Exploit remote attack test in operating system using arduino micro

HE Wahanani\textsuperscript{1}, M Idhom\textsuperscript{2}, D R Kurniawan\textsuperscript{3}

\textsuperscript{123} Department of Informatics, Faculty of Computer Science University of Pembangunan Nasional “Veteran” Jawa Timur, Surabaya, Indonesia

henniendah@if@upnjatim.ac.id

Abstract. The development of technology in this digital era has made people smarter so that they can find weaknesses in information technology. There are several studies that use weaknesses in open USB ports to inject attacks on remote exploits. The author conducts research on controlling a target computer or laptop using remote exploits by utilizing a gap in a computer system, the USB port. Exploitation of remote attacks is done by utilizing a gap in the open USB port. Test automated scripts that are integrated on the Arduino board to be integrated into an open USB port. The script tries to download the backdoor file that was created on the metasploit work task and runs automatically on the target. The impact maker remote exploits the attack gets access control of the target computer or laptop from the operating system Windows, Linux and Mac OS with the help of port forwarding. The most dangerous effects are those that can be done in the background which cannot be seen on the screen for the target computer or storing important data in the target file or directory.

Keywords: remote exploit, arduino micro, metasploit framework

1. Introduction
Computer systems that are vulnerable to many attacks where the system that can be opened is seriously protected. Security software, firewalls, antiviruses and the like have been implemented to protect valuable data on computers. There is no 100\% anti-approved system that is claimed to be the most sophisticated computer system ever. [1] Many do not realize that computer attacks can be done by using a common interface display such as Universal Serial Bus (USB) on a computer or laptop USB port [2][3][18].
The USB port on a computer system is basically an open port, so many people abuse these security weaknesses on the computer. Raising computer compilation is very risky to cause USB keystroke injection attacks, such as being able to restore important data files in system32 in Windows C. This open port on USB makes a computer machine can cause viruses or malware, and antivirus cannot be used to fight this system attack [4][5][11][14][20].
The Metasploit framework is a penetration tool that is strong enough to penetrate into a system. Metasploit is a free and open source computer network framework created by H.D. Moore in 2003 and is now acquired by Rapid7. Metasploit is usually opposed to the term remote exploitation, meaning the depreciation of a remote system that can control the victim's computer. Metasploit is considered multi-platform that runs on most Unix and Windows variations [6].
A new invention to start a keystroke injection tool or USB Rubber Ducky [16][17][19] is to use Arduino. Arduino can be launched an injection tool to an automatic keyboard that is already in the library.
goal is to send and download the backdoor of an attacker so that it can manage and exploit the target computer. The advantage of Arduino is winning the Arduino driver, not as an automatic HID keyboard or mouse.

In this study, we will discuss how to use the Arduino board to carry out remote attacks to exploit the use of injection tools with the help of the metasploit framework.

2. Literature Review

2.1 Exploit

This information can prove to be very useful in penetrating the target machine as can quickly look for exploits and vulnerabilities of the operating system in use. Well, the process is not straightforward, but knowledge about the target operating system can ease task to much extent. Each operating system has several bugs. After it was launched, the development process was exploited to get started. Operating systems such as Windows quickly develop patches for bugs or support and provide them for users. Systems that are not patched are safe for hackers, because they immediately launch exploits to compromise targets. Therefore, a regular and complex operating system is very important. In this research, focus on supported in some of the most popular operating systems. In the testing process, information about the target operating system is available, testing for exploits is available for certain operating system weaknesses [9]. This study focuses on several operating systems such as Microsoft, Linux and Mac OS.

2.2 Arduino Micro

Many methods were developed to penetrate the network as hackers or operating system testers. One practical strategy is to hack networks using an open USB port connected to a PC or laptop. USB vulnerabilities allow attackers to relatively easily perform and implement attacks. This can be done using a USB device issued by the victim's computer as a Human Interface Device (recognized as a keyboard) and running the code without the user's knowledge or use. USB is referred to as 'bad USB' [15]. However, bad USB attacks are often underestimated, perhaps considering that they are asking for more technical knowledge [7]. The purpose of this project is to make evidence of the concept of feasibility and poor distribution of USB using Arduino Micro [8] as a USB implementation (see figure 1).

![Figure 1. Arduino micro front [8]](image)

2.3 The metasploit framework

The Metasploit framework is a computer security project that can provide information about security and assistance in testing and development. Metasploit has several sub-projects which are most well known as open source. The metasploit framework, a tool for development and an exploiting code for exploiting remote target machines, an opcode database included, shellcode archives and other related research. Additionally, Metasploit is considered a multi-platform running on the most variations of Unix and Windows [6][13].

3. Research Method

3.1 Research requirements

In the process of this research, the authors divide the research needs in 2 aspects, the hardware and software requirements, the following research needs can be seen in table 1 below.
Table 1. Hardware and software requirements

| No. | Name             | Usability                                                   |
|-----|------------------|-------------------------------------------------------------|
|     | **Hardware**     |                                                             |
| 1   | Laptop           | The place to conduct research                               |
| 2   | Arduino board    | Hold automatic keyboard scripts                              |
| 3   | Modem USB        | Access internet network USB (attacker)                      |
| 4   | Mifi             | Access wifi internet network (target)                       |
|     | **Software**     |                                                             |
| 5   | Kali Linux[12]   | Attacking operating system                                  |
| 6   | Ubuntu 18.04 Lts | Target operating system 1                                   |
| 7   | Windows 10       | Target operating system 2                                   |
| 8   | OS X Mojave      | Target operating system 3                                   |
| 9   | Arduino IDE      | Program automatic keyboards                                 |
| 10  | Metasploit framework | The place to do a remote exploit attack                    |
| 11  | Apache web server| Hold the payload file locally                               |
| 12  | Ngrok            | Online localhost via tunnels                                |

3.2 Payload and listener
Payload and listeners are two things that are interrelated and connected. A payload is a file that will be executed or run on the target computer, while the listener tries to set the target computer that has a payload. The following is the payload for the 3 operating systems that will be tested in table 2.

Table 2. Payload on 3 operating systems

| Platform | Format | Payload                                      |
|----------|--------|----------------------------------------------|
| Windows  | Exe    | windows/meterpreter/reverse_tcp              |
| Linux    | Raw    | python/meterpreter/reverse_tcp               |
| Mac OS   | macho  | osx/x64/meterpreter/reverse_tcp              |

3.3 Draft attack
In the design of the attack in this study, the authors divided it into 3 stages where each stage has a different path but is still related to each other. At this stage it must be done sequentially. The following are 2 stages of attack design:

3.3.1 Exploit flow
For this second stage, the researcher made a step in the exploit path to run the exploitation process, before entering the first exploit stage, it was necessary to create a backdoor payload first through msfvenom. Here is the remote exploit path (figure 2):

![Figure 2. Exploit flowchart](image-url)
3.3.2 Arduino flow
For this third stage, the author makes the Arduino flow stage to be programmed so that it can run an automatic keyboard according to the author's wishes as an attacker. Following is the Arduino flow stage in figure 3.

![Arduino flowchart](image)

**Figure 3. Arduino flowchart**

3.4 flow of attacks
In the flow of the attack in this study, the authors made the initial steps until the attacker can get full access to the target laptop through a remote exploit attack. The following are the steps that are loaded in the attack path can be seen in figure 4 below:

![Remote Exploit Attack Flow](image)

**Figure 4. Remote Exploit Attack Flow**
In figure 4, the steps that must be done are:
a. Laptop attackers use a network connection on a USB modem
b. Connect to port forwarding ngrok
c. Attackers get dynamic links and ports from ngrok
d. Create an automatic keyboard script on Arduino and import it on the Arduino board
e. The attacker plugs the Arduino board into the target laptop through the laptop's USB port
f. The Arduino board runs automatic keyboard commands
g. The Arduino board downloads and runs the payload file from ngrok Link
h. Enter a meterpreter session, the target is connected and connected to the attacker
i. Finished

4. Result and Discussion

4.1 Analysis of Results
From the results of testing on 3 different operating systems, namely Windows, Linux, and Mac OS, the time for each activity starts from the execution stage of the payload, the meterpreter entry process, until the remote exploit process can be run when the network connection between the target and the attacker is stable. The results of the time record are used to measure the speed of the remote exploit attack. The data can be seen in table 3 below.

Table 3. remote exploit when the network is stable

| No. | Payload                                      | Delay (seconds) |
|-----|----------------------------------------------|-----------------|
|     |                                              | execution       | meterpreter | connection |
| 1   | windows/meterpreter/reverse_tcp              | 0               | 1-2         | 4-5        |
| 2   | python/meterpreter/reverse_tcp               | 0               | 1-2         | 4-5        |
| 3   | osx/x64/meterpreter/reverse_tcp              | 0               | 1-2         | 4-5        |

However, there are times when a network connection from one computer is unstable or there is no network signal, it will affect the process of entering the meterpreter so that it can affect the connection of the remote exploit connection to the attacker and target. The data can be seen in table 4 below.

Table 4. The remote exploit stage when the network is unstable

| Payload                                      | Remote exploit process stage (status) |
|----------------------------------------------|---------------------------------------|
|                                              | Network connection                | meterpreter | connection |
| windows/meterpreter/reverse_tcp              | not stable                      | enter       | long time   |
| python/meterpreter/reverse_tcp               | not stable                      | enter       | not connection |
| osx/x64/meterpreter/reverse_tcp              | no signal                       | not in      | not connection |

5. Conclusion
A remote exploit attack can work or can be run on Windows, Linux, or Mac OS operating systems. In the process of a remote exploit attack, the payload is an important role in the success or failure of the attack. A remote exploit attack will fail if the payload doesn’t match the executable format on the target operating system. Remote exploit attacks can be carried out on different networks, or generally referred to as public networks. Through tunnels on port forwarding, attacks that are initially on a local network or LAN can be transformed into attacks on public networks through dynamic ports provided by network, so that remote exploit attacks can work on different networks and at different distances. A remote exploit can be optimized by using Arduino IDE software and Arduino boards.
Acknowledgments
This work is supported by Department of Informatics, Faculty of Computer Science, Universitas Pembangunan Nasional Veteran Jawa Timur Indonesia.

References
[1] Wahab H and Zain J M 2018 Windows Privilege Escalation Through Network Backdoor And Information Mining Using USB Hacktool. Malaysian Journal of Computing.
[2] Bang and J E A 2010 Secure USB bypassing tool Digital Investigation 7, S114 - S120.
[3] Yang, B., Feng, D., Qin, Y., Zhang, Y., Wang, W.: TMSUI: A trust management scheme of USB storage devices for industrial control systems. In: Information and Communications Security: 17th International Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers, pp. 152{168. Springer International Publishing, Cham (2016)
[4] Cannols B and Ghafarian A 2017 Hacking Experiment by Using USB Rubber Ducky Scripting vol 15 (Systemics, Cybernetics and Informatics) pp 66-71.
[5] Mulliner C and Weippl E R 2018 USBlock: blocking USB-based keystress injection attacks In: Proceedings of the thirty-second annual IFIP WG 11.3 conference data and applications security and privacy XXXII: DBSec Springer; 2018. p. 16–18 (Vol. 10980, p. 278).
[6] Manjunatha T N Shashidhar M S et al 2016 Survey of Metasploit Framework Vol. 4 (International Journal for Research in Applied Science & Engineering Technology) pp 50-56
[7] S Vouteva 2015 Feasibility and Deployment of Bad USB University of Amsterdam, System and Network Engineering Master Research Project
[8] Arduino Micro, http://arduino.cc/en/Main/ArduinoBoardMicro, Accessed on 07 August 2019
[9] Abhinav Singh 2012 Metasploit Penetration Testing Cookbook Packt Publishing Ltd
[10] Nitzan Farhi Nir Nissim et al 2019 Malboard: A novel user keystroke impersonation attack and trusted detection framework based on side-channel analysis computer and security elsevier pp 240 – 269
[11] Neugschwandtner, M., Beitler, A., Kurmus, A. 2016.: A Transparent Defense Against USB Eavesdropping Attacks. In: Proceedings of the 9th European Workshop on System Security. pp. 6:1(6:6. EuroSec ’16, ACM
[12] Kali Linux, https://www.kali.org/, Accessed on 15 July 2019
[13] Offensive Security Ltd., About the Metasploit Meterpreter, http://www.offensive-security.com/metasploit-unleashed/About_Meterpreter. Accessed on 16 July 2019
[14] S. L. S. K. John Clark 2010 Compromise through USB-based Hardware Trojan Horse device Future Generation Computer Systems, vol. 27, pp. 555-563
[15] A. Caudill and B. Wilson. Phison 2014 Custom Firmware & Existing Firmware Patches (BadUSB).
[16] Hak5. 2013 USB Rubber Ducky Payloads. https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads
[17] Hak5. 2013 Episode 709: USB Rubber Ducky Part 1. http://hak5.org/episodes/episode-709
[18] Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., Bailey, M.2016 Users Really Do Plug in USB Drives They Find. In: Security and Privacy (SP), IEEE Symposium on. IEEE
[19] Teh, P.S., Teoh, A.B.J., Yue, S 2013. A survey of keystroke dynamics biometrics. The Scientific World Journal.
[20] Sebastian Neuner, Artemios G. Voyiatzis, dkk. 2018. USBlock: Blocking USB-based Keypress Injection Attacks. SBA Research, Austria.