LEARNING THE ART OF EXPLOITATION

Computer Security

Since 2002 we have had an 84% increase of computer intrusion investigations. Now in order to protect yourself from becoming part of these statistics you must learn how it works.

What this is all about

This projects purpose was to learn how to properly identify if a client computer has any base line security flaws, and from there determine if it’s vulnerable to an attack. Now once I have declared the machine as vulnerable I took the next step by taking advantage of the vulnerability elevating my privileges and setting up a persistent backdoor to exploit further at a later date.

Why?

This is a very touchy topic in a way that frightens some when mentioned, “hacking”. But the fact is it is happening out there and we all are not safe. In order to know what’s safe and what is not you must go through the full, Penetration Testers Lifecycle to be sure.

Reconnaissance
Vulnerability Assessment
DLL Payload Injection
Exploitation
Maintaining Access

“If I had six hours to chop down a tree, I’d spend the first four of them sharpening my axe.”

-Abraham Lincoln

“Thank you to all those contributing to Open source projects”
NMAP PROJECT

DESIGN

WAN

Router/Default Gateway

Windows 8.1 Pro Victim

Kali Linux Attacker
Running Metasploit Community
Running Armitage

NET 499
Spring 2015
Chris Johnson