CSCI 667 - Homework 4*

Assigned November 22nd; Due 11:59pm on December 5th

Prof. Adwait Nadkarni

Note: This homework assignment is worth 60 points.

1 Worms {25 points}

(a) {5 points} You are the network administrator of an enterprise network, and you can view all network *flows* on your network, where a flow is defined as a four-tuple of *(srcIP,srcPort,destIP,destPort)*. (You can think of a flow as a connection.) Due to privacy requirements, you cannot inspect the payloads of packets. Given this vantage point, how might you detect the presence of a worm in your network?

(b) {5 points} Suppose each instance of a worm launched at time t_0 finds on average 5 vulnerable nodes per hour and each infection takes 30 minutes. How many nodes will be infected at time $t_0 + 12$ hours? Assume each node's search and infection efforts cannot be parallelized (i.e., the process is search, infect, search, infect, . . .).

(c) {5 points} You are a firewall administrator at a large organization. You are responsible for protecting the corporate network from malicious traffic. One method of securing your network is to use whitelisting (i.e., allowing only whitelisted IPs to send information into your network). What is a **major** disadvantage of IP whitelisting as a technique to thwart attacks from worms and botnets? (Limit your answer to one sentence.)

(d) {5 points} What is a **major** disadvantage of IP blacklisting as a technique to thwart attacks from worms and botnets? (Limit your answer to one sentence.)

(e) {5 points} Prof. Pedantic designs a worm detection system for enterprise networks. His system works by counting the number of outgoing connections from each IP address. The occurrence of a large number of outgoing connections indicates worm activity since, by definition, a worm needs to seek connections in order to spread. By contrast, most machines on the enterprise network communicate only with a few hosts (mail server, file server, etc.)

Would you expect Prof. Pedantic's solution to have a high true positive rate?[1] Why or why not?

[*] Last revised on November 22, 2024.

[1] Recall that the true positive rate $TPR = \frac{TP}{TP+FN}$, where TP is the number of true positives and FN is the number of false negatives. Further, a TP indicates a true alarm, while a FN indicates no alarm when there should have been one.

Would you expect Prof. Pedantic's solution to have a high false positive rate?[2] Why or why not?

2 Routing {15 points}

(a) {5 points} BGP hijack attacks can be classified into two types: *prefix* and *subprefix*. Which is more dangerous and why?

(b) {5 points} AS relationships can be classified as *customer-provider* and *peer-peer*. A customer AS pays the provider AS to both send and receive traffic. In contrast, peer ASes commonly have a settlement-free peering arrangement, meaning they transit each others traffic for free. ASes typically avoid forwarding traffic from one neighbor to another if it cannot generate revenue for doing so.

BGP prefix filtering rules are a whitelisting technique used to filter out bogus BGP announcements. Rules are commonly based on an economically motivated rule of thumb: AS a will typically announce a route to a neighboring AS n only if: (1) n is a customer of a; (2) the route for a prefix originated by a; or (3) the route is through a customer of a.

For what type of sources (e.g., customer, provider, peer) does prefix filtering work well? For what type of sources does it not work well? For both cases, explain why.

(c) {5 points} Briefly describe sBGP and give two reasons why the Internet has been slow to adopt it (and similar protocols).

3 Wireless {20 points}

(a) {5 points} Prof. Pedantic is setting up his home wireless network. After hearing about attacks on WiFi security protocols, Prof. Pedantic has devised an alternative scheme to prevent anyone from accessing his network. Instead of using WEP or WPA, he turns on SSID hiding and chooses a 20 character random text string for the SSID. Only devices that know the 20 character random SSID can join the network. Will this configuration prevent others from joining Prof. Pedantic's network? Why or why not?

(b) {5 points} Prof. Pedantic enhances his network setup by configuring MAC address filtering on his access point. Does this fix problem? Why or why not?

(c) {5 points} Eduroam uses WPA Enterprise to control access to WiFi networks at thousands of educational and research institutions. A key advantage of Eduroam is that the WiFi network administrator does not need to setup new accounts for visitors. Instead, clients create a TLS connection with home institutions for authentication.

Brenza et al. found that many Eduroam clients are not configured correctly and therefore a malicious Eduroam AP (potentially a rogue AP) can eavesdrop on usernames and passwords. What configuration problems lead to this problem and how does it happen?

[2] Recall that the false positive rate $FPR = \frac{FP}{FP+TN}$, where FP is the number of false positives and TN is the number of true negatives.

(d) {5 points} A public university uses Eduroam with EAP-TLS rather than a combination of EAP-TTLS and a password authentication variant of EAP such as EAP-PAP. How does this change the attack on poorly configured clients?

Submission Instructions

Submit your solution as a single PDF using Blackboard. To upload your assignment, navigate to the “Concepts of Computer Security (Fall 2024) course. Use the “Homework 4” assignment.

Writeups submitted in Word, ASCII, PowerPoint, Corel, RTF, Pages, and other non-PDF formats will not be accepted. Consider using LaTeX to format your homework solutions. (For a good primer on LaTeX, see the Not So Short Introduction to LATEX.)

Note that you may submit a PDF scan of hand a hand written solution; however, you will receive **0 points** if the instructor cannot read your hand writing. If the instructor has any difficulty reading your hand writing, you may not submit hand written solutions for future assignments.

Please post questions (especially requests for clarification) about this homework to Piazza.