Final

• Final: Wednesday May 1st, 4:30pm-6:30pm.
• Similar to midterm in type of question: looking for how you think, not how you memorized
• Open note, open book (NOT open phone. NOT open laptop/ipad/etc.)
• IF YOU HAVE A CONFLICT, we need to work it out ASAP. Conflicts/exceptions need to be sorted out and approved by campus.
• I *have* to upload grades 96 hours after the final. I cannot give exceptions.
Content

- Intrusions to BGP Security (all lectures since the midterm)
  - Intrusion (e.g. phases and purpose, general approaches in each phase)
  - DDoS (e.g. types, challenges, current solutions, prevalence)
  - DNS (e.g. attacks/poisoning, how does DNS poisoning help an attacker? Defenses? ARP poisoning)
  - BGP attacks and defenses

- Very similar in style to midterm:
  - Open-ended questions for the most part, some short-answer
  - Explain your reasoning (even if you’re not sure, partial credit is better than no credit)

- May reference homeworks and CTF
  - If you skip a homework, be sure you at least read what the assignment was about
  - If you were not active in a CTF task, be sure you understand the gist of what was asked for
Final 1: Question 1: Discuss why users may have a misconception and why it’s incorrect

- To make a password strong it is enough to not use owner’s personal data, but one can use personal data
- To make a password strong it is enough to add a special character at the end
- If the password is strong it is OK to reuse it verbatim
Final 1: Question 2: DNS Security

- Explain in detail how Kaminsky attack works for DNS hijacking. Then specify what would be an
- effective defense against this attack and where it would have to be deployed (e.g., at the auth server of
- the network whose name is being hijacked, at a resolver, at a client).
• Final 1: Question 3: DDoS

• I propose a DDoS defense that serves graphical puzzles (CAPTCHAs) to clients of a Web server, when that server is under attack. Once the client solves the puzzle, its IP is marked as legitimate for the next hour and its traffic gets preferential treatment and is always forwarded to the server. The rest of the traffic is rate-limited, to protect the server against floods. For each statement below state if it is true or false, and elaborate why.
  • (2.5 pts) This defense can accurately detect legitimate clients during attack (i.e., all legitimate clients will be labeled as legitimate)
  • (2.5 pts) This defense cannot be fooled by the attacker to let attack traffic through
  • (2.5 pts) This defense can effectively protect the server from high-volume traffic
  • (2.5 pts) Can this defense reveal to the world that a server is under attack? How?
• Final 1: Buffer Overflows

• Explain how buffer overflow works. You must specify what features in the code cause the vulnerability, how is the vulnerability exploited and how can we prevent buffer overflows.
Final 1: Question 5: Routing Security

- Explain how anycast (announcing the same prefix from many different places in the Internet) helps protect from BGP prefix hijacking. Does it also help with subprefix hijacking?
Final 1: Question 6: Privacy

• Explain what third party cookies are and how they are intrusive to user privacy
Final 2: Passwords

• Company CheapStuff wants to revise their password policy to use passphrases instead of passwords
a) (5 pts) Discuss why passphrases may be better than passwords
b) (5 pts) Is there any downside to using a passphrase? If so, what is it and what could CheapStuff do to address this downside.
Final 2: Routing

- The following questions relate to BGP hijacking
- (3 pts). An attacker can announce a prefix P that he does not own. What is an effective defense against such an attack and where should it be deployed?
- (3 pts) An attacker can announce a short AS path to P. Why is this attack more difficult to handle than direct hijacking (attacker announcing the prefix P)?
- (4 pts) An attacker can announce either P or a subprefix S of P. Let H1 be the set of all ASes who adopt the fake route when the attacker announces P and H2 be the set of all ASes who adopt the fake route when the attacker announces S. Which set is larger and why?
Final 2: DDoS

• I propose a DDoS defense that asks each client during attack to send much more traffic. Those clients that send more traffic are marked as legitimate for the next hour, their traffic gets preferential treatment, and is always forwarded to the server. The rest of the traffic is rate-limited, to protect the server against floods. For each statement below state if it is true or false, and elaborate why.

• (2.5 pts) This defense can accurately label the legitimate clients as legitimate during attack

• (2.5 pts) This defense cannot be fooled by the attacker in any way

• (2.5 pts) This defense can effectively protect the server from high-volume traffic

• (2.5 pts) Does this defense reveal to the public that the server is under attack? How?
Final 2: Intrusions

• List six phases of intrusions and explain briefly what is the attacker’s goal in that phase and which activities comprise the phase.
Final 2: DNS

• Explain how DNSSEC works to protect against DNS hijacking. Make sure to explain what the owner of the name does, and what resolvers do to implement DNSSEC. Also explain how these measures prevent DNS hijacking.
Final 2: Privacy

- A user wants to use Tor to send data from its node C to server S over three routers X, Y and Z
  
  a) (6 pts) Explain how the packet is formed to travel from C to S
  
  b) (4 pts) Which source and destination does each of the X, Y and Z routers observe?