cs458 A2

j585zhan

October 2018

1 Writting

1
a.
1)
ALLOW 72.36.115.128/26 ==> 0.0.0.0/0 FROM PORT 80 TO ALL BY TCP
2)
ALLOW 0.0.0.0/0 ==> 72.36.115.150 FROM PORT 80 TO 443 BY ALL
3)
ALLOW 0.0.0.0/0 ==> 72.36.115.175 FROM PORT 4700-4799 TO 4761 BY UDP
ALLOW 72.36.115.175 ==> 0.0.0.0/0 FROM PORT 4761 TO 4700-4799 BY UDP
4)
ALLOW 0.0.0.0/0 ==> 72.36.115.175 FROM PORT ALL TO 6667 BY TCP
5)
ALLOW 56.172.1.164 ==> 72.36.115.175 FROM PORT ALL TO 6667 BY TCP
6)
ALLOW 70.36.0.0/20 ==> 72.36.115.150 FROM PORT ALL TO 22 BY TCP
7)
DROP ALL FROM 0.0.0.0/0 ==> 72.36.115.128/26 FROM PORT ALL TO ALL BY ALL
b.
Yes it is possible. Since he can open a tcp connection to external web, this action allowed by rule 1 in firewall. After the connection is established, the stateful firewall will not interfere the data flow anymore.
Add the following rule to the firewall on the very beginning of the rules. Otherwise it will be allowed by the current 1st rule, and will not be checked by the new rule.
DROP 72.36.115.191 ==> 0.0.0.0/0 FROM PORT 80 TO ALL BY TCP
c.
No it is not. Because it does not have TLS to protect the connection. It could use TLS to makesure the connect is secured.
d.

No, because the firewall is aimed to filter the traffic between internal and external, it cannot detect if any router is compromised. However, the black hole attack is caused by compromised router to drop the package and achieved the DoS attack.
e.
Adversary could gain customers by redirecting the traffic thrgh their network.
f.
Advantage: it can drop spoofed traffic
Disdvantage: it cannot detect the compromised node/router. Can combine with personal firewall.

2
a.
i) read
ii) read
iii) none
iv) both
v) none
vi) write
vii) read
viii) none
b.
OQ $(Management, \{\phi, \nu, \rho, \eta\})$ READ D269 $(Management, \{\nu, \rho\})$,

$OQ = glb((Management, \{\phi, \nu, \rho, \eta\}), (Management, \{\nu, \rho\})) = (Management, \{\nu, \rho\})$

OQ $(Management, \{\nu, \rho\})$ WRITE empty string to D413 $(Executive, \{\phi, \nu, \rho, \chi\})$,

$D413 = glb((Management, \{\nu, \rho\}), (Executive, \{\phi, \nu, \rho, \chi\})) = (Management, \{\nu, \rho\})$

OQ $(Management, \{\nu, \rho\})$ READ D926 $(Developer, \{\phi, \nu, \rho\, \eta\})$

$OQ = glb((Management, \{\nu, \rho\}), (Developer, \{\phi, \nu, \rho, \eta\})) = (Developer, \{\nu, \rho\})$

OQ $(Developer, \{\nu, \rho\})$ WRITE empty string to D413 $(Management, \{\nu, \rho\})$,

$D413 = glb((Developer, \{\nu, \rho\}), (Management, \{\nu, \rho\})) = (Developer, \{\nu, \rho\})$

OQ $(Developer, \{\nu, \rho\})$ READ D342 $(CustomerSupport, \{\nu, \rho, \eta, \chi\})$

$OQ = glb((Developer, \{\nu, \rho\}), (CustomerSupport, \{\nu, \rho, \eta, \chi\})) = (CustomerSupport, \{\nu, \rho\})$

OQ $(CustomerSupport, \{\nu, \rho\})$ WRITE empty string to D413 $(Developer, \{\nu, \rho\})$,

$D413 = glb((CustomerSupport, \{\nu, \rho\}), (Developer, \{\nu, \rho\})) = (CustomerSupport, \{\nu, \rho\})$

OQ $(CustomerSupport, \{\nu, \rho\})$ READ D200 $(Public, \{\varepsilon\})$,

$$OQ = glb((CustomerSupport, \{\nu, \rho\}), (Public, \{\varepsilon\})) = (Public, \emptyset)$$

OQ $(Public, \emptyset)$ WRITE empty string to D413 $(CustomerSupport, \{\nu, \rho\})$,

$$D413 = glb((Public, \emptyset), (CustomerSupport, \{\nu, \rho\})) = (Public, \emptyset)$$

3
a. This is a MD5 produced hash.
b. No it is not. MD5 should not be using for storing password since it is fast to hash, therefore easier to brute force and reverse the hash result to get original text.
c. The organization's password encryption does not use the salt to encrypt same password to different cybertext. This is easy to get an attack with a pre-computed hashed password dictionary. To avoid it, it's better to use distinct iv to salt each password.
d. diffident
e. Company could use two factor authentication. It could requires the employee to scan his or her fingerprint along with the password to pass the authentication. The password is what a person 'know', plus the fingerprint is what a person 'is'.
f. There will be one alarm for correct catch, and $4999 * 0.01 \approx 50$ for false positive. The false positive rate will be $50/51 \approx 98\%$.
Company should not adopt this system since the false positive rate is significantly higher than the correct reported rate.

2 Programming

1.
c.
iii.
Developers could use the prepared statement with the query parameter to distinguish between the query syntax and query data. This approach requires developers to first define all sql code. Prepared statement make sure the attacker cannot change the initial intention of the query. For example, even the attacker input 'or 0=0 for the username, it will still interpret the 'or 0=0 as a string instead of a sql command
2.
c.
No SoP does not prevent the XSS attack. Same origin policy states that the script contained in the first page of web can access data on the second web page only if two web page have same origin. However it does not prevent the injected javascript run on the same origin. In this case the script is running on the same web page that victim is browsing.
d.
To prevent this specific xss attack, every user input should be validated and sanitized. All special characters should be escaped and treated as a normal string to prevent being interpreted as valid syntax.
3.

c.
One way can append an unique CSRF token to each request body, thus the developer will make sure the request is directly from user instead of the source from different user.
d.
developers can validate and sanitize everything from user input, make sure everything user typed that will not affect the page source code. For example if user put a link to the website, developers need to validate the link not contains any special character that will affect the syntax, and if so, the character need to be sanitized or escaped.
e.
Https will not eliminate such an attack. Https only assures that the communication to the server is secured and not mutated by the man in the middle. However in this case, if the communication is secured but is pointing to the different location than the users initial intention, Https will not detect that.
f.
No, it will not accept by server. Since No 'Access-Control-Allow-Origin' header is present on the ugster website(allow-access-control is wildcard), it only allow the request from same domain, thus, example.com is not allowed access.