

CSE 498U – Homework 4

Due: Friday, November 19th, 5 PM

To be done in groups of 1-4 students

Problems

1. [6 pts] Searching the Internet for information about iptables (a UNIX implementation for local firewalls), write rules using iptables to allow traffic for ssh (port 22), allow all outgoing traffic, and deny all other traffic.

2. [8 pts] Using nmap, scan your computer and discuss any visible ports. See if you can determine the version of the OS that is running on your computer.

3. [6 pts] Suppose that you have a VPN with an X-bit symmetric key, a Y-bit public/private key, and an attacker that can test keys at a rate of N keys/second? How often should keys be changed in order to keep a B length (in terms of seconds) connection secure? You may assume that $Y \gg X$.

[5 pts] If X=48 bits, Y=2048 bits, N=1024 keys/sec, and B is 8 hours, does the symmetric key need to be changed?

4. [6 pts] Kerberos uses passwords as a key when the server sends the ticket/symmetric key to the user. Assuming the maximum password length is 8 characters, how big is the potential keyspace?

5. [6 pts] Recent research proposals by Microsoft to combat spam suggested making the sender compute a small math problem before the e-mail could be sent. Is this a viable solution and why or why not?

[4 pts] Would DES or RSA be good problems for this example?

6. [6 pts] IPSec is known to have issues with NAT. What are these issues and how can they be solved?