Akademia Techniczno-Humanistyczna w Bielsku-Białej

WYDZIAŁ BUDOWY MASZYN I INFORMATYKI

Inżynier XXI wieku

XI Inter University Conference „Engineer of XXI Century” – 10 December 2021

# Endpoint vulnerabilities detection by simulating modern attacks

*Kostiantyn Savchuk[1], Yurii Lakh[2], Morika Rusynko[3],*
*Opiekun naukowy: Elena Nyemkova[4]*

1.Lviv Polytechnic National University, student of department of Information Technology Security, specialty: cybersecurity, kostiantyn.savchuk.mkbbi.2021@lpnu.ua
2.PhD, Associate professor, Lviv Polytechnic National University, department of Information Security, yurii.v.lakh@lpnu.ua
3.PhD, Associate professor, Lviv Polytechnic National University, department of Information Technology Security, morika.k.rusinko@lpnu.ua
4.DSc, Professor, Lviv Polytechnic National University, department of Information Technology Security, olena.a.niemkova@lpnu.ua

## Abstract

The study is devoted to the analysis of endpoint vulnerabilities and methods of their protection. The modern attacks were simulated in the virtual laboratory. The automated attack detection software module was implemented using attacker behavior patterns and indicators of compromise. The module has been successfully tested by re-simulating the attacks.

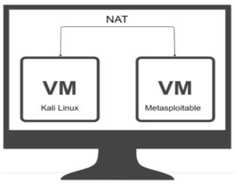
## Problem definition

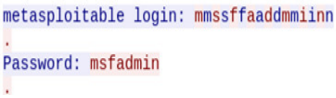
The purpose of the work is to develop a module for automatic search for indicators of compromise of attacks and patterns of attacker behavior based on the exploitation of vulnerabilities of the Linux operating system.

The following tasks are solved for this purpose:

– simulation of attacks using a virtual stand;
– determination of indicators of compromise and patterns of behavior of the attacker at the endpoint;
- development of an automatic software module for finding attacks based on the found indicators of compromise and patterns of behavior of the attacker.

## The practical part





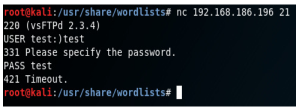
```
metasploitable login: mmssffaaddmmiinn
.
Password: msfadmin
.
```

✓ **scanning of open ports (utility nmap )**

```
Scanning 192.168.186.196 [30 ports]
```

✓ **exploitation of vulnerable software (Metasploit platform )**

vsftpd service version 2.3.4: exploit/unix/ftp/vsftp_234_backdoor



```
root@kali:/usr/share/wordlists# nc 192.168.186.196 21
220 (vsFTPd 2.3.4)
USER test:)test
331 Please specify the password.
PASS test
421 Timeout.
root@kali:/usr/share/wordlists# 
```

: )

✓ **brute force attack (Hydra utility)**
✓ **attack of a man in the middle (telnet connection, Wireshark)**

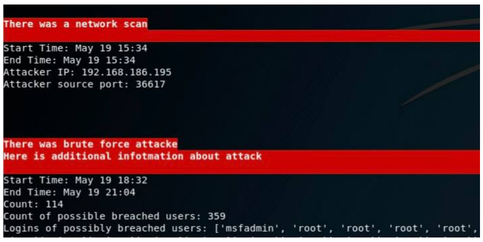
| Attack | Tactics Mitre | Technique Mitre | Phase Kill Chain |
|---|---|---|---|
| Scanning open ports | Reconnaissance, Discovery | Active Scanning, Network Service Scanning | Reconnaissance |
| Exploitation of vulnerable software | Initial Access | Exploit Public-Facing Application | Exploitation |
| Brute Force attack | Credential Access | Brute Force | Reconnaissance |
| Attack Man-in-the-Middle | Credential Access, Collection | Man-in-the-Middle | Reconnaissance |

## Indicators of compromise

- ✓ scanning ports with the nmap utility with the -sS parameter (handshake is not completed, query length is the same in all records)
- ✓ attemptions to enter with logins that contained “:)”
- ✓ large number of unsuccessful attempts to enter the endpoint using the SSH protocol

## Automation of attack detection

- Get login, password and IP address of the endpoint.
- Download log files from the endpoint for further local analysis.
- Parsing and formatting log files for easy analysis.
- Find indicators of compromise and patterns of behavior of the attacker.
- Obtain general statistics on the attack, or state the absence of indicators of compromise, and hence the attack itself.



```
There was a network scan

Start Time: May 19 15:34
End Time: May 19 15:34
Attacker IP: 192.168.186.195
Attacker source port: 36617



There was brute force attacke
Here is additional infotmation about attack

Start Time: May 19 18:32
End Time: May 19 21:04
Count: 114
Count of possible breached users: 359
Logins of possibly breached users: ['msfadmin', 'root', 'root', 'root', 'root',
```

✓ **exploitation of the vsftpd vulnerability**
✓ **brute force attack**
✓ **scanning of open ports**

## Acknowledgments

The research had been performed in the framework of International Project of CRDF Global “Developing software and hardware complex for dynamical authentication of information processing devices in a corporate network for cybersecurity purposes”, supported by the U.S. Department of State, the Bureau of European and Eurasian Affairs. Grant Agreement: G-202102-67366.

CRDFGLOBAL
INSPIRED BY PEOPLE | DRIVEN BY SCIENCE

## Conclusion

Manual analysis of attacks on endpoints was performed. As a result, patterns and indicators of compromise were detected, which were then used in the program to automatically detect these attacks. Three attacks were detected, namely: open port scanning, brute force, and exploitation of vulnerable software. The attack of the man in the middle was not detected due to the lack of his traces at the end point. This attack is best detected using network equipment log files, which contain records of packets being sent between all points on the network, as well as records of devices connected to that network.

The program is implemented in Python and tested in the following ways: testing on log files from previous attacks, testing on log files without traces of attacks and testing on log files generated during re-simulation of attacks. The program was proven to work as a result of multiple simulations and the extent to which it speeds up the analysis of attacks.

Further research will focus on expanding the range of endpoint attacks.

Ministerstwo Edukacji i Nauki

Dofinansowano z programu „Doskonała nauka” Ministra Edukacji i Nauki