*International Journals of Advanced Research in Computer Science and Software Engineering*
*ISSN: 2277-128X (Volume-9, Issue-8)*

**Research Article** | **August 2019**

# Metasploit Framework: An Attack Scenario

**Navninderjit Singh**
*Department of Commerce, Punjabi University, Patiala, Punjab, India*
Email: navninder@gmail.com

***Abstract— This research paper presents an attack on a Windows XP machine using the Metasploit framework. The paper presents that there are ways to take over a system without even touching it or alerting a user. Various tools could learn to use in a couple of hours. The take away is that all of this could have been avoided entirely if the victim was running the latest patches on its operating system and software.***

***Keywords— Metasploit, attack, operating system, patch, alert***

## I. INTRODUCTION

The Metasploit Framework is a collection of software utilities that interoperate to create an environment for building, preparing, and launching attacks against a system, network, or whatever you have an exploit designed for [8]. Metasploit is often thought of as "The script kiddie's toy" because it is simple to use, and has many different user interfaces, if you do not want to interface with the command-line interface. Fortunately, its ease of use simply magnifies how effective it can be at its job, which is penetration testing [21]. Yes, it is usable by people who do not quite know what they are doing, but its effectiveness is limited unless you have a solid understanding of networking, security and the framework itself.

## II. BACKGROUND AND HISTORY

The Metasploit framework was created by H. D. More in 2003 as a portable network tool [5]. At the time Metasploit was written in Perl. By 2007, the Metasploit tool was completely rewritten in Ruby and had grown to be a full-blown software framework [11]. In 2009, the Metasploit software was acquired by Rapid7, a security company that provides unified vulnerability management solutions. It is now split into a free version with a few features stripped out, and a professional version containing the entire feature set and professional support. Fortunately, the free version of the Metasploit framework still has all the features which make it a potent penetration testing suite [18]. The features of the professional version are mostly related to testing at scale and automation.

Last but not least, the Metasploit framework is considered dual-use software. That means you must be very careful with what you know about the Metasploit framework [25]. The Metasploit framework can be used for legal and authorized penetration testing as well as illegal attacks against another system, remote or local [1]. The general rule of thumb is if you explicitly own the system/network you are operating on, or you have clear and written authorization allowing you to perform attacks on the systems or devices under the reason of penetration testing, you are fine [7]. Otherwise, you should not be using the Metasploit framework. Society is still figuring out how to deal with the legalities of technology in the 21st century, and being charged with performing unauthorized attacks against a system carries a very scary sentence.

## III. METHODOLOGY

The lab-esque environment is required to build, document, and perform the attacks using the Metasploit framework while keeping legalities in check. A couple of virtual machines, virtualbox, and an internal host-only network, and some software were used to facilitate the attacks [10]. The first virtual machine was a Windows XP SP3 machine that did not have any security patches applied to it [3]. The second was a Linux machine running the Kali Linux security testing distribution. Three different exploits, one local, one remote, and one web-based were performed. Then the attack was launched against the machine as shown in fig. 1 below while documenting all the steps and noted the visual feedback on the victim (or lack of) and gathered Wireshark captures of the attack to visualize and demonstrate the attack happening.

The first attack, and probably the most well-known due to basic computer/Internet training telling you not to open unknown attachments in emails or downloads and the like, is the local attack. The local attack was performed on a PDF exploit affecting Adobe Reader v8 and v9 [17]. How the attack works is that you take a PDF into Metasploit, configure your options and payload, and Metasploit modifies the PDF to take advantage of the flaws in the code of the Reader, and execute your payload. The PDF is visually no different from the clean PDF. The following fig. 2 presents the exploit.

 


**Figure 1: An attack launched on a virtual machine Windows XP SP3**


**Figure 2: Configuring options and payload for Metasploit attack**

First adobe PDF embed exploit is applied in the fileformat class of exploits. The fileformat class generally refers to exploits that involve the victim opening a file to trigger the hack. In this case, a PDF [2]. The payload is the reverse TCP meterpreter. The first part, Reverse TCP, means that the victim connects back to the attacker. This is very effective in a lot of home network situations that deploy NAT and system-level firewalls [22]. The connection will usually bypass all that and connect right back to the attacker who is already configured to receive it. The second part, meterpreter, is the actual payload as shown in fig. 3. It is a special shell that has many operating-system-specific commands depending on the operating system of the machine that is being attacked. It also has ways of making sure the shell is persistent on the machine and survives reboots. It shares a lot of UNIX'isms in the way the shell operates.


**Figure 3: PDF exploit**

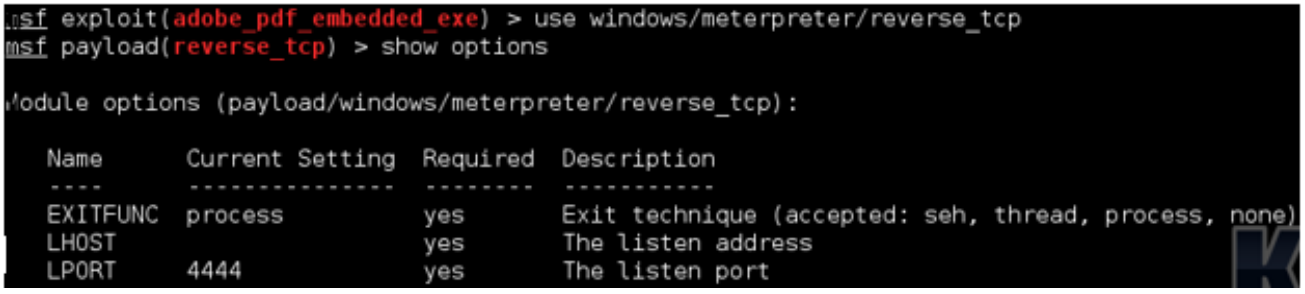


**Figure 4: meterpreter payload**

The EXEFILE was ignored in the PDF exploit, and the infected PDF name is evil.pdf. Very innocuous. When the user opens the PDF the user is automatically greeted with a random safe file dialog. Statistically most users would not care about this and simply click save [15]. Big mistake. This triggers the exploit to run and send a connection back to the attacker. The attacker then sends the meterpreter shell to the victim and launches it. The attacker then has full control. The scary part is the victim has no idea in the slightest that the attacker now owns his system.

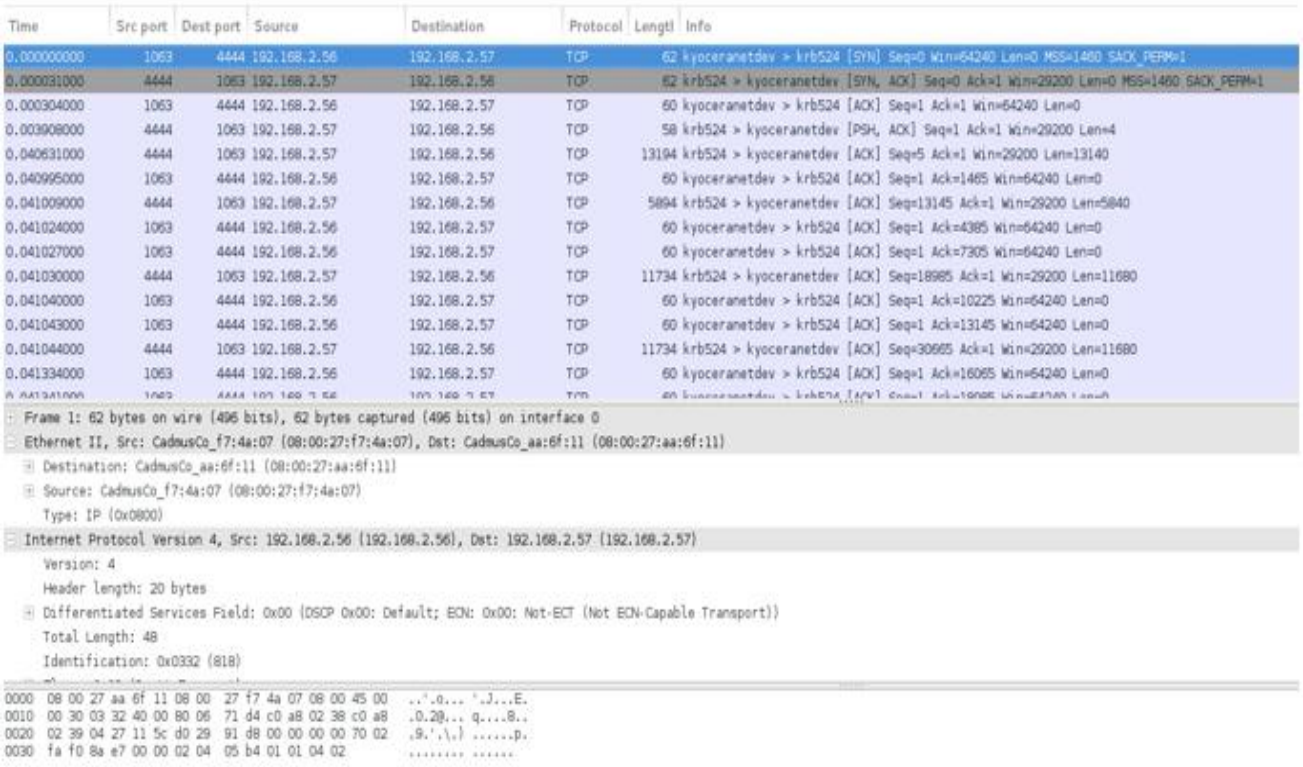


**Figure 5: Wireshark packet capture**

From wireshark packet capture the fig. 5 above, the network is quiet until the exploit happens, then the wire is lit up with traffic on port 1603 [19]. The connection is established in the two entries highlighted at the top. Next a remote exploit is performed that works on a system in the same subnet as the attacker [6]. We leveraged a weakness in the Server Message Protocol to perform the attack.

```
Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOST                     yes       The target address
  RPORT    445              yes       Set the SMB service port
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload information:
  Space: 400
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.
```

**Figure 6: Various options with a description of attack**

 

The fig 6 above shows the options and the description of this particular attack. What is new about this attack, is that RHOST option is executed [24]. This option is the IP address of the target machine to launch the attack. Only the IP is filled in the XP virtual machine, and ran the exploit with the same payload. Within seconds, another Meterpreter shell opened, an attacker could do with it as pleases. What is even scarier about this attack is that there were *no* visual signs that anything was wrong with the victim's system, and we didn't even need to touch the system.

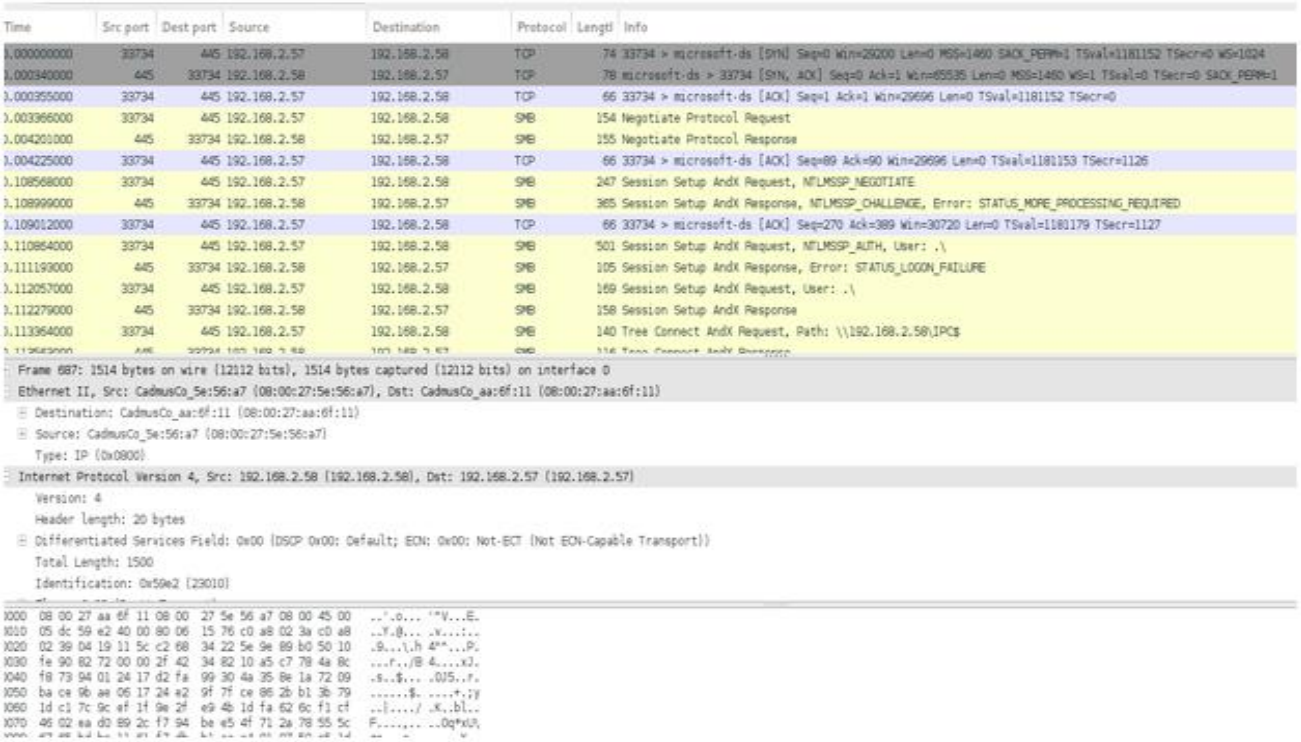


**Figure 7: Wireshark dump of traffic**

The Wireshark dump is shown in fig. 7 is a bit more interesting here. The traffic is a lot more varied as shown in the info column, but it all mostly resides on port 33734 and 445. The third exploit is a web-based exploit that takes advantage of a flaw in Internet Explorer [14]. This exploit is functional even if you are not on the same subnet, making it an effective tool for mass exploitation. Just set up the exploit on a web server somewhere, and send the URL through spam.


**Figure 8: The port used to listen data**

The above fig. 8 presents the port to listen on, and a URIPATH, which is the URL suffixed to the domain name. It could be set to whatever is the required port. As is shown above, the exploit is created and the server is started [17]. The client is directed to the bank webpage and the client is simply greeted with a blank website. However, in the background, it is shown that the payload is sent and executed.

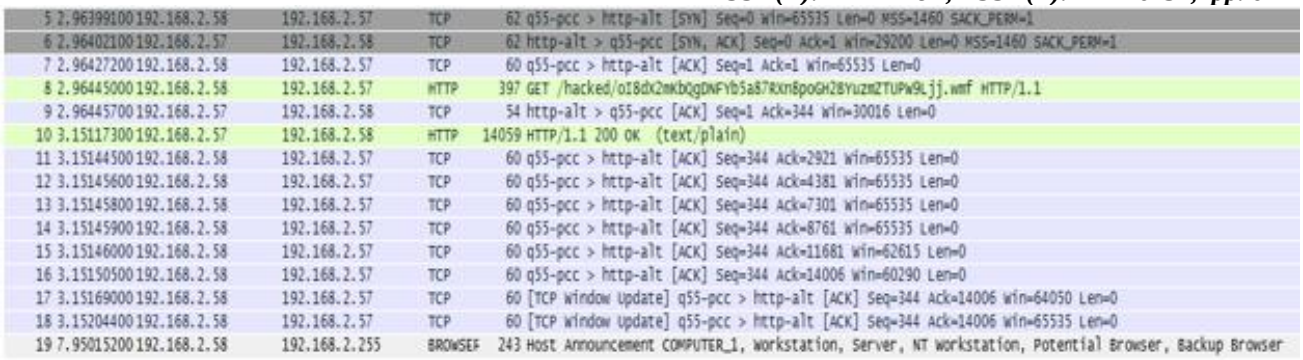


**Figure 9: Wireshark capture shows the successful attack**

The Wireshark capture shows the HTTP request, then the OK. After that, the exploit is being sent in the packets beneath.

## IV. CONCLUSIONS

In conclusion, this paper presents that security is a terrifying place. There are ways to take over a system without even touching it or alerting a user. All with tools could be learn to use in a couple of hours. It is also worth mentioning though, that all of this could have been avoided entirely if the victim was running the latest patches on its operating system and software. A very effective program at monitoring updates for Windows and the third-party apps, Secunia PSI, is free and can do this silently. It can often auto-update many programs by itself. Do not take security lightly.

## REFERENCES

[1] K. Kaur, X. Xiaojiang Du and K. Nygard, “Enhanced routing in Heterogeneous Sensor Networks”, IEEE Computation World’09, pp. 569-574, Athens, Greece, Nov. 15-20, 2009.

[2] Lauren Evanoff, Nicole Hatch, Gagneja K.K., “Home Network Security: Beginner vs Advanced”, ICWN, Las Vegas, USA, July 27-30, 2015.

[3] Gagneja K.K. and Nygard K., "Heuristic Clustering with Secured Routing in Heterogeneous Sensor Networks", IEEE SECON, New Orleans, USA, pages 51-58, June 24-26, 2013.

[4] Gagneja K.K., “Knowing the Ransomware and Building Defense Against it - Specific to HealthCare Institutes”, IEEE MobiSecServ, Miami, USA, pp. 1-5, Feb. 11-12, 2017.

[5] Gagneja K.K., “Secure Communication Scheme for Wireless Sensor Networks to maintain Anonymity”, IEEE ICNC, Anaheim, California, USA, pp. 1142-1147, Feb. 16-19, 2015.

[6] Gagneja K.K., "Pairwise Post Deployment Key Management Scheme for Heterogeneous Sensor Networks", 13th IEEE WoWMoM 2012, San Francisco, California, USA, pages 1-2, June 25-28, 2012.

[7] Gagneja K.K., “Global Perspective of Security Breaches in Facebook”, FECS, Las Vegas, USA, July 21-24, 2014.

[8] Gagneja K.K., "Pairwise Key Distribution Scheme for Two-Tier Sensor Networks", IEEE ICNC, Honolulu, Hawaii, USA, pp 1081-1086, Feb. 3-6, 2014.

[9] Gagneja K., Nygard K., "Energy Efficient Approach with Integrated Key Management Scheme for Wireless Sensor Networks", ACM MOBIHOC, Bangalore, India, pp 13-18, July 29, 2013.

[10] Gagneja K.K., Nygard K., "A QoS based Heuristics for Clustering in Two-Tier Sensor Networks", IEEE FedCSIS 2012, Wroclaw, Poland, pages 779-784, Sept. 9-12, 2012.

[11] K. K. Gagneja, K. E. Nygard and N. Singh, "Tabu-Voronoi Clustering Heuristics with Key Management Scheme for Heterogeneous Sensor Networks", IEEE ICUFN 2012, Phuket, Thailand, pages 46-51, July 4-6, 2012.

[12] Gagneja K.K., Nygard K., "Key Management Scheme for Routing in Clustered Heterogeneous Sensor Networks", IEEE NTMS 2012, Security Track, Istanbul, Turkey, pp. 1-5, 7-10 May, 2012.

[13] Runia Max, Gagneja K.K., “Raspberry Pi Webserver”, ESA, Las Vegas, USA, July 27-30, 2015.

[14] A. S. Gagneja and K. K. Gagneja, "Incident Response through Behavioral Science: An Industrial Approach," 2015 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2015, pp. 36-41.

[15] Tirado E., Turpin B., Beltz C., Roshon P., Judge R., Gagneja K., “A New Distributed Brute-Force Password Cracking Technique”, Future Network Systems and Security, FNSS Communications in Computer and Information Science, vol. 878, pp 117-127, 2018

[16] Caleb Riggs, Tanner Douglas and Kanwal Gagneja, "Image Mapping through Metadata," Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 2018, pp. 1-8.

[17] Keely Hill, Gagneja K.K., "Concept network design for a young Mars science station and Trans-planetary communication", IEEE MobiSecServ 2018, Miami, FL, USA, Feb. 24-25, 2018.

[18] Javier Campos, Slater Colteryahn, Gagneja Kanwal, "IPv6 transmission over BLE Using Raspberry PI 3", International Conference on Computing, Networking and Communications, Wireless Networks (ICNC'18 WN), March, 2018, pp. 200-204.

[19] Gagneja K., Jaimes L.G., "Computational Security and the Economics of Password Hacking", Future Network Systems and Security. FNSS 2017. Communications in Computer and Information Science, vol. 759, pp. 30-40, Springer, 2017.

[20] Gagneja K.K. Ranganathan P., Boughosn S., Loree P. and Nygard K., "Limiting Transmit Power of Antennas in Heterogeneous Sensor Networks", IEEE EIT2012, IUPUI Indianapolis, IN, USA, pages 1-4, May 6-8, 2012.

[21] C. Riggs, J. Patel and K. Gagneja, "IoT Device Discovery for Incidence Response," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2019, pp. 1-8.

[22] S. Godwin, B. Glendenning and K. Gagneja, "Future Security of Smart Speaker and IoT Smart Home Devices," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2019, pp. 1-6.

[23] Keely Hill, Kanwalinderjit Kaur Gagneja, Navninderjit Singh, "LoRa PHY Range Tests and Software Decoding- Physical Layer Security", 6th IEEE International Conference on Signal Processing and Integrated Networks (SPIN 2019), 7 - 8 March 2019.

[24] Alexandro Riuz, Carloas Machdo, Kanwal Gagneja, Navninderjit Singh, "Messaging App uses IRC Servers and any Available Channel", 6th IEEE International Conference on Signal Processing and Integrated Networks (SPIN 2019), 7 - 8 March 2019.

[25] Nica Ameeno, Kalib Sherry, Kanwal Gagneja, "Using Machine Learning to detect the File Compression or Encryption", AJCS, 2019.

[26] Broderick Wolff, Alexander Hughes, Xin Wang, Kanwal Gagneja, "The Nature of Phishing and Payload Delivery", AJCS, 2019.

 