

## CS 444/544 Spring 2017 Lab 3 and opportunities for extra credit

Lab 3 is due by 11:59pm on Friday, 5 May 2017.

Lab 3 is relatively informal and your grade is based only upon participation and effort, because I don't want to "cramp your style" in terms of learning cool things together and anything involving servers and networking and deadlines is likely to have serious snags. Only 9 people will email me anything for Lab 3 that is graded: specifically, one representative from each group should email me the list of people who participated enough in that group throughout the assignment that they deserve to get 100 points instead of 0. If your name appears on the list for the group you were assigned to, you get a 100. Switching groups is not permitted. Hopefully there will be no surprises, because if someone is not participating in any group I want to know in the beginning, not in the end, about it. So hopefully one group member emailing me the list of all the group members for the group who participated (which I hope is the whole list of people assigned to the group) is a perfunctory thing, but if someone really didn't participate then don't include their name. Send a single email per group with just a list of names in the body of the email (no attachments) to [crandall@cs.unm.edu](mailto:crandall@cs.unm.edu). If you'd like to send me attachments (like your exploit code, a writeup if you choose to do it individually or as a group, or whatever) send it as a separate email.

Here is the basic calendar for Lab 3 for your reference:

April 12<sup>th</sup> and 19<sup>th</sup>: you will meet up with your groupmates in class (come to the classroom first and then you can branch out to other areas of campus to meet).

April 24<sup>th</sup>: Groups 0, 1, and 2 will present and moderate Werewolves games

April 26<sup>th</sup>: Groups 3, 4, and 5 will present and moderate Werewolves games

May 1<sup>st</sup>: Groups 6, 7, and 8 will present and moderate Werewolves games

May 3<sup>rd</sup>: Final presentations

The groups were randomly assigned, I only did a minimal amount of moving people around to balance out the groups after removing people that haven't been doing enough labs, midterms, *etc.* to convince me that they're still planning on being in the class.

Lab 3 is relatively informal, but the usual restrictions about plagiarism or mis-representing someone else's work as your own apply. You also may not violate University policies, civil or criminal laws, ethical norms, B146 room rules, *etc.* Additionally, a restriction for Lab 3 is that you may not commit denial of service in any sense. This means no denial of service attacks on networks or systems, no holding games hostage or interrupting games (*e.g.*, gaining moderator privileges and then killing the server or locking groups out from playing), no annoying behavior like sending someone else system messages that mess up their terminal, and pretty much just nothing that prevents anyone from playing Werewolves at any time. It also means that if you find a foolproof way to know who the Werewolves are or otherwise win games easily, you should use it in moderation and not dominate every game just because you can. At all times your overarching goal, beyond winning, is for you and your classmates to learn as much as possible. You guys are hopefully a bit more mature than the high school students that I've had play Werewolves in B146 in the past, but just so you know things like unplugging machines, harassment (verbal or within the chat feature of the game), and so on won't be tolerated.

**Other than the above restrictions and requests, if you're not cheating you're not trying for Lab 3!**

You should be having fun and you should be expanding everyone's knowledge (including mine) by being creative in your ways of gaining advantages at Werewolves games.

Your mission as a group is to teach the rest of the class at least one concept by giving a short presentation (5 minutes) about it and then moderating some Werewolves games where students will apply what you told them. Every group has been given one concept that they should convey at a minimum. Doing just this one concept is perfectly fine as long as you do it well, but you're also welcome to have additional servers running so you can convey other concepts of your choosing.

In terms of server logistics, we have 60 VMs that the TA is the sysadmin for. The TA's email address is [nvaquera@unm.edu](mailto:nvaquera@unm.edu) and her name is Nidia. Your group needs to work with her (and please realize that she's supporting 9 groups, so get in touch with her early and be respectful of the fact that she also has other classes and such) to get access to however many VMs you need (between one and ten, it depends on what your group is trying to do). You're responsible for setting up Werewolves, making sure other students have a way to SSH into your server(s) to play Werewolves, and all other sysadmin aspects of your project, but the TA and I are here to help with that, too.

On the two days that you have to prepare (I hope you'll meet---at least virtually---outside of the usual class time as well, two one-hour-ish sessions is not enough time to prepare), which are April 12<sup>th</sup> and 19<sup>th</sup>, you should come to class in the usual place at the usual time, **then** we'll break up into groups and you can disappear to different parts of campus to meet for as long as you need to. This is to keep logistics simple, so that there are at least two meeting times where everyone in the group had already been planning on being in the same place at the same time anyway. I recommend running at least two or three Werewolves games as a group for debugging and so that everyone is ready and understands how the game works and how to moderate games and participate in them *via* the command line.

On the three days where three different groups each day are moderating Werewolves games, everyone will still come to class in the regular place at the regularly scheduled time. We'll have three 5-minute presentations, one from each group for that day, and then spend 1 hour playing Werewolves. Make sure I have your slides for the presentation (other presentation techniques are okay, too, but if you want to project slides I'll need them) in PDF format 24 hours before your group's presentation, and make sure your presentation is well polished because I will be bringing my Cap'n Crunch whistle and I will cut you off at exactly 5 minutes. I recommend nominating one group member to give the entire presentation to keep it simple, but it's completely up to you how you want to do it. The point of the presentation is to tell the class about your concept and how they're going to exploit it on your Werewolves server or servers (and other logistics, like how they're going to get into your Werewolves server or servers). If you're the second group to present a concept, try to add something new but even if you simply reinforce what the previous group already taught the class that's okay.

I recommend between eight and twelve players for any Werewolves game at a time. An easy way to do this is to give all eight groups that are not your group a group account to play a game on a single server (or one account per server), and leave it up to the groups how to divide who is playing what on which servers when. All three groups will be running games concurrently for the whole hour. Having a backup server is not a bad idea, especially if part of your concept involves others getting elevated privileges on your server. Logistically speaking, we're trying to pull off something complicated with very little time to prepare, so don't stress if things go fubar. Just make the most of it, your grade is based on effort and depends on you doing the best you can to make sure your group teaches the class something interesting, if your server goes fubar that won't affect your grade. Things go fubar a lot with Werewolves.

Then, on May 3<sup>rd</sup>, all nine groups will give a 5-minute presentation each. You should say what you did

and what you learned, both for the games you moderated and for the games you participated in as players. If you had an interesting strategy to cheat, this is your time to reveal it. If you have some closing comments about the concept you were trying to convey in the game or games you moderated, this is your chance to sum things up at the end. If you want to project slides I need them 24 hours beforehand, and, again, I will bring my Cap'n Crunch whistle and cut you off at 5 minutes sharp.

Other concepts you might consider conveying with additional Werewolves games: password management and password cracking, buffer overflows, social engineering, side channel leaks in the Linux system (*e.g.*, in `/proc`), or whatever piques your interest.

If any of the above requirements for the lab are in the way of doing what you want to do, just let me know and we can discuss it. Everything is flexible, the only thing that is paramount is teaching your classmates something really cool and working as a group to do so.

In terms of group work, you should keep two things in mind at all times. One is that you have unique perspectives and great ideas, and you have a responsibility to share those with the group. Don't sit silently, be an active participant throughout. The other is that others in the group have unique perspectives and great ideas, so don't let anyone sit silently and don't be dismissive of anybody's ideas until you fully understand them. Be a leader, instead.

**Opportunity for extra credit as an individual (not part of Lab 3):** Not necessarily related to Lab 3, you have the opportunity to get up to 50 points extra credit (added to your lab grade, so a half a lab's worth of extra credit) as an individual effort (*i.e.*, not as a group). If your grade goes *significantly* above 100%, I may give you an A+ in the class. Or, if you missed a lab or didn't do well on one this can help make up part of that to improve your grade. Anyhow, you have to do two things to get extra credit:

1. Before 11:59pm on Friday, April 14<sup>th</sup> email me your intent to do something for extra credit and propose what that's going to be. I'll give you feedback about what you would need to do for it to count, how many points of extra credit I think it would be worth, and just general feedback.
2. Before 11:59pm on May, 5<sup>th</sup> send me a tar ball with everything you want graded as extra credit. I have final say on if something even counts as extra credit and how many points it's worth.

Your extra credit should be something I can use for next year's 444/544 class. You'll turn in a single tar ball, which might include source code, PDFs (but something I can edit like LaTeX or LibreOffice documents is preferred), a video, a flash animation, *etc.* Examples include:

- Implement a client and server for something like Lab 2, but based on RSA malleability and a padding oracle for RSA rather than CBC padding oracles. This would be worth 50 points, probably.
- Write documentation for Werewolves (how to install it, how to play, *etc.*) This would be worth maybe 25 points.
- Find a new vulnerability in Werewolves and develop an exploit in it. Probably worth 50 points.
- Make up a whole new lab of your own, perhaps based on IDS evasion *via* IP fragments or password cracking, for example. This would probably be worth 50 points.
- Create a cool visualization (*e.g.*, an image or video) of something. For example, you could make a video of Lab 2 that shows different bytes being tried until one locks in, just like the

cheesy “hacker” scenes in Hollywood where they crack a code one digit at a time but with a real CBC padding oracle attack underneath what you're seeing. This would definitely be worth 50 points and an A+.