Exam #3

COMP-5370/-6370

Released: Thur, 11Nov2021

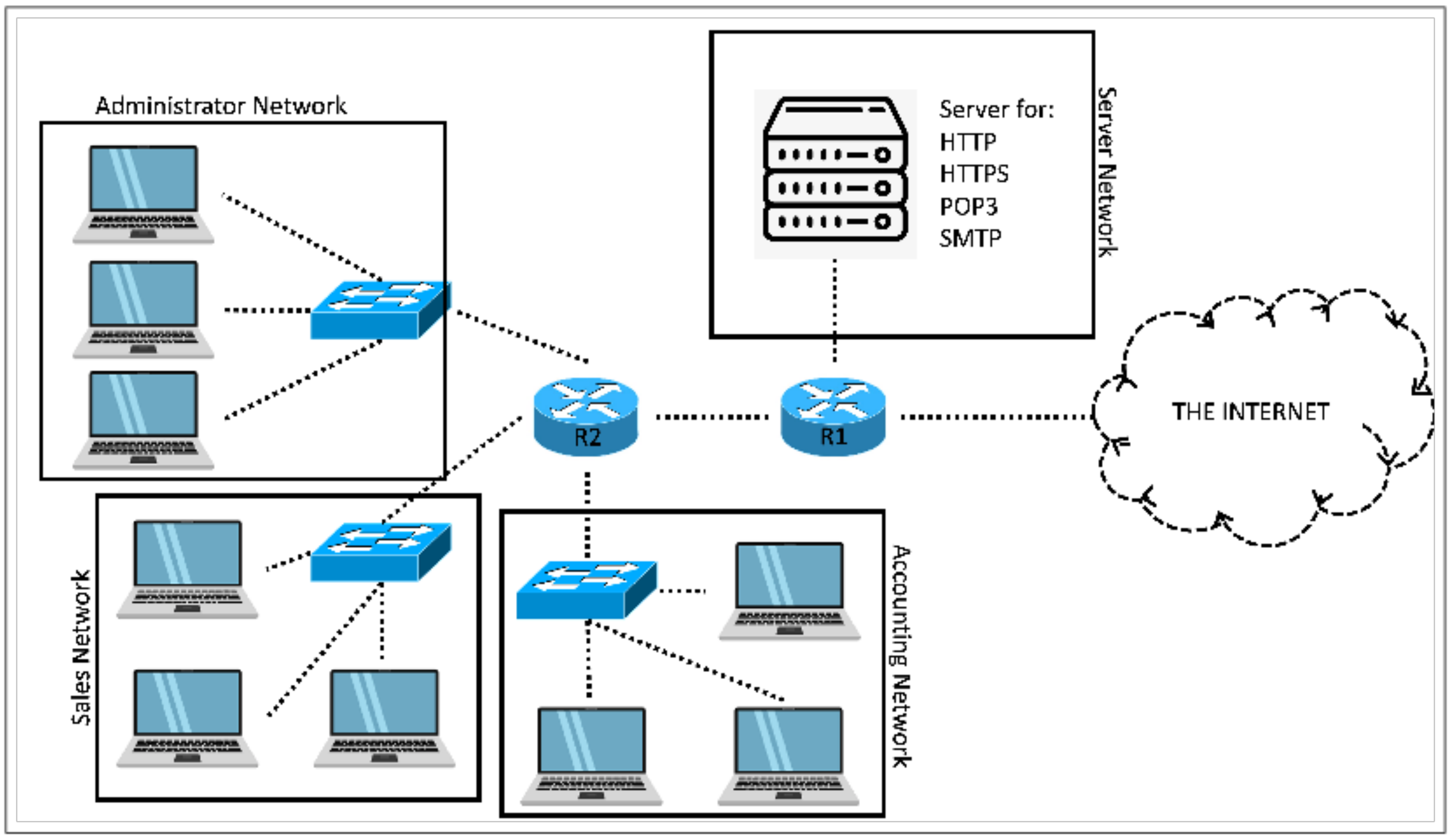
Due: Mon, 15Nov2021 at 6pm CT

This is a take-home exam and you are welcome to use the lecture-slides (available on the website) and any notes you took. You are **not** allowed to use the Internet, lecture videos/recordings, or collaborate with others in any way whatsoever. The questions have specifically been designed to not require deeper technical knowledge than what was discussed in-lecture so there should be no need to add new, external information.

If you have questions, please contact the instructor or TA via Discord or email at any time and we will respond as soon as possible. Do **not** use the Discord channels (#general, #distance, etc.) to ask questions about any aspect of the exam.

1. **Directional Firewall Rules** For the corporate network described in the below diagram, describe both where you would place the network firewall(s)[1] and what the configurations should be in order to protect the network. Don't forget that:

    1. Firewalls can have different inbound and outbound rule sets.
    2. "outbound" means "heading in the direction of the Internet" and "inbound" means "heading away from the Internet"
    3. You should have a catch-all as the last-rule.
    4. You have to tell us **where** each firewall is placed.
    5. Rules are evaluated in-order.



[1] up to 3 allowed

You are welcome to describe in any *logical and simple to interpret format* you wish. You should **NOT** provide commands, `iptables` rules, or any other hard-to-read format. It is safe to assume that:

1. SSH traffic is used for all administration.
2. No one needs to work remotely but customers still need to be able to access the website and communicate with employees over email.

An example of a good format is:
Firewall #1 placed between The Internet and R1.
Outbound Rules:

1. BLOCK traffic with destination TCP port 9999
2. ALLOW traffic with source TCP port 8888
3. ALLOW traffic with destination TCP port 7777 but only if the source IP is in the Sales Network
4. BLOCK all other traffic

Inbound Rules:

1. BLOCK traffic with destination TCP port 6666
2. ALLOW traffic with destination TCP port 5555 if destined for the Accounting Network
3. BLOCK traffic with source TCP port 5555
4. ALLOW all other traffic

2. Using the network and **your defined firewall configuration** from the above question, describe how an XSS and/or CSRF technique could be leveraged to nullify the defenses you have created. Your answer should be 3-5 sentence and demonstrate not only the attack but also your understanding of how the specific attributes of an XSS and/or CSRF style technique allow this attack to be possible.

3. **Attacker Anonymity vs. User Anonymity** An anonymous Denial of Service (DoS) attack can be accomplished by bouncing traffic through a non-cooperating server to hide the attack's true origin. The attacker does this by forging the source IP on traffic sent to the non-cooperating server. While this provides anonymity for the attacker, the same technique can **not** be used to add anonymity to the TLS protocol (i.e. can not forge the source IP on TLS traffic and expect it to function as-normal).

   In 2-4 sentences, describe both A) why this is the case and B) what would happen if it were attempted.

4. **Tor Circuit Selection** The Tor network's default circuit is three distinct nodes (Entry, Middle, and Exit) but allows the user to override that setting if they so wish. Why would it be dangerous to change the setting to 1 even if it is guaranteed that the lone Tor node is trustworthy and entirely well-intentioned?

5. **Tor Entry-Node Selection** When selecting an Entry node for a Tor circuit, the Tor client requires that the node be a functional Tor node for a minimum amount of time (nominally 1 month). This protects against a very particular type of attack which moderately-resourced actors could (and have been known to) launch in order to create a Denial of Service attack against Tor clients. Thinking from an attacker's perspective, what Denial of Service attack would be possible if Tor clients randomly selected an Entry node from all current Tor nodes every time they wished to create a new circuit?

6. **HTTPS Validation Logic** When an HTTPS client is validating the SSL certificate provided by the server, they check the "Common Name" field (among others) to ensure that it is the expected domain. While it is possible to put many different domain names in a single certificate, servers often use what's called a "wild-card certificate" to cover all sub-domains of a base domain name. A Common Name field of "*.google.com" would be validated as correct for "www.google.com", "mail.google.com", "docs.google.com", etc.

   If Dr. Springall was able to obtain a valid, browser-trusted certificate with a Common Name of "*google.com", how could he use that to attack clients with naively implemented validation logic?

NOTE — The logic for wildcards is **NOT** a regular expression. A "*" simply means string of zero or more ascii letters, numbers, dashes ("-"), or periods ".".

7. **Protection over Time** In versions of SSL/TLS prior to 1.3, a Diffie-Hellman KEX was **not** required and a shared secret could be created through a "client-write KEX" mechanism. The client would generate a random secret, encrypt it to the server's long-term SSL key, send the ciphertext value to the server, and the server would decrypt it using its SSL private key.

   This technique was removed entirely from TLS 1.3 due to the possibility of the server being compromised days, weeks, or months after the TLS tunnel was closed, a specific value being stolen, and that value being used to decrypt any TLS connection that used a client-write KEX. What was this value that could be stolen from the server? Why was this value likely to still exist on the server so long after the connection had been closed?

   NOTE — This is *not* related to session resumption nor to TLS 1.3's "early data".