Which Tools Are the Best for the Job

Honor Pledge: I acknowledge that the Capstone Project is an independent study project to be completed individually. On my honor, I have not received aid on my Capstone Project other than what was provided by my faculty mentor and any persons explicitly cited in my work. I further acknowledge that if I have given any aid to another student in this course, the instructor of this course was made aware of my contributions.

Table of Contents

Objective

My project is centered around the use of penetration testing in the subject of cybersecurity. I will learn to use about three tools in depth. These three tools are considered to be some of the most powerful tools in penetration testing. Each of the separate tools all have an individual task they are utilized for. I will provide a compare and contrast with each tool compared to the many other tools that can be used for the same purpose. The purpose of my project will be to prove that they are better than many other tools that are out there. The project will use some of the capabilities and options of each tools and compare the results of each side by side and show how the other tools are sort of inferior in comparison to these tools I have identified. The beginning weeks will consist of me gaining traction with my project by gathering names and the reputations of various tools for each step (recon, enumeration, attacking). Dr. Ali Bicak will be assisting me in locating and learning how to utilize the many options the tools possess. I will be taking advantage of the safe zone network located in 4040 to prevent any damage to Marymount's network and any legal trouble for myself. Next I will begin to learn the many options and settings of the three tools I have listed and how to properly use them. I will provide a tutorial on each of them and provide side by side screenshots of the information and results created from the use of each compared to the other tools chosen in the beginning weeks. The final month will be dedicated to becoming adept with each tool and providing a good enough tutorial that future aspiring pen testers will be able to utilize my tutorials and have a good grasp on how to use them effectively and not harm anyone else unless that is there intention.

Content Advisor

Dr. Ali Bicak is an Associate Professor of Computer Science at Marymount University, teaching computer networking and cybersecurity courses both at the graduate and undergraduate level. In collaboration with other faculty, Dr. Bicak leads Marymount's NSF CyberCorps Scholarship for Service and Cisco Academy programs, and the university's designation as a NSA/DHS Center of Academic Excellence in Information Assurance Education (CAE/IAE) institution.

Prior to joining Marymount, he held positions with the Maryland Center for Telecommunications Research and TeleniX Corporation in Maryland, and the National Research Institute of Electronics and Cryptology in Turkey. In addition to his academic credential in mathematics (bachelors and masters) and computer science (doctorate), he holds a number of professional certifications including CISSP, CAP, CEH, CCAI, CCNA, Network+ and Security+.

Dr. Bicak is also a Certified Information Systems Security Professional (CISSP) with professional experience in design, development, and technical support of network systems. At Marymount, he teaches undergraduate and graduate courses in computer networks and information security. His research interests include routing and security issues in wireless and peer-to-peer networks, discrete mathematics, and cryptology.

Project Plan

I will run through the main features of the main I listed and run them side by side against the competitor tools. For example, I will attempt to establish a reverse shell using Metasploit and attempt to do this with “ICMPSH” tool to see if my one or more attempts on the multiple target systems I have will be successful. With Nmap I will run a scan with computers in different modes to attempt to gain the most information I can on a node on a network while making minimal noise (Noise is activity on a network that could be monitored by another tool or someone trying to prevent attacks on their network.). Another tool for network mapping is called Fing it can help scan a network as well and provide a list of the number of nodes on the system. They will be pitted against each other in how well each one does the amount of information they collect on the target computers and how much traffic they generate that may be malicious. Open Vas is the best in my opinion vulnerability scanner. I will attempt to make the target system vulnerable on purpose and see if each scan will pick up the issues and tell me about it in detail. Retina CS Community is another vulnerability scanner that is ranked highly as well in regards to finding computer vulnerabilities. Each of these tool comparisons will take the most time because of the setting of the target the actual action and recording of the results will take but a moment’s notice. However, for complete understanding of the results and how to properly implement the actions will take the most time. I am current still in the process of learning how to utilize the tools and learning what the results are supposed to be.

Resources

Each of these tools and my workspace will be provided by myself. The tools are all online and free for access. I have received no outside assistance in obtaining my tools for this project.

Project Details

I have not begun this part I am still in the process of learning the terms and actions of each of the tools before I begin performing attacks and actions.

Knowledge

All my knowledge comes from my past research project based on penetration testing tools I have used. Penetration testing is my hobby I often pick tools offline and tinker with them to see what the effects are on my target system in a Virtual Machine I have on my computer. I am also currently in a Cybersecurity class that is based on the Attack/Defense of a computer and is basically the usage of tools for the sole purpose of learning specific kinds of attacks and what they can do to a targets computer. Another class was based on the understanding of the attacks more than actually doing it was my security plus class that I had taken last year. I am in possession of a large amount of books that provide me with the workings of techniques and tools of pro hackers utilize on their targets and how well they workout. I will need to learn a good number of these tools and the process in which they run these scans and drop these payloads on unsuspecting victims.

Risk Factors

There is a large risk in performing test with these tools. As mentioned above each tool can cause significant harm to a computer that is being targeted if the attack is not implemented correctly. I will need to be in a controlled environment which will be provided by the 4040 cyber lab on my own network that I have obtained permission to use from the Network Administrator at Marymount. A misstep or fat fingered command could bring the entire Marymount network down or even get my access to the Marymount network revoked.

References

Sterling, B. (1992). ***The hacker crackdown: Law and disorder on the electronic frontier*****. New York: Bantam Books.**

Clark, B. (n.d.). ***RTFM: Red Team field manual*****.**

Mitnick, K. D., & Simon, W. L. (2005). ***The art of intrusion: The real stories behind the exploits of hackers, intruders, & deceivers*****. Indianapolis, IN: Wiley.**

Scambray, J., McClure, S., & Kurtz, G. (2001). ***Hacking exposed: Network security secrets & solutions*****. Berkeley, CA: Osborne/McGraw-Hill.**

Dean, T. (2010). ***Network guide to networks*****. Boston: Course Technology Cengage Learning.**

Kim, P. (n.d.). ***The hacker playbook: Practical guide to penetration testing*****.**

Kennedy, D. (2011). ***Metasploit: The penetration tester's guide*****. San Francisco: No Starch Press.**

Tanenbaum, A. S. (1992). ***Modern operating systems*****. Englewood Cliffs, NJ: Prentice Hall.**

Erickson, J. (2008). ***Hacking: The art of exploitation*****. San Francisco, CA: No Starch Press.**

Marsh, N. (2015). ***Nmap 6 cookbook: The fat-free guide to network scanning*****. North Charlestown, SC: CreateSpace.**