How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	I used John The Ripper and ran through the shadow and passwd with the main password list provided by JTR.	
2	baseball:jampam35 gibson:amanda guesses:sss	First I exected the unshadow script which merge the etc/passwd and etc/shadow files in to single file called 'passfile.txt'.Then I used the following commands to crack passwords from passfile.txt file. ./john -wordlist:password.list passfile.txt ./john -single passfile.txt ./john -incremental:lanman passfile.txt ./john --show	
4	tonymonaco:jumbos jampam35:baseball amanda:gibson provost:Barnum	Below are the commands i used to crack the above passwords: ./john unshadow /etc/passwd /etc/shadow > passfile.txt // combined passed and shadow files and redirected output to passfile.txt ./john --single passfile.txt ./john --wordlist=password.lst --rules passfile.txt ./john --wordlist=all.lst --rules passfile.txt ./john --increment:lanman passfile.txt	
7	tonymonaco:jumbos:1001:1001:,,,:/home/tonymonaco:/bin/bash cisco:sanfran:1002:1002:,,,:/home/cisco:/bin/bash jampam35:baseball:1003:1003:,,,:/home/jampam35:/bin/bash amanda:gibson:1008:1008:,,,:/home/amanda:/bin/bash homer:lobster8:1009:1009:,,,:/home/homer:/bin/bash provost:Barnum:1010:1010:,,,:/home/provost:/bin/bash paris:t1nkerbell:1011:1011:,,,:/home/paris:/bin/bash	0. ./unshadow passwd shadow > unshadowed 1. Ran ./john on unshadowed with no wordlists; found 3 passwords and aborted when it was taking too long 2. Wrote a Python script to run ./john on unshadowed using wordlists that come with Metasploit and against those found on the internet (http://www.outpost9.com/files/WordLists.html, http://wiki.skullsecurity.org/Passwords, and http://apasscracker.com/dictionaries/); ran both with and without the --mangle tag; found 4 more passwords and aborted before completion	
6	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 paris:t1nkerbell	I just ran John The Ripper with a long password list I grabbed from the Internet. The list was concatenated with the original list that came with the software.	
3	tonymonaco:jumbos jampam35:baseball amanda:gibson	1. Unshadowed the passwd and shadow files to generate mypasswd 2. Ran ./john mypasswd . Also tried human-only wordlist from crackstation, but gave up after 7 hours.	
4	cisco:sanfran jampam35:baseball amanda:gibson paris:t1nkerbell	Used default and rockyou wordlists in John the Ripper.	
5	provost:Barnum tonymonoco:jumbos cisco:sanfran jampam345:baseball amanda:gibson	First, I used the "john the ripper" default password list and I got three passwords through that method within 20 minutes. I then looked at the user names and created by own wordlists to see if anything matched up. Luckily, in my tufts wordlist, (which had names of past provosts, locations on campus, and random tufts words that came to mind), Barnum showed up as a password. Lastly, I used the Cain and Abel wordlist to try cracking the rest. I was only able to get sanfran after a very long time. The cracker is still running whenever my laptop is on so it is possible I will be getting more than 5, but unlikely. I tried some other wordlists that did not succeed (i.e. a wordlist of cartoon characters, movie actors, etc). I have not tried brute force as this would take a VERY long time and I figure I will have better luck with wordlists	

How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
6	amanda:gibson tonymanoco:jumbos jampam35:baseball cisco:sanfran provost:Barnum ---------- ---NEW ONE---- ---------- defcon:!templinuxpw!	see my previous submission. For the 6th password, I realized that defcon is the username given for the VM and thought that the VM password might be the same as the hashes given... and it was	
4	jampam35:baseball amanda:gibson tonymonaco:jumbos provost:Barnum	1. Used John the Ripper single crack mode 2. Used John the Ripper with a default wordlist (password.lst) 3. Compiled a word list of words and phrases related to Tufts and used John the Ripper with the list of: - academic buildings - residential halls - fraternities and sororities - traditions - common studies - foreign languages offerred - nearby roads - popular student organizations	
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	Downloaded john the ripper, called './unshadow passwd shadow > mypasswd' then called ./john mypasswd and let it run while it cracked the passwords.	
5	jampam35: baseball amanda: gibson tonymonaco: jumbos provost: Barnum cisco: sanfran	On my first attempt I ran john with a wordlist suggested by the john documentation (one larger than the default). This gave me the 5 cracked passwords that I have listed above. I also tried running john in incremental mode, where only combinations of digits are tried, after a while I stopped running this because it seemed it would take a really long time and it did not seem as if I was going to get anywhere. I noticed that the passwords I retrieved are all around the same length, between 6 and 8 characters, so this may help me in cracking more passwords. I'm currently writing custom rules for john and will resubmit if I have any luck cracking more passwords.	
3	tonymonaco:jumbos jampam35:baseball amanda:gibson	I ran plain ol' john the ripper against the unshadowed passwd + shadow file. My machine is really slow so to just do that it took about five hours. I also downloaded a 4 GB password list from online and ran john against it but as of the last check, it was .45 % through and hadn't returned conclusive results. If I find more, I'll resubmit.	
7	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 provost:Barnum paris:t1nkerbell	I used john the ripper on my laptop with the -fork=2 option for it to use both cores of my CPU as well as the -rules option to use wordlist rules. I ran it on the word list rockyou.txt which is the biggest password leak in recent history. I also ran it on /usr/share/dict/american-english file that came with my install of Debian.	
3	tonymonaco:jumbos jampam35:baseball amanda:gibson	- Unshadow the passwd file - Download word list from openwall.com - Run ./john on the unshadowed passwd file	
10	tonymonaco:jumbos cisco:sanfran jampam35:baseball tarin:daisies123 lrrr:Barney123 sgerrard:L!verpool amanda:gibson homer:lobster8 provost:Barnum paris:t1nkerbell nr: defcon:	Hi Ming, It's Chris Smith. I miss this class, so I took this lab. Can't wait for CTF! Also I'm sorry I missed you at OWASP. I get too many emails from them and I ignored the meeting notice.... Anyway, let me know what's up if you've got anymore talks coming up. My email is Christopher. Smith116@gmail.com Methodology: cudacat and 200 GB of dictionary passwords! (too bad SHA-512 takes so long, but 2 graphics cards gets several thousand guesses per second pretty easy.	

How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
5	defcon:!templinuxpw! tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson	- Ran John the Ripper using the included wordlist: cracked 2 - Re-ran using word mangling: cracked 1 - Used the wordlists in the metasploit framework: cracked 1 - Saw defcon was a user and tried the password given earlier in the semester: cracked 1	
5	tonymonaco:jumbos:1001:1001:,,,:/home/tonymonaco:/bin/bash cisco:sanfran:1002:1002:,,,:/home/cisco:/bin/bash jampam35:baseball:1003:1003:,,,:/home/jampam35:/bin/bash amanda:gibson:1008:1008:,,,:/home/amanda:/bin/bash provost:Barnum:1010:1010:,,,:/home/provost:/bin/bash	I got a wordlist (all.lst) from john the ripper and ran it. It ran for a little less than 2 days.	
2	jampam35:baseball amanda:gibson	I compiled "John the Ripper" from source and ran "unshadow" on the files you gave as. Then I ran John with "password.lst," which comes with the source code. The bundled password.lst yielded two combinations. I downloaded another list from Github and some others from this site: http://www.outpost9.com/files/wordlists.html None of the shorter lists yielded new passwords, and the longer ones cause my machine to shutdown on overheat protection. (This is a general problem I have with computationally intensive tasks.) It made it about 13% through an unabridged dictionary. With more time, I would create a Tufts specific list of passwords containing permutations of "Jumbo" and "Tufts."	
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	ran john the ripper with the unshadowed shadow file command: ./john shadow	
6	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 provost:Barnum	I used John the Ripper to crack all of the password. I initially started with JTR's default cracking mode order and let it run for a long time. This cracked 4 passwords. Then I tried other wordlists, such as commonly used passwords, with the default mangling rules applied. This cracked two more passwords.	
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	Downloaded John the ripper, unshadowed the shadow file using the password file and run the cracker.	
4	6.gPOCM. P$Wo6vjQ2foZCrlaDNKWGnHb9C5LmbC9h2hmQ/0/Ca 6hlQACyTH$8w0Lgwm8RIdPxHbCJzOlEv2GZMmx. XfXBI. rYsPoA9xd4xayKK7NUuVMq9tlbRwuSlpFlEsQp6puK0D 6prmyJqT0$NZMo8396xc4VZTe. DtnehfmXhuBKEF9cOa. uGbx8UIHMxolGioaDRRNqJwNOvQKk9/d4JVovnwaYaf 6ziATV. k2$HPbaiMpdRAbWYrnaGp1oNTlnPe9qs1hB8.q. nQyhxsyT2hlHpC9PKpDfFlWNklsiJnLm1y3N7iyZY4Elx1	So far I have run John the Ripper with the RockYou password list on the unshadowed hashes that were provided.	Uh...
6	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 paris:tinkerbell	Use unshadow from john to combine shadow and passwd information. Use john with a wordlist to perform dictionary attacks to solve the hash for the password.	

How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
6	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 paris:t1nkerbell	Use different wordlist (Rockyou.txt etc) to crack the password: john --wordlist=pwdlist.txt crack.txt Use incremental brute force john -i crack.txt	
4	cisco:sanfran jampam35:baseball amanda:gibson paris:tinkerbell	I used John the Ripper with both it's supplied wordlist and one I found online. I used the command ./john -w="wordlist here" -ru	
4	tonymonaco:jumbos jampam35:baseball amanda:gibson provost:Barnum	I used John the Ripper and a combination of the password.lst wordlist that comes bundled by default and the all.lst wordlist I found on the Openwall site. With the first wordlist, I found two passwords very quickly; with the second, I found another two very SLOWLY. For all.lst, I tried both the default ./john <password list> (with all.lst as the default wordlist in my config) and ./john --wordlist=all.lst <password list>. Both ran VERY slowly, and I ended up sticking with one mode --wordlist - and just letting it run in the background. After running for over 13 hours, it had gone through less than 40% of the wordlist and was cracking the passwords very infrequently. Given more time (or more processes), I would have experimented with fewer word mangling rules and wordlists that were longer than password.lst but shorter than all.lst!	
7	tonymonaco:jumbos:1001:1001:,,,:/home/tonymonaco:/bin/bash cisco:sanfran:1002:1002:,,,:/home/cisco:/bin/bash jampam35:baseball:1003:1003:,,,:/home/jampam35:/bin/bash amanda:gibson:1008:1008:,,,:/home/amanda:/bin/bash homer:lobster8:1009:1009:,,,:/home/homer:/bin/bash provost:Barnum:1010:1010:,,,:/home/provost:/bin/bash paris:t1nkerbell:1011:1011:,,,:/home/paris:/bin/bash 7 password hashes cracked, 5 left	Basically, I ran John the Ripper in a variety of modes (single, wordlist, rules, and unspecified/everything) with a few different wordlists: the password.lst supplied, all.lst from Openwall, and the rockyou wordlist. I did not complete most of the sessions, especially those with the rockyou wordlist, due to time constraints; e.g., rules mode with rockyou had completed 0% of the total after running for about 24 hours. I also tried Hashcat for a bit but it sounded even more like my computer was about to explode so I cut it short pretty quickly!	
3	tonymonaco:jumbos:1001:1001:,,,:/home/tonymonaco:/bin/bash jampam35:baseball:1003:1003:,,,:/home/jampam35:/bin/bash amanda:gibson:1008:1008:,,,:/home/amanda:/bin/bash	Downloaded a dictionary wordlist from hashcat, downloaded john the ripper, ran locally against wordlists and retrieved three passwords. Attempted to crack the SALTED passwords but made such minimal progress (<1% after a day) that I realized I wouldn't have enough time. Interested in running against a larger wordlist; like wikipedia for unsalted passwords.	
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	Download and install John the Ripper (V 1.7.9). Download both passwd and shadow. Run ./unshadow passwd shadow > ushadow Then run ./john ushadow Watch the magic happen	
5	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson provost:Barnum	I used john the ripper with a large wordlist downloaded from the Internet. I turned on mangling rules as well, but as of yet it doesn't look like any mangled passwords were found. I plan on updating my pot if more passwords are cracked before the due date next week. I am running john on an 8 core machine, with 7 john processes forked using the --fork option. The 7 processes each have an effective password rate of around 18 p/s, so my overall rate is 126 p/s. So at a rate of (assuming all passwords 8 chars long): 126*(4*8)*3600 / 1024 / 1024 = 14 MB/hr It will take around 36 hours to go through the 500 MB wordlist I have (without mangling). With mangling it will take forever.	

How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
6	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 provost:Barnum	Found one more (homer:lobster8).	
7	defcon:!templinuxpw! tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 provost:Barnum	For defcon I guessed the default password used for the provided ubuntu vm. The other 6 passwords were cracked using john the ripper with mangling enabled.	
5	jampam35:baseball tonymonaco:jumbos provost:Barnum cisco:sanfran amanda:gibson	Two sessions of John the Ripper- one with no wordlist, one with the Openwall wordlist (all.lst).	
5	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson provost:Barnum	I used John the Ripper to crack the password, and I used the included wordlist. I also used the wordlists included with the metasploit framework, and I tried to create my own Tufts related wordlist (social engineering).	
7	defcon:!templinuxpw! tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 provost:Barnum	John the ripper on wormhole. defcon you literally gave to us. The others I found with wordlists on the internet. I discovered John's forking ability with ps aux | grep john.	
8	amanda:gibson jampam35:basebal tonymonaco:jumbos homer:lobster8 cisco:sanfran paris:t1nkerbell lrrr:Barney123 provost:Barnum	I ran john on wormhole for about 5 days using 32 of the 64 cores. After I exhausted the first default password wordlist, I went to the largest password dictionary I know of: rockyou. It's about 130mb of passwords. My process was killed after several days. mjames03@wormhole$ ./john --wordlist=/tmp/rockyou.txt --fork=32 --rules ~/116-security/lab2/shadow	
7	defcon:!templinuxpw! provost:Barnum tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8	I mainly used John the Ripper with the default password list and various other password lists I found on the internet, along with the "-i" option to try and brute force some passwords.	
4	amanda:gibson jampam35:baseball provost:Barnum tonymonaco:jumbos	John with wordlists...pretty vanilla.	

How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
10	paris:tinkerbell jampam35:baseball amanda:gibson homer:lobster8 tarin:daisies123 cisco:sanfran lrrr:Barney123 tonymonaco:jumbos provost:Barnum nr:F00tball!	I used cudaHashcat-plus64 with the rockyou wordlist and the best64 rules list. This took advantage of my graphics card to crack the passwords in just under 11 hours.	
7	tonymonaco:jumbos cisco:sanfran jampam35:baseball lrrr:Barney123 amanda:gibson homer:lobster8 provost:Barnum	I got some wordlists and ran 3 simultaneous john sessions for a few days on a 4 core desktop.	
3	jampam35: baseball amanda: gibson tonymonaco: jumbos	Using John the Ripper: john --format=sha512crypt shadow John was able to find 3 passwords in around 10 minutes time, probably could have found the other 9 passwords given more time.	
5	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson provost:Barnum	I first used john the ripper in fast crack mode. This got the first three passwords very quickly. Then, I downloaded the Cain and Abel wordlist and began to do a dictionary attack with it. It would have taken two weeks to get through the whole dictionary, but it gave me two more passwords in the time that it was able to run.	
3	tonymonaco:jumbos jampam35:baseball amanda:gibson	I have been running John the Ripper on the files you gave us with for 2 days and 1 hour now and it still hasn't finished. Unfortunately I have only been able to uncover three passwords and they all came within the first 20 minutes or so :(	
9	jampam35:baseball amanda:gibson tonymonaco:jumbos provost:Barnum cisco:sanfran lrrr:Barney123 homer:lobster8 paris:t1kerbell tarin:daisies123	First ran the RockYou password list against the hashes with john, Cracked 8. Started john ascii rules attack, no successes after 7 days. Used CUDA-accelerated hashcat rules attack on /usr/share/dict/words, which cracked daisies123. Started running rules attack using RockYou, but ran out of free EC2 hours.	
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	I used Jack The Ripper with the default word list and rules list.	
7	defcon:!templinuxpw! tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 provost:Barnum	Ran --single, which cracked at least 2 passwords, then --wordlist with the wordlists provided with john the riper that was 3 more passwords, then realized we already know the password for defcon and lastly ran another wordlist with the "10000 most common passwords". tried the --rules switch and that yielded at least one extra password.Sadly couldnt figure out lrrr. norman ramsey and paris (hilton?) and the others... created my own wordlists with keywords related to futurama, paris hilton's leaked tmobile password, french words, etc. but to no avail.	
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	Simply ran $> john shadow without unshadowing.	
0	ehhhh	I DLed John the Ripper, made unshadow, unshadowed the file, and ran john --wordlist=wordlist crackme after piping unshadow into the file crackme. Wordlist was pulled from openwall. Unfortunately, my community build of john failed repeatedly because of missing openssl. I ran brew install, but could not get it to find openssl. So I have nothing. Sorry ming. Did my best here, had me beating my head on the desk	Bah!
3	jampam35:baseball amanda:gibson tonymonaco:jumbos	Run john on halligan servers to take advantage of increases processing power.	

How many passwords did you crack?	Put your pot of passwords here	Briefly describe your methodology	My Comments
7	jampam35:baseball amanda:gibson tonymonaco:jumbos cisco:sanfran homer:lobster8 defcon:!templinuxpw! provost:Barnum	I used Jack the Ripper with wordlists (using --rules option to mangle the word in the wordlist) to attempt to find the passwords. I used multiple lists to find all the passwords. The list that found the most passwords was a compilation of the top 10,000 used passwords. I also used Jack the Ripper in brute force mode, but the passwords I found using brute force, I had previously found using the wordlists.	
8	jampam35:baseball amanda:gibson tonymonaco:jumbos cisco:sanfran homer:lobster8 paris:t1nkerbell lrrr:Barney123 provost:Barnum	I used John the Ripper with a wordlist I found online. I got an Amazon EC2 high GPU instance (still using EC2 credit from last year's hackathon). I split the password file in half and ran half on a CUDA build of john on the machine's 2 massive NVIDIA GPUs, and ran the other half on a standard build of john with the machine's 16 2.93Ghz Xeon CPUs.	
6	tonymonaco:jumbos cisco:sanfran jampam35:baseball amanda:gibson homer:lobster8 paris:t1nkerbell	I downloaded the rockyou password leak word list and ran it with John the Ripper. Its only about 4% done, so I probably could get more...may resubmit after I get back if its not too late!	