally, an extensive list of cyber security resources can be found at:
https://www.cyberdegrees.org/resources/the-big-list/
They include the following:

6.1 News and Opinions

- Ars Technica – Risk Assessment
- CIO Security
- CSO Online
- Dark Reading
- Guardian Information Security Hub
- Homeland Security News Wire – Cybersecurity
- Infosecurity Magazine
- Naked Security
- SC Magazine
- SecureList
- SecurityWatch
- Threat Level
- ThreatPost

6.2 Blogs

- Google Online Security Blog
- InfoSec Resources
- Krebs on Security
- Microsoft Malware Protection Center Blog
- Schneier on Security
- Security Bloggers Network
- Terebrate
- Threat Track Security Labs Blog
- Veracode Blog
- Zero Day Blog

6.3 Other useful websites

- UTPA Center of Excellence in STEM Education
- CERIAS: Tools and Resources
- CVE: Common Vulnerabilities and Exposures
- Information Security Stack Exchange
- Infotec Pro
- ISC: Internet Storm Center
- National Centers of Academic Excellence (CAE) in Information Assurance (IA)/Cyber Defense (CD)
- OVAL: Open Vulnerability and Assessment Language
- Scholarship Opportunities
- US-CERT
- U.S. Department of Homeland Security – Cybersecurity

6.4 Organisations

- ACM SIGSAC: Special Interest Group on Security, Audit and Control
- ASIS International
- CSA: Cloud Security Alliance
- DC3: Defense Cyber Crime Center
- HTCIA: High Technology Crime Investigation Association
- ISF: Information Security Forum
- ISSA: Information Systems Security Association
- NICCS: National Initiative for Cybersecurity Careers and Studies
- NSI: National Security Institute
- NW3C: National White Collar Crime Center
- OWASP: Open Web Application Security Project
- SANS
- Science of Security Virtual Organization

6.5 Training

- Damn Vulnerable Web Application (DVWA)
- Evolve Security Academy
- HackThisSite (HTS)
- Metasploitable
- Mutillidae
- NATAS
- National Institute of Building Sciences
- SecureSet
- SlaveHack

6.6 Security Groups

6.7 Contests and Competitions

6.8 Conferences

Bibliography

[1] *Binary Payloads*. URL: https://www.offensive-security.com/metasploit-unleashed/binary-payloads/.

[2] *Command-line Flags Chapter 4. Port Scanning Overview*. URL: https://nmap.org/book/port-scanning-options.html.

[3] *Manage Meterpreter and Shell sessions*. URL: https://docs.rapid7.com/metasploit/manage-meterpreter-and-shell-sessions/#view-available-meterpreter-shell-commands.

[4] Carlos Joshua Marquez. "An analysis of the ids penetration tool: Metasploit". In: *The InfoSec Writers Text Library, Dec* 9 (2010).

[5] *Meterpreter Basic Commands*. URL: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/.

[6] *Meterpreter: Security encyclopedia*. URL: https://www.hypr.com/meterpreter/.

[7] Sudhanshu Raj and Navpreet Kaur Walia. "A Study on Metasploit Framework: A Pen-Testing Tool". In: *2020 International Conference on Computational Performance Evaluation (ComPE)*. IEEE. 2020, pp. 296–302.

[8] *What is Meterpreter ? - Security Wiki*. Aug. 2021. URL: https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/.

[9] Mohammed Zain. *How It Works: Reverse_tcp Attack*. Apr. 2020. URL: https://medium.com/@mzainkh/how-it-works-reverse-tcp-attack-d7610dd8e55.