CSCI 3403: Project 3

Ethical Hacking Fundamentals

Due: 4/20/2020 at 11:59 PM

Background

At this point in the semester, we already have a grasp of HTML, CSS, Javascript, PHP, Linux, and very minimal Flask. In addition to this, you may need to refresh yourself on some material from Computer Systems. If you do not have this, this project will be difficult to complete, and you are strongly encouraged to learn those things before beginning this project. In this project we are going to be taking a look at some basic exploits, and get experience breaking into things. Please note: *this is a long, difficult project. Please start this project early and work on it often*. Hacking always involves trying dozens and dozens of things that don't work until you finally find one that does.

Goal

The goal of this project is to understand some contemporary challenges in ethical hacking. So far the content in this course has been very theoretical, so this will be a chance to take some of your knowledge and apply it. Please note that for many of these challenges, you will be able to find the solutions online. **If you submit something and you don't understand how it works, you will be given a 0 for the project and reported for an honor code violation**. We can and will call you in and have you explain your exploits to us if something seems off. Moreover, it is not to your advantage to look up the solutions. In fact, you will find some challenges where the solutions are not online, and the previous challenges are meant to prepare you for those.

As mentioned above, hacking is a process of repeatedly trying many things that don't work. You will get the most out of this lab if you spend a lot of time banging your head against the keyboard, trying every possible trick you can think of until you can get something to work. The more you do this, the more you will benefit. Once you've made an honest effort, you are welcome to use online resources where they exist. However, you should go back later and re-attempt the challenge if you were unable to complete it the first time.

Instructions

Create a report detailing all your work. For each challenge listed below, provide:

1) Things you tried that didn't work
2) Amount of time spent trying to solve the challenge
3) How you arrived at your solution
4) An explanation of why the solution breaks into the system

5) A screenshot or evidence that you did, in fact break it (may not be necessary for every challenge. See details for each challenge)

You don't have to be extremely detailed, but it should be enough to convince the reader that you know what you're talking about. For example, if you complete a SQL injection, a good explanation might be, "First we entered a single quotation in the box to see if I'd get an error. Then once that returned an error, we entered some of the other commands from the SQL injection cheat sheet to see if anything worked. When that threw an error, but not the result we wanted, we looked at the shown underlying SQL query and crafted the following statement that worked: "asdf' UNION SELECT * from credit_cards; -- ". This statement provides input, then combines what the query should return with what we want it to return, showing all the data to the user, and comments out the rest of the query. This took about 1.5 hours to figure out with Abhinav and Matt working on it." A poor response would be the following: "I tried the SQL tricks from recitation, but that didn't work, so I changed it and that gave me the credit card number. It took about three hours."

As a couple of side notes. Evidently, sometimes anti-virus will block some of the website challenges. If this is the case for you, you may need to disable your antivirus or run the challenges in a virtual machine in order to access these. Also, on Overthewire challenges, sometimes if you double-click to copy and paste the passcode, it will copy a trailing whitespace, causing you to not be able to complete the challenge. Finally, for each section there is a tentative, highly subjective rating of the difficulty of each challenge. Please note that this is completely relative, and you may find some challenges easier or more difficult depending on your experience, background, and luck. This rating is from 1 to 10, 1 being trivial and 10 being a little too difficult for this class.

Very Basic Linux Exploits (20 points)

Difficulty: 2

Go to https://overthewire.org/wargames/bandit/ and complete the first 25 levels (get the passcode for bandit26). Okay, most of these levels are extremely basic and designed for people who have never used Linux before. Therefore you may find them to be a little condescending in what they expect you to know. But you should breeze through them! And, if you get a little too confident, feel free to hop over to one of the other harder challenges on the page when you're done! To submit your work for this challenge, please provide all of the passcodes for each stage, as well as a screenshot while you're breaking the final challenge.

Hint: These are intended to be simpler exploits, and really just trying to get you into an adversarial way of thinking. They'll also give you a refresher on Linux if it's been a while since you've used it. Make sure you get these down well!

General Web Exploits (30 points)

Difficulty: 5
Go to https://overthewire.org/wargames/natas/ and complete the first ten levels (i.e. get the passcode for natas11). This will challenge you to be thinking about basic ways that some web sites can be exploited, as well as with some of the many tools you have at your disposal. Submit this in the same way as the previous challenges, keeping track as you go and submitting all passcodes.

Hint: These ones are a little bit more involved than the previous ones, but you should solve them with a bit of effort. Everything you need to solve them was discussed in week 9 and 10 lectures, so if you're stumped, try taking a look at some of those tools and tactics! And don't forget about *robots.txt*.

PortSwigger Specific Attacks (10 points)

Difficulty: 4
Now go to https://portswigger.net/web-security and register for an account. Go through and complete any 5 of the SQL Injection labs, as well as any 5 XSS attacks and any two CSRF attacks. They are very generous with their solutions, in that it's extremely easy to click on all of them and complete them right away. Resist this urge, and try it for a while before giving in. However, even more importantly, they offer a wealth of good information about each of these attacks, so please read that as you're going about each section to try and gain a deeper understanding. In your report, please make sure you specify which ones you completed. There's no need to provide a solution, since they're all on the respective page.

Hint: There are solutions for each of the challenges, but **don't look at them immediately!** If you do not review the content carefully and struggle through each of the challenges, you will not learn what you need to in order to complete the next challenge. Also, PortSwigger is the company that creates BurpSuite, so of course their solutions will tend to want you to use their product. You should set up a session and install an SSL cert - see links to do this on Piazza. Also, don't forget about URL encodings!

A Real Challenge (40 points)

Difficulty: 7
Many companies have hacking challenges where, if you break them, then you get fast-tracked to a job at their company. Now… go get a job! Because of the nature of these challenges, the solutions are not likely to be online. Also, if you work on some company's challenge as a group, do not take that submission and apply for a job with it. That is dishonest, and a violation of our goal of ethical behavior in this class. However, if you all complete the challenge individually, simply note that on your report, and then go claim your job! You are all welcome to each

perform this challenge individually. Also note that some of these challenges may be a small step up from what we're used to in this course, which is why they're worth so much credit. However, if you've understood everything, it should be well within reason to complete.

So, this challenge is a little different. The challenges are for the company Assured Information Security (AIS), at https://hack.ainfosec.com/. The course staff is in no way affiliated with this company. Go here and complete all 3 Input Validation challenges, as well as the first Exploitation challenge (for 75 points). To receive credit, submit all of the regular explanations for each challenge, as well as your ID for the challenge. It will look something like Your ID: 26ab8eb9-238c-aa8b-8319-c8cb21394a5e.

Hint: Because these are used by actual companies to recruit top talent, we can't provide much help in office hours. In fact, if you find you're completely stumped, you should go back to the previous challenges and work through those. However, if you really put your mind to the previous challenges, then this one should be very manageable! Just pay close attention to the descriptions of what they want you to do.

Extra Credit: Go Further! (10 points)

Difficulty: ???
Go back to the challenges that we asked about before and go do additional levels! You will receive 1 point for each additional level/challenge broken. Note: You may not submit challenges here after looking at the solutions. You must complete them blindly, on the honor system.

Extra Credit: Get a Job (40 points)

Difficulty: 9
Take the AIS challenge, or some other comparable challenge, and complete it! For full credit, you must show that you completed a challenge by a company sufficiently to get a job. You're already on a good start after the "A Real Challenge" section, so feel free to use your progress there. You will receive 40 points if you complete a challenge to the company's satisfaction. However, on the AIS site, you'll need to complete 670 points to receive all 40 extra credit points, since 300 came from the regular homework. From there it's a linear scale, so you'll receive (***x***-300)/(670-300)*(40) points. For example, if you earn 450 points, you'll receive (**450**-300)/(670-300)*(40) = 18.75 extra credit points.

Once again, all team members are welcome to complete this individually, then apply for the job. However, if you complete it as a team, then you shouldn't apply for the position using that code. Please don't ruin the experience for the company, your classmates, and future students, as well as your own reputation and credibility. To submit your work for this one for AIS, please use the same ID as the last challenge. If you use a different site, submit their token or whatever they use. You may also need to document

Hint: Good luck.

Submission

Upload a new document with your answers. At one point in the document it should contain the following:

1. Your team members’ names and emails.
2. A description of what each team member contributed. One person in the group should turn in a single document to Moodle, but each member should contribute, though naturally, you will contribute to different things.
3. Your descriptions and proofs of challenge completions, as specified in each section.