Metasploit Lit Review

**Introduction**

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.

**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.\cite{testIDS}

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.\cite{goodDef, testIDS}

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.\cite{goodDef}

Metasploit was originally equipped with many modules that can be used. The four main modules include: \cite{goodDef}

* Exploit module which allows for a means to attack a compromised system,
* Payload which allows for a means for attackers to gather data by interacting with the target,
* Auxiliary module, which is equipped to test, scan and recon the target and
* Encoders module which is used for evading firewall and anti-virus tools.

It should also be noted that since Metasploit is an open source, meaning the code to how it was built is publicly available for download, this allows users and security experts to develop their own modules if the need for then is required. \cite{goodDef}

There are also two other notable items that are coupled with Metasploit – those being Meterpreter and Msf-Venom. Meterpreter is a powerful payload that came to Metasploit some time after it was developed. It is an advanced dynamically integrated payload that is stored entirely within the memory of a system. \cite{testIDS}When a vulnerable system is found and consequentially infected with this payload via any exploit, it establishes a connection between the infected and attacker systems through a client side, the infected system, command which bypasses most firewall restrictions. \cite{testIDS} Meterpreter is also a powerful payload for another reason – it is very elusive and often goes by undetected by most security experts. \cite{testIDS} Meterpreter also comes with a command line style interface that has various commands such as getting system information, interacting with peripherals on the infected system and making use of the infected systems command line or power shell.

Msf-Venom on the other hand is not a payload but a Metasploit standalone payload generator. It is the updated replacement of msfpayload and msfencode. \cite{goodDef} It allows a user to generate any type of shellcode or payload that will affect a platform of their choice - such as on Linux, Windows or Android to name a few. \cite{goodDef}

**How it counters security in the wrong hands**

“Security in the wrong hands” is likely referring to people or organisations that are making use of security measures to halt, attack or generally inconvenience others. As such, Metasploit and its’ accompanying modules are a tool that will counter these types of attacks.

The clearest way that Metasploit can be used in this capacity is that it directly provides the tools to infiltrate and attack the system to remove the security measures in place and as such counters the given attack. Additionally, it can also be used to study the system itself to find any vulnerabilities and then generate payloads and exploits that match the systems security measures with Msf-Venom.

Metasploit allows for this with several keywords within the framework – namely those being:

* Search
* Use
* Exploit and run

The search keyword allows for a Metasploit user to comb through the massive library of modules Metasploit provides and quickly and easily find the appropriate payload they require. \cite{goodDef}

The use keyword allows for a Metasploit user to implement the particular module they want to and begin the exploitation process. \cite{goodDef}

The exploit and run keywords allow a Metasploit user to activate their choice of payload and module and begin the actual infiltration of a vulnerably system. \cite{goodDef} There are two keywords for this particular action.

However, Metasploit can also be used by security experts within an organisation to test their internal security systems and measures that they have in place.

**How it improves the cyber security of an organisation**

Security experts and system administrators within organisations have begun taking the approach of viewing their control measures as an ever-evolving system that needs constant attention as it is a matter of when the measures will fail and not if they will fail. \cite{usesEvade}

These experts and administrators can make use of Metasploit to test their systems and find any vulnerabilities in a controlled environment before they are exploited by any malicious attacker. This is a needed aspect of the security department of any organisation that wished to keep their data and information safe as one of the biggest issues to solve with exploits is how they evade detection. This is typically done by avoiding detection of an anti-virus or anti-malware program through the use of \cite{usesEvade} \cite{testIDS}:

* Manual Binary Editing
* Polymorphic code

Most anti-virus programs have been ineffective at detecting the payloads distributed by Metasploit and as such making use of these exact payloads to further secure a system is ideal. \cite{testIDS} However, before being able to update a security system to detect these payloads, the means of evasion must be understood. Manual binary editing is the process by which the malware in question changes a particular signature to avoid detection by signature-based security programs. \cite{usesEvade} Due to this, the security experts could modify the means by which these applications check for signatures – as one suggestion is to sub-divide the files being scanned and checking if there is a partial match to a known malware or virus signature. \cite{usesEvade}

The above method, however, may not work on the second means of evasion -polymorphic code. A virus or piece of malware with this specific trait changes each time it is run and therefore has a different signature each time - avoiding signature-based detection entirely. \cite{usesEvade} Therefore using payloads from Metasploit with this characteristic allows for system administrators and security experts to efficiently test the intrusion detection systems and any heuristic-based anti-malware or anti-virus programs. \cite{usesEvade}

Another use is that Metasploit can also be used to test the security measures of websites and web applications. \cite{testweb}

From this section, it is clear that Metasploit can be used to strengthen the security measures put in place by an organisation by allowing the security experts and system administrators to firstly identify what vulnerabilities the system has, then exploit it to understand how the exploit uses the vulnerability and then find a means to patch this vulnerability.

**Conclusion**

Metasploit is shown to be a powerful tool for security experts as it allows for a controlled means to study system vulnerabilities and exploits while aiding in the process of strengthening the systems themselves as well as the programs used to safeguard the systems.

**Sources**:

@inproceedings{goodDef,

title={A Study on Metasploit Framework: A Pen-Testing Tool},

author={Raj, Sudhanshu and Walia, Navpreet Kaur},

booktitle={2020 International Conference on Computational Performance Evaluation (ComPE)},

pages={296--302},

year={2020},

organization={IEEE}

}

@inproceedings{usesEvade,

title={Applied comparative evaluation of the metasploit evasion module},

author={Casey, Peter and Topor, Mateusz and Hennessy, Emily and Alrabaee, Saed and Aloqaily, Moayad and Boukerche, Azzedine},

booktitle={2019 IEEE symposium on computers and communications (ISCC)},

pages={1--6},

year={2019},

organization={IEEE}

}

@article{testIDS,

title={An analysis of the ids penetration tool: Metasploit},

author={Marquez, Carlos Joshua},

journal={The InfoSec Writers Text Library, Dec},

volume={9},

year={2010}

}

@article{testweb,

title={Web penetration testing using nessus and metasploit tool},

author={Mukhopadhyay, Indraneel and Goswami, S and Mandal, E},

journal={IOSR Journal of Computer Engineering},

volume={16},

number={3},

pages={126--129},

year={2014}

}

Scenario 2 Overview

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.

Scenario 2 Counter measures

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.

Josh Reflection

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.