

Forum:[Hack Forums](#)

Thread: [Intro to the Hacker Methodology](#)

mrflex312 - June 14, 2013, 9:42 pm

Intro to the Hacker Methodology

By Mr Flex

Introduction

During this tutorial I will be introducing you to the hacker methodology. This tutorial is going to be fairly short and sweet but should provide you with a basic methodology you can use when performing a hack or penetration test. I hope that by the end of this tutorial you will understand the steps required for you to perform a successful hacking attack. This is based off of other hacking methodologies I have seen before. I will be posting detailed tutorials on Information gathering – Post Exploitation sometime soon, the goal of this tutorial is just to give you an overview of the various steps in the Hacker Methodology.

Planning

The planning stage is where the attacker defines what objectives they would like to accomplish during their attack. This may include things like intellectual property theft, stealing credit card numbers, website defacement, getting root access (for the fun of getting root access :/) or something else. Who knows maybe the hacker just wants to have a look around the system.

Information Gathering

Information Gathering is the process of gathering information on the target organization. There are two types of information gathering active and passive.

Passive Information Gathering

Passive information gathering is using search engines like Google and Shodan along with databases like the Edgar database and looking at other publicly available records like whois domain name lookups. It also involves things like searching the company website for details about employees. Many company websites are very verbose about the various details of their websites; also remember interns usually know little to anything about security and usually use weak passwords.

Active Information Gathering

Active information gathering is actively probing the network, this includes things like port scanning, banner grabbing and running vulnerability scanners (noisy as hell don't recommend for highly secured environments).

Exploitation

Exploitation is where you actually exploit the target. This can involve things like Web Application attacks like XSRF, XSS and SQL Injection, exploiting software vulnerabilities like Stack Based Overflows, Heap Based Overflows, Off By One vulnerabilities and format string exploits. It also may

involve doing things like performing a DDOS attack, or performing a social engineering attack. Note that you rarely ever use just one exploit you almost always use multiple exploits to get to where you would like to be.

Post Exploitation

Post exploitation where you accomplish the goal you have originally set out to do this may include things like defacing the website, stealing intellectual property etc.

Comments

Let me know what you think! I try to make my tutorials as clear and concise as possible!

My Policy

I am not responsible for anything you do with this tutorial.

Dedication

This tutorial is dedicated to anyone and everyone who understands that hacking and learning is a way to live your life, not just a day job or list of instructions.

Reptilian - June 15, 2013, 8:57 am

Very nice tutorial but it's a bit short.

Keep it going though :)

Conch - June 15, 2013, 11:04 am

3 posts and already contribution? Nice.

This is a great tutorial for beginners.

Keep it up :) You'll fit in nicely.

mrflex312 - June 19, 2013, 2:56 pm

Thanks Conch, Investigator I plan on expanding this post I have posted this tutorial on other forums and have been told it is so I am going to add even more to it when I have a chance.

Baldicus34 - June 19, 2013, 3:24 pm

I've noticed you've used some stuff from other tuts and this is a very nice start to a compilation!

I'm looking forward to you either expanding or making other threads like this!

Pedal - June 19, 2013, 5:37 pm

And the FBI be like...