Cyberattacks are on the rise, costing companies millions to tenth of millions in average.[1, 2] Stolen private information and denial of service also affected individuals extensively. Attackers are becoming more proficient than our system administrators in using preinstalled system management tool[3]. An example is the massive global ransomware cyberattack known as “WannaCrypt” or “WannaCry”. It affected more than 150 countries whereby tenth over thousands of computers were infected. Critical infrastructure like hospital were also affected which forced them to partially stop servicing.[4]

File-based cyberattacks has been a norm since the launch of computer system while file-less cyberattacks were discovered in 2010 and has been on a rise since then. File based cyberattack, also known as malware, is easily trackable by Security Analyst. However, recent high-profile attack uses “living off the land” technique where it is a file-less attack and leverages heavily on legitimate system management tool such as Windows Management Instrumentation.[3] These attacks normally goes under the radar of security protection software and is nearly impossible to track as it is usually stored in very unusual places such as the Registry.[5] These legitimate system management tool brings convenience to system admin, however the flip side is that it also increases the risk of the system being compromise.

One of those system management tool is Windows Management Instrument, also known as WMI. WMI is preinstalled since the early Windows 2000 Operating System. It is a Web-Based Enterprise Management System for accessing system information in an enterprise environment. Administrator can utilize Windows Management Instrumentation Command-line to interact with WMI. WMI consist of various privileged functions such as retrieving sensitive system data, script automated task, manipulate system registry and many more. This is also where WMI becomes dangerous, attackers are using creative ways to abuse WMI. An example is using WMI to inject payload, normally an executable script, into the system registry and bind the payload to a startup event. Hence, the malicious script will be automatically executed upon computer startup and this technique hijacked the victim to actively listen to Control and Command Server.[6] One example about cyberattack that utilized WMI is NotPetya, a cousin of WannaCry. NotPetya make use of PsExec and WMIC to spread its infection. Although NotPetya is not as deadly compared to WannaCry, but it infected over 12,500 machines and further the possibilities of WMI based attack.[7]

This paper presents the study on both offensive and defensive component of WMI security. For offensive component, WMI is used to remotely abuse and attack victim computer without any use of payload while in the case of defensive component, a defensive tool will be created to mitigate and ultimately prevent WMI-based attack. Both components are then used to compiled into a penetration testing tool for cooperate usage.

[1] 1E, "Cyber Attacks Is The Rise A Surprise?," *MIT SOLAN CIO SYMPOSIUM 2015,* 2015.

[2] K. Chandrasekar *et al.*, "2017 Internet Security Threat Report," *ISTR,* vol. 22, April 2017 2017.

[3] M. Graeber, "Abusing Windows Management Instrumentation WMI To Build A Persistent, Asynchronous, And Fileless Backdoor," *Black Hat USA 2015,* 2015.

[4] M. N. C. S. I. R. Team, "The WannaCry Ransomware Attack," *CERT-MU,* 2017.

[5] W. Ballenthin, M. Graeber, and C. Teodorescu, "Windows Managment Instrumentation (WMI) Offense, Defence, And Forensics," *FireEye Blog,* 2015.

[6] M. Graeber, "Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asyncronous, and Fileless Backdoor," *Black Hat 2015,* 2015.

[7] M. N. C. S. I. R. Team, "The Petya Cyber Attack," *CERT-MU,* 2017.