https://doi.org/10.48009/3_iis_2020_105-116

*Issues in Information Systems*
*Volume 21, Issue 3, pp. 105-116, 2020*

# LESSONS ON THE POWER OF KNOWLEDGE FOR CYBER DEFENSE FROM SUN TZU'S *THE ART OF WAR*

***Ping Wang, Robert Morris University, wangp@rmu.edu***
***Hubert D'Cruze, University of Maryland, hubert.dcruze@yahoo.com***

## ABSTRACT

*As cybersecurity vulnerabilities emerge with more dependence on digitization in various industries, there have been increasing challenges in defending against various cyber threats and attacks for all types of organizations including critical infrastructure facilities. Significant research is needed to address such challenges. The Art of War, a masterpiece of military strategies and tactics by Sun Tzu over 2,500 years ago, has been applied to strategic management and tactical operations in a wide range of fields, including cybersecurity and information warfare. This research paper draws upon the power of knowledge from Sun Tzu's classic work and proposes a knowledge-based model for cyber defense. The model focuses on the role of knowledge (and the lack of knowledge) of vulnerabilities of yourself and your opponent in cyber defense. The proposed model is illustrated with simulations of knowledge discovery for cyber defense with penetration testing using a virtual network environment.*

**Keywords**: Art of war, cyber defense, knowledge, knowledge discovery, vulnerabilities, penetration testing

## INTRODUCTION

Industries and organizations around the world have become increasingly dependent on information technology and cyberspace for innovation and productivity. Accordingly, cybersecurity vulnerabilities, threats, and attacks have been on the rise and present a serious challenge for all types of organizations including critical infrastructure facilities. For example, supervisory control and data acquisition (SCADA) systems, the most common type of digital infrastructure and ICS (industrial control system) responsible for monitoring and controlling intelligent networks, have become a major target for malicious cyberattacks (Bracho, Saygin, Wan, Lee, & Zarreh, 2018). In the United States, the latest report by Government Accountability Office (GAO), the nonpartisan congressional watchdog, has concluded that the electric grid dependent on ICS networks and devices is more vulnerable to cyberattacks with significant risks (GAO, 2019). The cybersecurity vulnerabilities could pose a challenge to national security as well. The fact that our critical economic and military systems are so vulnerable to cyber war makes them more attractive and tempting for opponents to attack especially in times of tensions (Clarke & Knake, 2010).

The increasingly sophisticated cyber threats and attacks make it more challenging for organizations and nations to defend their cyber space and critical assets due to a lack of true knowledge and understanding of the vulnerabilities and threats. Overloading data does not necessarily lead to true and useful knowledge. Cybersecurity analysts and responders often have to rely on incomplete and uncertain information for decision making and response as they are swamped with too much "diverse and noisy" data for them to assess the cyber threat adequately (Booker & Musman, 2019). The evolution of the next-generation digital technologies such as Internet of Things (IoT) and artificial intelligence (AI) creates many new cybersecurity vulnerabilities, including state-sponsored adversaries and threats to IoT systems, elections, and public utilities; Organizations with the best knowledge of the threat landscape will be the best prepared to defend against increasing cyberattacks (Booz Allen Hamilton, 2019).

Knowledge of the adversary and yourself is highly valued in *The Art of War*, a classic of military strategies and tactics by Sun Tzu in the 5th century B.C., which has now been found applicable to a wide range of fields from military to business management as well as cybersecurity. Knowing the hacker's motivation, goal, and likely target as well as our own weaknesses will help us properly prepare for and defend against cyberattacks (Madsen, 2017). For example, knowledge of the common techniques and tools of ransomware used by attackers is found to be a powerful defense

against ransomware attacks (Dunn, 2019). On the other hand, lack of knowledge at various extent may cause different decisions in responding to online security risks (Wang, 2013). Lack of knowledge also adds to the difficulty for security analysts to make decisions under risk and uncertain conditions (M'manga et al., 2019). Vulnerability assessment and penetration testing are an important method for gaining knowledge and discovering and addressing security vulnerabilities.

The knowledge factor is a significant and complex factor for cybersecurity research. Knowledge is relative to ignorance or the lack of knowledge, which may lead to different consequences. Knowledge or the lack of knowledge may involve you and your adversary. This study will focus on the factor of knowledge and the lack of knowledge involving the defender and the adversary. The goal of the study is to contribute a proposed knowledge model for cyber defense illustrated with vulnerability assessment and penetration testing simulations. The following sections will review the relevant theoretical background, explain the proposed model, describe the simulation method, and discuss the findings from the simulation.

## BACKGROUND

Knowledge is a strategic factor critical to the outcome of a warfare in Sun Tzu's *The Art of War.* Sun Tzu's concept of knowledge falls into three categories of awareness and assessment of the strengths and weaknesses of yourself and the enemy as seen from his following statements:

- If you know the enemy and know yourself, you need not fear the result of a hundred battles.
- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
- If you know neither the enemy nor yourself, you will succumb in every battle.
  (Sun, trans. 1910, p.45)

A more accurate translation for the first statement listed above is "Know the enemy and know yourself, and you can fight a hundred battles with no danger of defeat" (Michaelson & Michaelson, 2003). So this statement by Sun Tzu lays out the best scenario of knowledge – having knowledge of the strengths and weaknesses of both yourself and the adversary – so you can win every battle with a 100% success rate. The second statement means that you can only have a 50% success rate if you have knowledge of yourself but lack knowledge of your adversary. The third statement means that you have 0 or no chance of winning if you lack knowledge of yourself and your adversary. These scenarios and concepts of knowledge and lack of knowledge apply to the domain of cyber defense and offense as well. For example, knowing the cyberwarfare capabilities of yourself and those of the adversary is essential for victory in the cyber domain (Wilson, 2018).

There are two conditional knowledge-related essentials for victory in Sun Tzu's *The Art of War:*

1. He will win who knows when to fight and when not fight.
2. He will win who knows how to handle both superior and inferior forces.
   (Sun, trans. 1910, p.45)

The first essential condition for victory is knowing the best timing or opportunity for taking the offensive or defensive. The second essential condition for victory is the knowledge of how to deal with stronger and weaker forces. These essential knowledge conditions apply to the cyber domain as well. Knowing the best time and location for battle and the strengths and weaknesses of our own cyber forces and those of the adversary is essential to securing our cyberspace (Wilson, 2018).

Security vulnerabilities are weaknesses that have no or poor defense and become the low-hanging fruit or prime target for attacks. Sun Tzu says: "You can be sure of succeeding in your attacks if you only attack places which are undefended … You can ensure the safety of your defense if you only hold positions that cannot be attacked" (Sun, trans. 1910, p.58). The generic pronoun *you* here is used for both the attacker and defender, and the defense and attack positions could apply to anyone, including us and our opponents. The vulnerable or weak spots may apply to our vulnerabilities or those of our opponents. Knowledge overpowers ignorance or lack of knowledge in both attack and defense situations as Sun Tzu states further on the subject of weaknesses and strengths: "A general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to

attack" (Sun, trans. 1910, p.58). In other words, the attack will succeed if the attacker knows the opponent's vulnerabilities and poor defense which the opponent does not even know; the defense will be successful if the defender knows his vulnerabilities and how to defend them well which the opponent does not know. Cyber warfare needs both offensive and defensive capabilities and keeping knowledge of our own vulnerabilities or potential entry points for attacks will lower the chances of successful attacks by our adversary (Wilson, 2018).

Sun Tzu has consistent emphasis on the significance of discovering vulnerabilities for mitigation or exploitation in *The Art of War*. Sun Tzu sees the opponent's weaknesses as opportunities for victory in his statement "To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself" (Sun, trans. 1910, p.47). He compares strengths and weaknesses to a stone and an egg: "That the impact of your army may be like a grindstone dashed against an egg – this is effected by the science of weak points and strong" (Sun, trans. 1910, p.52). The weak points are those undefended and easy targets for exploitation. "You can be sure of succeeding in your attacks if you only attack places which are undefended" (Sun, trans. 1910, p.58); "So in war, the way is to avoid what is strong and to strike at what is weak" (Sun, trans. 1910, p.62).

Sun Tzu also discusses the importance of gathering knowledge or intelligence about the opponent while making ourselves invisible to the opponent: "By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided" (Sun, trans. 1910, p.59). He continues to explain the division of the opponent as a result of lack of knowledge: "The spot where we intend to fight must not be made known; for then the enemy will have to prepare against a possible attack at several different points" (Sun, trans. 1910, p.60). Sun Tzu shares his thoughts on the importance of using spies for "foreknowledge" or intelligence gathering:

> Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge [knowledge of the opponent's dispositions] … Now this foreknowledge cannot be elicited from spirits; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy's dispositions can only be obtained from other men [spies]. (Sun, trans. 1910, pp.130-131).

While encouraging the use of spies for reconnaissance, Sun Tzu emphasizes our defense against spying to minimize the opponent's knowledge of us: "In making tactical dispositions, the highest pitch you can attain is to conceal them; conceal your dispositions, and you will be safe from the prying of the subtlest spies, from the machinations of the wisest brains" (Sun, trans. 1910, p.62).

Applicable to the cybersecurity domain, vulnerability identification is essential knowledge that is critical to cybersecurity risk assessment and management. Identifying our own vulnerabilities will be valuable to our risk mitigation and help to strengthen our defense whereas knowing the opponent's vulnerabilities will be useful intelligence for victory in offense. Footprinting, port scanning, enumeration, and pentesting are important methods and techniques to discover and identify security vulnerabilities. Footprinting is an initial process of reconnaissance or gathering information such as operating systems about a target system or network using passive and/or active tools and techniques; Port scanning is a method of discovering open and vulnerable ports and services running on a target system or network using scanning tools, such as Nmap; Enumeration is a step further to extract more specific knowledge about a target system or network including resources, shares, network typology and architecture, usernames, groups, and recent logins (Simpson & Antill, 2017). Pentesting (or penetration testing) is typically a sophisticated, authorized, and simulated "attack" or test on an organization's network and systems on a regular basis in order to discover weaknesses that can be exploited (Whitman & Mattord, 2019).

Valuable cyber defense knowledge can be obtained through the knowledge discovery or reconnaissance methods. For example, the MITRE Corporation conducts regular research and provides two useful community knowledge resources on known cyber attacks and vulnerabilities: (1) The Common Attack Pattern Enumeration and Classification (CAPEC) that lists and categorizes cyber attack patterns and methods used for exploiting hardware and software vulnerabilities (MITRE, 2020a); (2) The Common Vulnerabilities and Exposures (CVE) that lists the CVE character, identifier, and description of known cybersecurity vulnerabilities (MITRE, 2020b). The identifiers, descriptions, and attributes of attacks and vulnerabilities are included in the Goal and Effect modelling of the goals and damage effects of various cyber attacks, including social engineering, reconnaissance, privilege escalation, forgery, denial of service, command and control, exfiltration, destroy device, spreading, resource consumption, and unknown attacks (Ahn, Kim, & Lee,

2020). It is important to include unknown attacks, such as Zero Day attacks, to motivate the defenders to increase their awareness and knowledge while reducing their ignorance.

Knowledge and lack of knowledge (or ignorance) are relative to each other, so one's power from knowledge will increase if the opponent's knowledge decreases and ignorance grows. In addition to obscuring and hiding yourself to be invisible to your opponent, deception can be used to mislead and minimize your opponent's knowledge. Sun Tzu underscores the strategies of deception in *The Art of War*:

> 18. All warfare is based on deception.
>
> 19. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.
>
> 20. Hold out baits to entice the enemy. Feign disorder, and crush him.
>
> 21. … Pretend to be weak, that he may grow arrogant.
>
> (Sun, trans. 1910, p.62).

The strategy of deception has been applied to the cyber defense domain as well. For example, honeypots are a typical deceptive strategy using a bait to lure the attackers into a fake system to track and distract them. Apparently, Sun Tzu showed his understanding of the honeypot concept 2,500 years ago (Wilson, 2018). Deception strategies and tactics can be incorporated into cyber defense modelling to cause confusion and distraction in the adversary, such as by broadcasting fake SSID and hidden fake SSID for deceived WiFi access to deter snooping or by exposing intentional vulnerabilities like deceptive passwords or CAPTCHA mechanisms to allow attackers access to deceptive services (Faveri, Moreira, & Amaral, 2018). The implementations and deployment of deceptive strategies and tactics in cyber defense help to strengthen your cyber defense by minimizing the adversary's knowledge of your systems, strengths, and vulnerabilities.

## PROPOSED MODEL

This study proposes a knowledge model for cyber defense based on Sun Tzu's defensive knowledge principles. The proposed model consists of two parts: (1) The Knowledge and Goals Matrix; (2) The Knowledge Discovery Process. The Knowledge and Goals Matrix is to formulate the knowledge status and desired goals and consequences for yourself relative to your opponent in the cyber defense domain. The overall goal is to benefit the defense of yourself against your opponent in cyber defense. Table 1 below shows the Knowledge and Goals Matrix. The Knowledge Discovery Process part outlines the process and steps of knowledge discovery and assessment in the cyber defense domain. Figure 1 below shows the Knowledge Discovery Process.

**Table 1.** Knowledge and Goals Matrix

| | **Knowledge** | **Goals** |
|---|---|---|
| **Yourself** | • Know your own vulnerabilities<br>• Know how to mitigate your own vulnerabilities<br>• Know how to hide your assets and vulnerabilities from your opponent<br>• Know how to set up fake vulnerabilities | • To minimize your vulnerabilities<br>• To assess and manage your vulnerabilities and risks<br>• Minimize your opponent's knowledge of your vulnerabilities<br>• To mislead, misinform, distract, and deceive your opponent |
| **Opponent** | • Know your opponent's strengths<br>• Know your opponent's assets and vulnerabilities<br>• Know how to discover your opponent's vulnerabilities | • To be aware of threats and avoid striking the strong spots of your opponent<br>• To exploit the vulnerabilities of your opponent<br>• To maximize your knowledge of your opponent |

In the Knowledge and Goals Matrix in Table 1, knowledge of yourself is essential. For example, you should scan your critical systems and networks regularly for awareness of your own vulnerabilities, such as missing software packages, updates, and insufficient network screening or IDS/IPS protection or inadequate security policies, to discover weaknesses for the goal of minimizing them. Security vulnerabilities are weaknesses that may exist in people, processes, and technical systems, and not all vulnerabilities are high risks (Hodson, 2019). You should know how to properly manage the vulnerabilities by analyzing and assessing the weaknesses and know what measures and actions to take to mitigate and minimize the critical vulnerabilities and risks for yourself. Knowing your own assets and vulnerabilities, you should also know how to hide them or keep them "invisible" from the opponent to reach the goal of minimizing your opponent's knowledge of your assets and weaknesses. In addition, you should know how to set up fake vulnerabilities or decoys such as a honeypot or honeynets to lure intruding opponents to achieve the goal of deceiving your opponents by misleading, misinforming, or distracting them.

Knowledge of your opponent(s) is also critical for important cybersecurity goals. First of all, knowing your opponent's strengths adequately will motivate you to improve your defense to handle potential threats from your opponent; it will also help you avoid striking the strong spots of your opponent with high risks of losses if offense becomes necessary. More importantly for cyber defense, you should know your opponent's critical assets and vulnerabilities so that you are prepared to exploit the vulnerabilities successfully if necessary. The knowledge may come from a variety of sources, including indirect or second-hand sources. The goal here is to maximize your best knowledge of your opponent's critical assets and weaknesses. To achieve this goal, you need to know how to discover the knowledge by first-hand methods including reconnaissance efforts such as footprinting, scanning, enumeration, and pentesting.

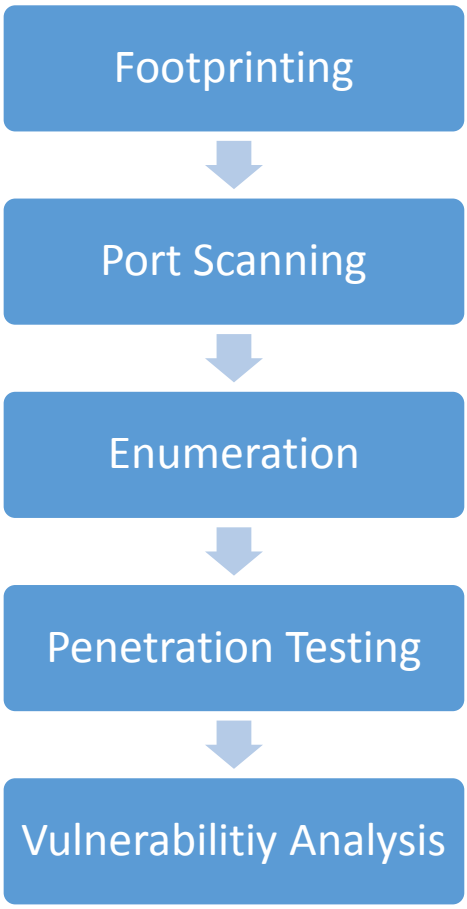


**Figure 1.** Cyber Defense Knowledge Discovery Process

Footprinting is the initial step in the Cyber Defense Knowledge Discovery Process in Figure 1 above. Footprinting is also known as reconnaissance commonly used by black-hat, white-hat, and gray-hat hackers in their discoveries of computer network systems. Footprinting is a process that passively gathers information about a target from many diverse sources. It is the act of using different tools and techniques to acquire as much information as they can before exploiting any vulnerabilities of the target (Hassan & Hijazi, 2018; Oriyano & Gregg, 2013). Footprints are regarded as the first stage of a system compromise conducted by individuals wishing to escalate key system privileges with a view to exploiting known system vulnerabilities (Wren, Reilly, & Berry, 2010). Footprinting can be used to discover information and vulnerabilities of your own or your opponent's systems, networks, and security controls. This is in line with Sun Tzu's thought of winning a hundred battles and winning thousands of miles away with no risk of defeat if you know the enemy and know yourself (Wang & Lin, 2018).

Port Scanning often occurs after the initial footprinting. Port scanning is used to identify open ports and services available on a network host. Once the hacker has sufficient footprints of the target, then the hacker performs scanning of the target network or system to seek open ports and related services (Shah et al., 2019). The goal of performing port scanning is to identify open and closed ports as well as the services running on a given system. Port scanning forms a critical step in the reconnaissance or intelligence knowledge discovery process because the hacker needs to identify what services are present and running on a target system prior to finding any vulnerabilities for exploitation. Port scanning also helps to determine the course of action in future steps because once the nature of running services are identified, proper tools can be selected from the hacker's toolbox (Oriyano & Gregg, 2013).

Enumeration is usually the next step in cyber reconnaissance that uses active connections to the target system to perform more aggressive, methodical, and more organized information gathering. During enumeration you should be able to extract information such as usernames, machine names, shares, and services from a system as well as other information depending on the operating environment. Unlike previous steps, you are initiating active connections to a system in an effort to gather the information you are seeking. Consequently, you should consider this phase a high-risk process that involves extra effort and precision to retrieve sufficient information before you can assess the strengths and weaknesses or vulnerabilities of the system (Oriyano, 2014).

Penetration testing or pentesting is more aggressive knowledge discovery to test the vulnerabilities of the target system. Pentesting helps to determine which vulnerabilities are exploitable and the degree of information exposure or network control that the organization could expect an attacker to achieve after successfully exploiting a vulnerability. Pentesting may be performed by authorized pentesters to discover your own vulnerabilities or done by Black-hat hackers on target systems stealthily and without authorization. Authorized pentesting may not be the same as real hacking due to necessary limitations placed on penetration tests conducted by "white hats" (Vacca, 2017). The use of pentesters for discovering and invasive testing of the target is consistent with the use of spying techniques for intelligence gathering to discover and exploit vulnerabilities within target systems and networks.

Once the vulnerabilities are identified and tested from the previous steps, the final step for the knowledge discovery process is vulnerability analysis. This is to analyze and assess the potential impact of the vulnerabilities with consideration of the associated threats and risks. Since not all vulnerabilities are risks with high level of impact, it is necessary to categorize the weaknesses and identify high-risk vulnerabilities. The goal of this step is to prioritize the potential threats and risks of losses in case of cyber attacks in order to better manage the risks in cybersecurity (Muckin & Fitch, 2019).

## METHODOLOGY

This study uses a virtual simulation approach to illustrate the proposed knowledge discovery model for cyber defense. The virtual network for simulation includes three virtual machines running Kali Linux, Windows 7, and Windows 10 respectively on the VirtualBox platform. VirtualBox is a free cross-platform virtualization application provided by Oracle. VirtualBox offers an ideal platform for simulation as it can run as many virtual machines and guest operating systems simultaneously as the host hardware can support. VirtualBox is widely used for simulation, testing, and disaster recovery as it allows easy switch to the saved snapshot of a previous virtual machine state if something goes wrong. Kali Linux is an enterprise-ready security auditing Linux distribution based on DebianGNU/Linux. Kali primarily serves cybersecurity professionals and IT administrators, enabling them to conduct advanced reconnaissance and penetration testing, forensic analysis, and security auditing. Kali comes with a number of security tools for knowledge discovery and analysis, including vulnerability analysis tools such as Nmap/Zenmap and exploitation tools like Metasploit.

The simulation network for this study uses the three virtual machines on VirtualBox to conduct sample scanning and pentesting for reconnaissance and knowledge discovery of the target system information and vulnerabilities. The reconnaissance and knowledge discovery activities are initiated from the Kali Linux virtual machine (VM). The Windows 7 VM and Windows 10 VM serve as the target machines on the network. The following section presents and discusses the key findings from the simulation.

## FINDINGS & DISCUSSIONS

Figure 2 below shows the scan and discovery results using Zenmap installed on the Kali Linux VM. Zenmap is the official Nmap Security Scanner GUI utility for network discovery and security auditing. Like Nmap, Zenmap uses raw IP packets in novel ways to determine available hosts on the target network, open ports, and running services and operating systems and versions, as well as any defensive packet filters or firewalls in use. Nmap/Zenmap was designed

to rapidly scan large networks but it works fine on single hosts. The scan in Figure 2 targets the 10.0.0.0/24 network using the command of **nmap -sV -T4 -O -v -F 10.0.0.0/24**. The highlighted target host is the Windows 7 VM with the IP of 10.0.0.78. The highlights in Figure 2 show rich information gathered about the target, including open ports, services running, and operating system (Windows 7 Enterprise 7601 Service Pack 1). The comprehensive information gathered here by Zenmap represents the result of footprinting, port scanning, and enumeration. This knowledge is very important for the next step of finding and testing the vulnerabilities on the target. This scan can be performed on an internal network for self-discovery or on an external network to gain knowledge of your opponent.

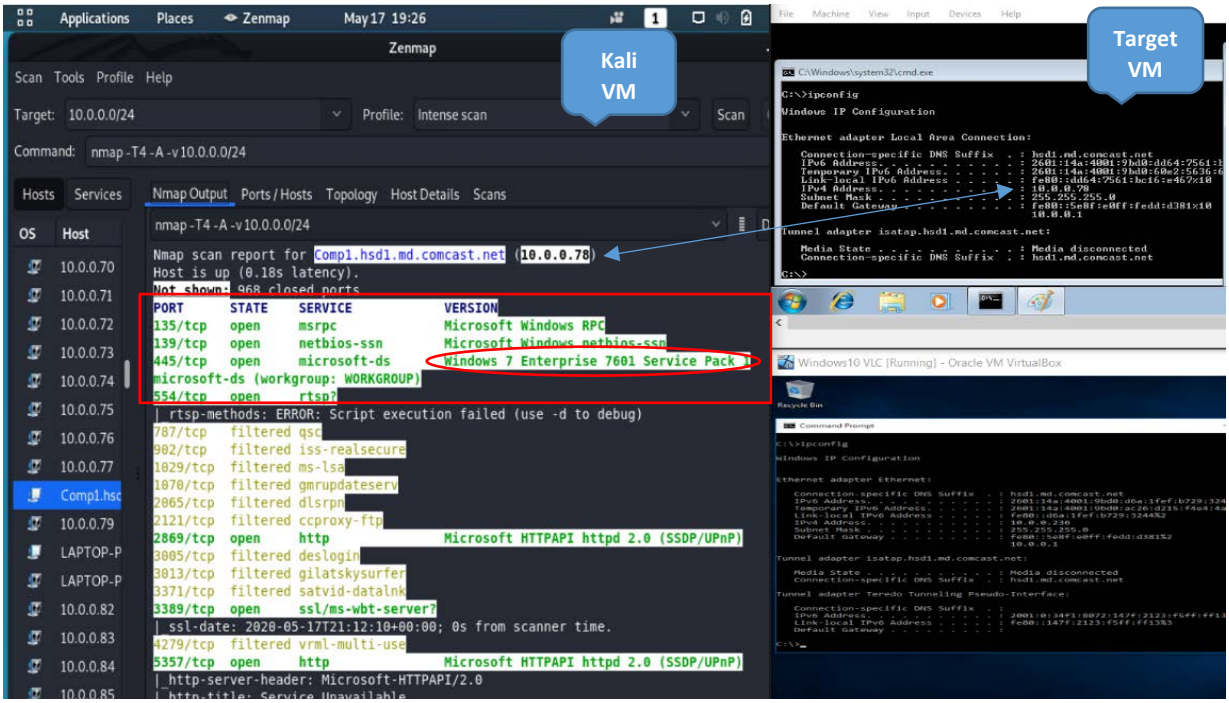


**Figure 2.** Zenmap Scan Results

The next step is to pentest and discover the vulnerabilities associated with information gathered above. Executing the command **locate *vul*.nse"** in Nmap on Kali VM will output the known vulnerability scripts shown in Figure 3 below.

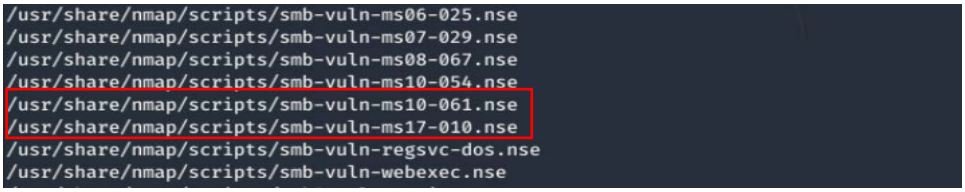


**Figure 3.** List of Known Vulnerability Scripts (excerpt)

Any of the scripts on the list in Figure 3 can be tested on a target machine to see if it is vulnerable. We randomly selected the two scripts in the red rectangle in Figure 3 and tested them on the target machine of Windows 7 VM (10.0.0.78) by running the following two Nmap scripts on the Kali VM:

1) **nmap -v -p445 -script smb-vuln-ms10-061.nse 10.0.0.78**
2) **nmap -v -p445 -script smb-vuln-ms17-010.nse 10.0.0.78**

The details of the vulnerabilities are available in the Common Vulnerabilities and Exposures (CVE) online database (MITRE, 2020b). The test scan report for the vulnerability **smb-vuln-ms10-061** (Printer Spooler Service Vulnerability) comes up negative (Access Denied) indicating that the target machine is not vulnerable as shown in Figure 4 below.

```
Nmap scan report for Comp1.hsd1.md.comcast.net (10.0.0.78)
Host is up (0.00059s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

**Figure 4.** Test Result for **smb-vuln-ms10-061**

The test scan report for the second selected vulnerability **smb-vuln-ms17-010** is positive as shown in Figure 5 below, which indicates that the target is vulnerable to **smb-vuln-ms17-010** (Remote Code Execution vulnerability in Microsoft SMBv1 servers) with a high risk factor at the critical level.

```
Nmap scan report for Comp1.hsd1.md.comcast.net (10.0.0.78)
Host is up (0.00067s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

**Figure 5.** Test Result for **smb-vuln-ms17-010**

A further pentesting step is done to validate if the vulnerability on the Windows 7 VM can be exploited by running the exploit script in the Metasploit Framework console on the Kali Linux VM as shown in Figure 6 below:

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.0.78
RHOSTS => 10.0.0.78
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.0.100
LHOST => 10.0.0.100
msf5 exploit(windows/smb/ms17_010_eternalblue) > set TARGET 0
TARGET => 0
msf5 exploit(windows/smb/ms17_010_eternalblue) > set encoder generic/none
encoder => generic/none
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.0.100:4444
[*] 10.0.0.78:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.0.78:445         - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.0.78:445         - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.0.78:445 - Connecting to target for exploitation.
[+] 10.0.0.78:445 - Connection established for exploitation.
[+] 10.0.0.78:445 - Target OS selected valid for OS indicated by SMB reply
```

**Figure 6.** Metasploit Test Script and Result for **smb-vuln-ms17-010**

The test result in Figure 6 shows that the **smb-vuln-ms17-010** vulnerability (also known as "Eternal Blue") can be exploited on the target Windows 7 VM. This penetration test validates the discovered knowledge of the vulnerability on this Windows 7 machine.

An additional simulation test of a honeypot is conducted on the virtual network to deceive, track, and identify intruders. The honeypot application is PentBox version 1.8 running on the Kali Linux VM with an intentionally attractive setup of no firewalls and all ports open. The honeypot is activated for fake Telnet connections at port 23 as shown in Figure 7 below and detects an intrusion attempt from 10.0.0.88, the Windows 10 VM. The intrusion attempt is also recorded in the log file shown in Figure 8 below that can be used for further analysis and discovery of the intruder or opponent.

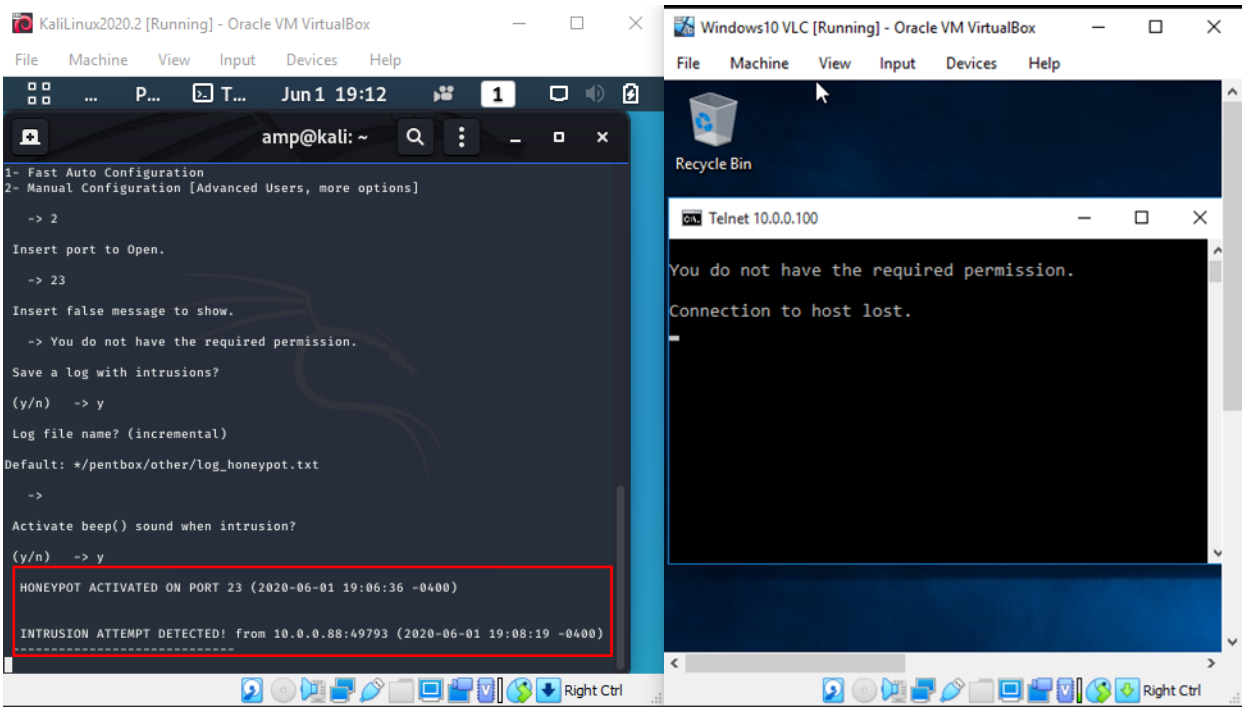


**Figure 7.** Intrusion Attempt Detected on Honeypot

The final step of the vulnerability knowledge discovery process is to report the findings for vulnerability analysis and risk management. The results of footprinting, scans, penetration tests, and the nature and the risk factor of the vulnerabilities will be useful data for business impact analysis and risk management decisions.

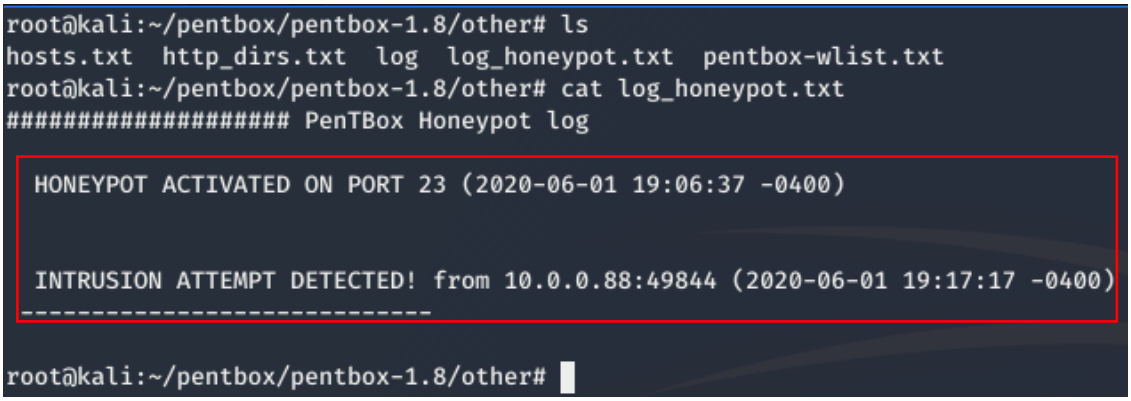


**Figure 8.** Honeypot Log of Intrusion Attempt

## CONCLUSION

This study draws upon the power of knowledge in Sun Tzu's *The Art of War* and proposes a knowledge model of discovering vulnerabilities for cyber defense. The model consists of the goals of knowing yourself and the adversary as well as the knowledge discovery process that includes footprinting, port scanning, enumeration, pentesting, and vulnerability analysis. The proposed model is illustrated with simulated tests in a virtual network using VirutalBox with Kali Linux and Windows virtual machines.

Creative thinking is essential in the future of cyber defense as more unforeseeable threats emerge. Classics like Sun Tzu's *The Art of War* are valuable sources of food for thoughts for cyber defense. This study is only a preliminary effort on this topic. There could be other inspirational lessons for cybersecurity strategies and management from *The Art of War* that are worth pursuing in future research. Future studies may also focus on the impact of principles in *The Art of War* on specific cybersecurity cases and solutions.

## REFERENCES

Ahn, M.K., Kim, Y.H., & Lee, J. (2020). Hierarchical multi-stage cyber attack scenario modeling based on G&E model for cyber risk simulation analysis. *Applied Sciences*, *10*(1426), 1-16.

Booker, L.B., & Musman, S.A. (2019). A model-based, decision-theoretic perspective on automated cyber response. Retrieved from https://arxiv.org/abs/2002.08957

Booz Allen Hamilton. (2019). 2020 Cybersecurity Threat Trends Outlook. Retrieved from www.boozallen.com

Bracho, A., Saygin, C., Wan, H., Lee, Y., & Zarreh, A. (2018). A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems. *Procedia Manufacturing*, *26*(2018), 1116-1127.

Clarke, R.A., & Knake, R.K. (2010). *Cyber war: The next threat to national security and what to do about it.* New York, NY: HarperCollins Publishers Inc.

Dunn, J.E. (2019). How ransomware attacks. Retrieved from https://nakedsecurity.sophos.com/2019/11/15/how-ransomware-attacks

Faveri, C.D., Moreira, A., & Amaral, V. (2018). Multi-paradigm deception modeling for cyber defense. *The Journal of Systems and Software, 141*(2018), 32-51.

GAO (U.S. Government Accountability Office). (2019, August). Critical infrastructure protection: Actions needed to address significant cybersecurity risks facing the electric grid. Retrieved from https://www.gao.gov/

Hassan, N. A., & Hijazi, R. (2018). Technical footprinting. Open Source Intelligence Methods and Tools, 313-339. doi:10.1007/978-1-4842-3213-2_8

Hodson, C.J. (2019). *Cyber risk management: Prioritize threats, identify vulnerabilities, and apply controls.* New York, NY: Kogan Page Limited.

Madsen, T. (2017). Sun Tzu's 'The Art of War' for Cybersecurity. *InfoSecurity.* Retrieved from www.infosecurity-magazine.com/opinions/sun-tzus-art-of-war-cybersecurity/

Michaelson, G., & Michaelson, S. (2003). *Sun Tzu for success.* Avon, MA: Adams Media Corporation.

MITRE. (2020a). Common Attack Pattern Enumeration and Classification (CAPEC). Retrieved from http://capec.mitre.org/index.html

MITRE. (2020b). Common Vulnerabilities and Exposures (CVE). Retrieved from http://cve.mitre.org/

M'manga,A., Faily,S., McAlaney, J., Williams, C., Kadobayashi, Y., & Miyamoto, D. (2019). A normative decision-making model for cyber security. *Information & Computer Security, 27*(5), 636-646.

Muckin, M., & Fitch, S.C. (2019). A threat-driven approach to cyber security. Retrieved from https://www.lockheedmartin.com/

Oriyano. (2014). *CEH: Certified Ethical Hacker version 8 study guide.* Sybex.

Oriyano, S., & Gregg, P.M. (2013). *Port scanning. In Hacker techniques, tools, and incident handling (2nd ed..).* Burlington, MA: Jones & Bartlett Learning.

Shah, M., Ahmed, S., Saeed, K., Junaid, M., Khan, H., & Ata-ur-rehman. (2019). Penetration testing active reconnaissance phase – optimized port scanning with Nmap tool. *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. doi:10.1109/icomet.2019.8673520

Simpson, M.T., & Antill, N. (2017). *Hands-on ethical hacking and network defense.* Boston, MA: Cengage Learning.

Sun, T. (1910). *The art of war* (L. Giles, Trans.). BookYards.com.

Vacca, J.R. (2017). *Computer and information security handbook (3rd ed.).* Waltham, MA: Morgan Kaufmann.

Wang, P. (2013). Decision under uncertainties of online phishing. In S. Ao & L. Gelman (Eds.), Electrical engineering and intelligent systems (pp. 207-218). New York, NY: Springer Science+Business Media, LLC.

Wang, H., & Lin, W. (2018). Analysis of the art of war of Sun Tzu by text mining technology. *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 626-628.

Whitman, M.E., & Mattord, H.J. (2019). *Management of information security.* Boston, MA: Cengage Learning.

Wilson, R. (2018). Sun Tzu and the art of cyberwar. *Defense AT&L, January-February 2018,* 30-34.

Wren, C., Reilly, D., & Berry, T. (2010). Footprinting: A methodology for auditing e-system vulnerabilities. 2010 *Developments in E-systems Engineering, 1,* 263-267.