Protonbolt Penetration Testing

RED TEAM HANDBOOK

PART ONE: Hacking Theory

A guide for new pentesters

w/ notes by M.B.

Reading the information in this document without prior authorisation may constitute a breach of the 1990 Digital Intellectual Property Protection Act, which regulates all attempts to use information technology to perform unauthorised activities. Offenders will be prosecuted immediately upon discovery.

Welcome

If you're reading this, you've passed the rigorous selection tests for our pentesting program. Or, your uncle shared a drink with Bob from HR three months ago. We don't know, and I personally don't really care. The point is, you're a hacker now, and it's my job to get you up to speed. Wait - did I just say "hacker"? In the biz you're called a "pentester": penetration tester, or in other words companies pay you to break in, and then politely tell them how exactly you did it. It's great fun! Trust me, I would know.

This booklet should get you up to speed on the theory behind most of what we do here at Protonbolt, with an emphasis on the human element. Part 2 will give you instructions on how to use certain software packages and common tools (*nmap* etc.) we have installed on your work machine along with exploitation techiques, and Part 3 gives you the boring documentation information so you can write up your exploits in a safe and responsible fashion. Now, without further ado, let's get started!

Table of Contents

Stages of Pentesting

Hacking can take many forms: disassembling a binary, crafting malicious payloads, force-rebooting a memory implant until it spits out the goods, phreaking telephone lines for free calls... However, what we're interested in here is what we call "the full package" - you're given a large (usually corporate) target, mostly free range, and your job is to probe some aspect of the target: for example, the R&D Department or the CEO's machine. You'll need to chain together multiple exploits to get through the layers of security most of our clients employ, and put all your skills to the test. This isn't a computer science class at College!

Checklist

There are six stages to any operation. I've organised them in a handy checklist below:

1. Contract
2. Scouting
3. Identification
4. Penetration
5. Escalation
6. Reporting

Stage One: Contract

This is very important: *Do Not Start a Job Without a Contract*. I'll repeat it again. DO NOT START A JOB WITHOUT A CONTRACT. That is how you get headhunted the wrong way by corporate enforcement squads. Our legal team will handle the setting of any red lines, (un)acceptable exploits, as well as payment for any jobs completed. Once you have a signed contract, you can begin the operation.

Stage Two: Scouting

Scouting is often neglected in movies and books, but it is vital to the success of any mission. Scour any public or personally available sources for information they may have about the target. The important thing is to not spook the target at this stage: operations should be kept above-board and to the public domain as much as possible.

Stage Three: Identification

Your scouting should have shown you some weak links: maybe a branch office has an inattentive security guard. Maybe the CEO likes bars a little too much. Maybe they don't make everyone card in all the time. At this point, you should start creating a map of the structure of the company, mapping out people, technical details, corporate structure etc. Once you have a good idea where the weak points are, it's time for step 4.

Stage Four: Penetration

Here's the fun part. Dial up the network, call the guard and ask for details because "the bank needs to verify your identity", follow someone in, crack the software. Be careful – Now they have a clear reason (especially if the contract isn't widely known) to try and nab you. You may fail, and that's alright. Return to stage two: There's always a weak link somewhere.

Stage Five: Escalation

Now you're in, but you're not winning yet. You might have control of some lowly clerk's shell account, but they don't have the keys to the secret R&D files. You'll need to repeat stages two to four, updating your map and identifying new opportunities for mischief using your new position of power. This will continue until you're the system administrator ("root") or you have enough permissions and privileges to do what you need to. Good luck, and don't get caught.

Where's stage 6 LOL

Techniques and Methods

This next section is a common list of methods used in various stages of the pentesting process. For the sake of our collective sanity, they have been sorted by the rough stages outlined above. Of course, a real op might not follow the neat 5-step plan, but that's part of the fun! (We'll start with stage two so you don't have to read 20 pages of contract negotiation)

Stage Two Techniques

- **Public Resources** – Use 'em! This includes libraries, phonebooks, newspapers, company publications, newspapers, interviews, and leaked documents (especially from prior intrusions)
- **Take Notes** – Manufacturer, software name, software type, version number, date of installation, any operational statistics (memory, CPU, clock cycles)
- **The Web** – Check these BBSes, sites, and archives:
  - *Last Call BBS* (Grey-hat bulletin board, friendly chatter, technical advice)
  - *The Company Manhunt* (Business-centric newsfeed, up-to-date corporate news and press both good and bad, job postings, up to date stock market and public info)
  - *Pwn.Club* (Members-only black-hat BBS, contains just about every type of arse you can think of, help available for a price)
  - *<Gen.h>* (Chatroom and miscellaneous news/entertainment site with a tech focus, helpful for keeping up to date with the latest gizmos)

Try Exploit.DB

- **Asking Questions** – Here are some easy aliases to adopt when asking questions over the phone or web. These won't get you very far, but are plausibly true and rarely incite suspicion.
  - ~~Angry~~ customer

Confused

- Student/researcher in the field
- Low-level employee from another branch/subsidiary

Stage Three Techniques

- **Look for the Human** – A faulty card gate means that a security guard has to check IDs manually. A special assignment requires am inspector from H.Q. to oversee it. Important documents may be delivered by courier. If the Web service is down, someone has to man the hotline. Where there's a human there's a way in.
- **Look for Flaws** – Procedures, over time, devolve into rote patterns that can be exploited. Maybe the guards know a programmer and won't search their bag thoroughly because they're distracted. Maybe someone critical enjoys a late-night snack at the local fast-food diner, and carries confidential documents out of the building to work while they eat. Maybe if you leave a floppy disk outside the building someone curious will take it in for you.
- **Look for the Unusual** – Machines acting erratically usually indicates a way in. Does a system respond with what looks like gibberish or raw data when you feed it too much input, or nothing at all? Maybe that's a memory exploit. Try shortcuts or commands when programs error out or stall. Do devices rely on limited hardware to generate random numbers, resulting in patterns in what should be chaotic? Maybe you can exploit that to bypass encryption.

Stage Four Techniques

If you need to go where you shouldn't, these are the ways to do it.

- **Tailgating** – Just... follow someone in. Pretend you forgot your key card, loiter around, maybe even smile apologetically.
- **Shoulder Surfing** – Is someone logging on or talking over the phone in a public place? Listen in or look over their shoulder.
- **Get Legit** – I know, I know. But there are many ways to slip out of a tour group, especially a large one. Maybe even get a low-level job. Getting in the door is the first step to victory.
- **Know People** – People are the weak link in any security scheme. People leak passwords by accident, open doors, reveal personal details that match their password.
- **Claim Authority** – Maybe you represent an agency or a branch office executive, and you need to do a surprise inspection. Something that's plausibly deniable, but can get you the access you need and gets you out before they cotton on.

Act like you're in a hurry...

Stage Five Techniques

Once you're in...

- **Make Friends** – Friends do favours. Friends do things the handbook says not to. Friends let you stay alone to finish "just a little bit of work" or sneak back in to "grab my pager".
- **Keep Looking** – Passwords are everywhere: written in journals, in unencrypted text documents, in manuals, on post-it notes, and in internal memos.
- **Ask for Help** – Once you're in (legitimately), you're within the circle of trust. Anything you could plausibly invent to exploit that should be used. Internal help lines might be a good place to start.
- **Cover Your Tracks** – Stay out of record books, visitor records, and computer logs.

Take what you can, don't leave open drawers or unlocked doors lying around. Watch out for cameras, alarms, and security.

- **Delay, Delay, Delay** - If it seems like you're about to get caught, play for time. Ask for a supervisor or manager. Call your "boss". Fish for paperwork. Anything to engineer a chance to slip away.

Sage Advice

Finally, here's a few words from someone who's done quite a lot of it, if not it all.

- **Stay calm** - When you're scared, you make mistakes. When you're scared, you get messy. When you're scared, suspicion becomes certainty.
- **Study your target** - Strike when it suits you, not when you feel the urge. Missing an opportunity may sometimes allow another, better one to emerge.
- **Have fun** - After all, it's not like you're going to go to jail if you get caught! (If you have a contract, that is)

Some more fun tips -

— Did you know tapes fit in boots?

— Everyone ignores maintenance contractors...

— When a problem seems too big, break it down