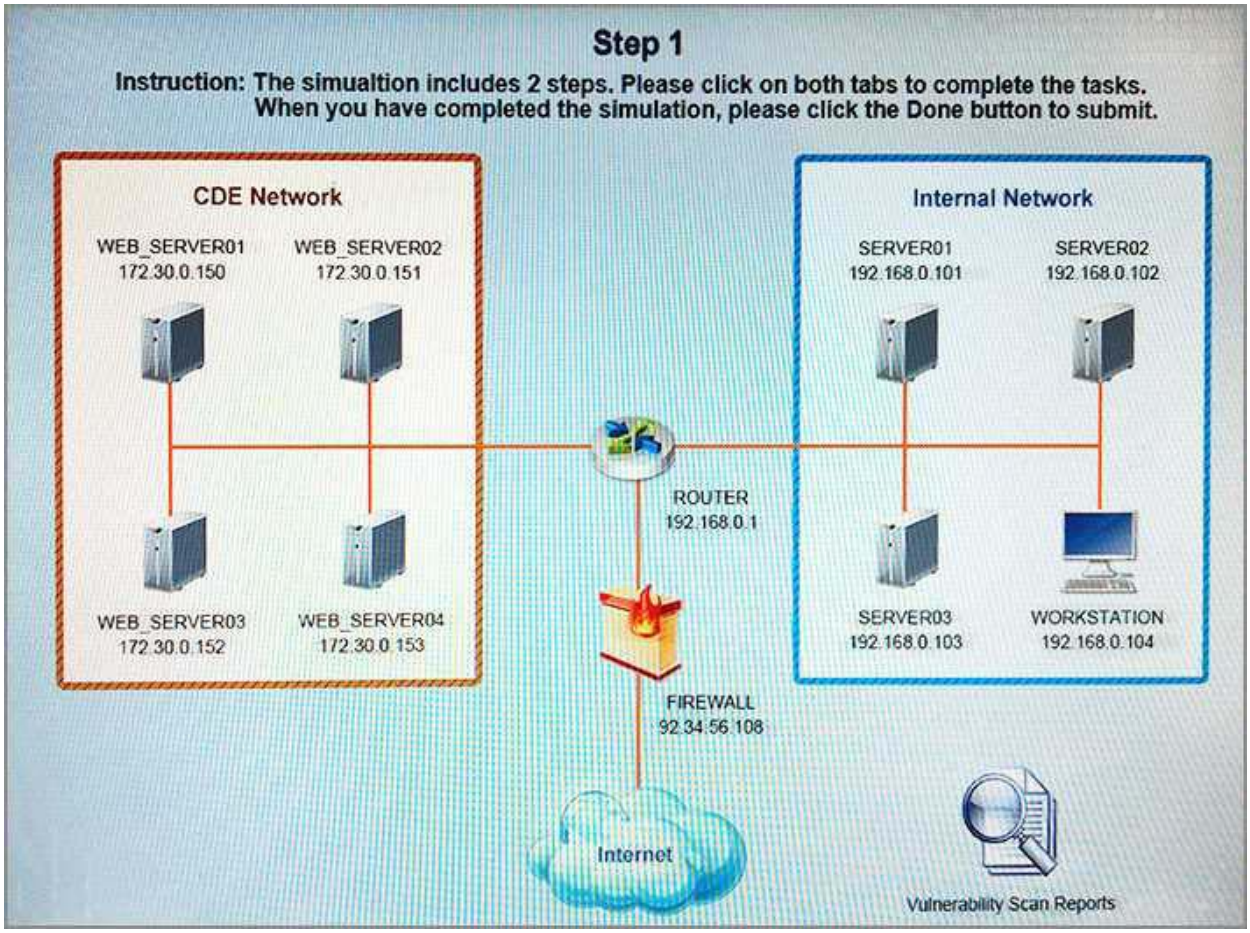
Question: 1

The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS.
If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean.
If the vulnerability is valid, the analyst must remediate the finding.
After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.
Instructions
STEP 1: Review the information provided in the network diagram.
STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button.



Step 2

Given the scenario, determine which remediation action is required to address the vulnerabilities.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Negative True Positive	Encrypt entire session Encrypt all session cookies Implement input validation Submit as non-issue Employ unique token in hidden field Avoid using redirects and forwards Disable http Request certificate from a public CA Renew the current certificate
WEB_SERVER02	False Positive False Negative True Negative True Positive	Encrypt entire session Encrypt all session cookies Implement input validation Submit as non-issue Employ unique token in hidden field Avoid using redirects and forwards Disable http Request certificate from a public CA Renew the current certificate
WEB_SERVER03	False Positive False Negative True Negative True Positive	Encrypt entire session Encrypt all session cookies Implement input validation Submit as non-issue Employ unique token in hidden field Avoid using redirects and forwards Disable http Request certificate from a public CA Renew the current certificate

Vulnerability Scan Report X

Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected Asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

MEDIUM SEVERITY

Title: Sensitive Cookie in HTTPS session without 'Secure' Attribute

Description: The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.

Affected Asset: 172.30.0.151

Risk: Session Sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 Certificate

Description: The server's TLS/SSL certificate is signed by a Certificate Authority that is untrusted or unknown.

Affected Asset: 172.30.0.152

Risk: May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

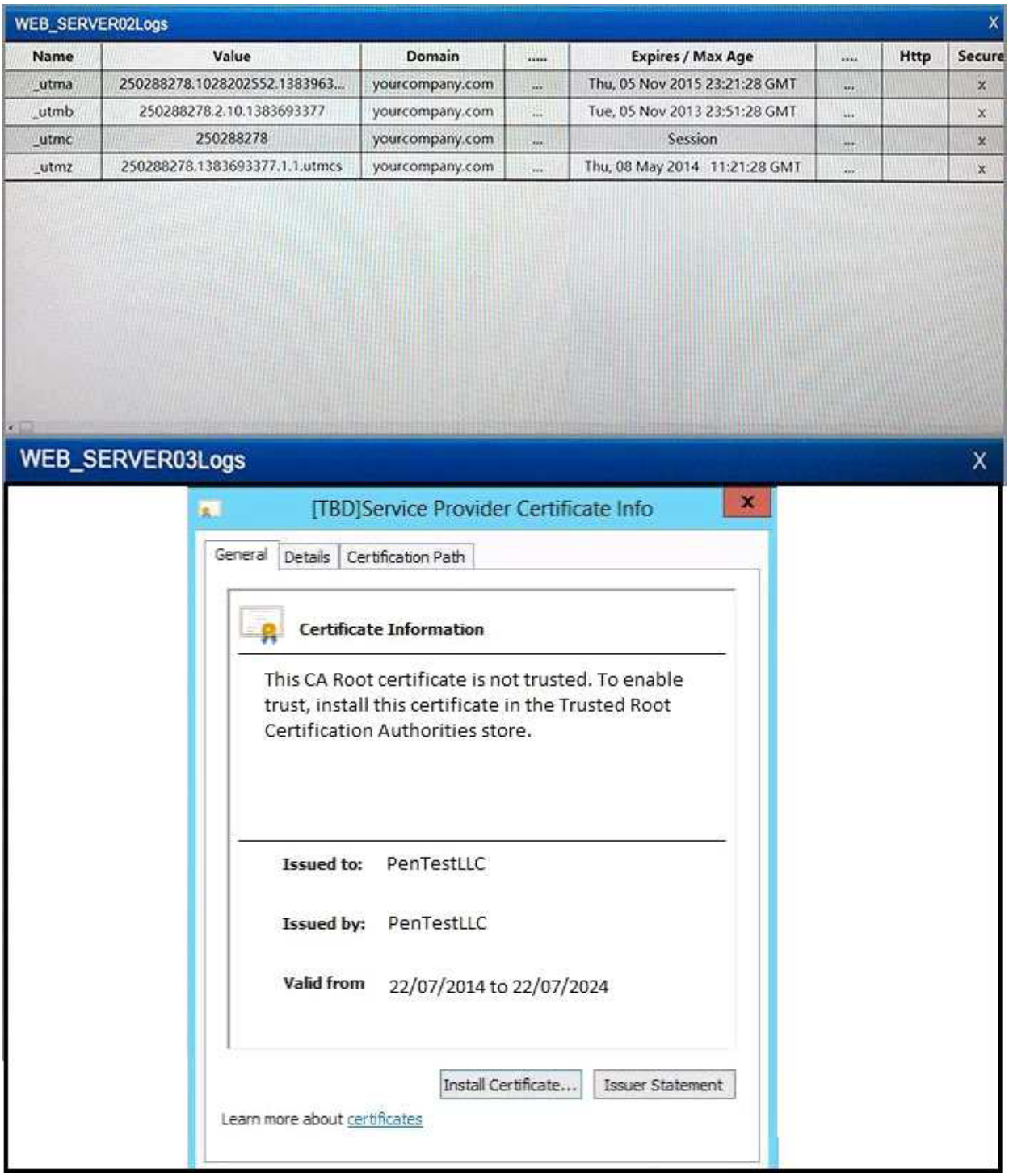
Reference: CVE-2005-1234

WEB_SERVER01Logs X

While logged in to the web portal (172.30.0.150) from the workstation (192.168.0.104) you perform an account password change. This process requires you to reenter the original password and enter a new password twice.

192.168.0.104	172.30.0.151	TLSv1	733	Application Data
172.30.0.151	192.168.0.104	TLSv1	1107	Application Data
192.168.0.104	172.30.0.151	TCP	66	44088 > https [ACK] Seq=1510 Ack=12723 Win=42368
192.168.0.104	172.30.0.150	HTTP	608	GET /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
172.30.0.151	192.168.0.104	TCP	66	http > 60928 [ACK] Seq=622 Ack=847 Win=5154 Len=...

Frame 4021: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: Vmware 00:03:22 (00:50:56:00:03:22), Dst: PaloAlto_39:1c:30 (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 172.30.0.150 (172.30.0.150)
[2 Reassembled TCP Segments (1496 bytes): #4820(1448), #4821(48)]
Hypertext Transfer Protocol
GET /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
Host: XXXXX\r\n
User – Agent: Mozilla/5.0 (x11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1\r\n
Accept: text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0\r\n
Accept-Language: en=US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http:/XXXXX/Shared/Portal/CustomProfiles/A_Profile.real\r\n
[truncated] Cookie: ASPSESSIONIDQABRBT BC=HEJCAHEDJPK08CEP; ZZZ; ECUSERPROPS=
Connection: keep alive\r\n
Content-Type: application/x-www- form-urlendcoded\r\n
Content-Length: 121\r\n
\r\n
[Full request URI: http//XXX/Shared/Portal/CustomProfiles/PostProfile.real?47=25378158]
Line-based text data: application/x-www-form-urlencoded
EMAIL=someone@cloud.org m&PASSold=PassWord1 m&PASSnew1=PassWord2 m&PASSnewv=PassWord2

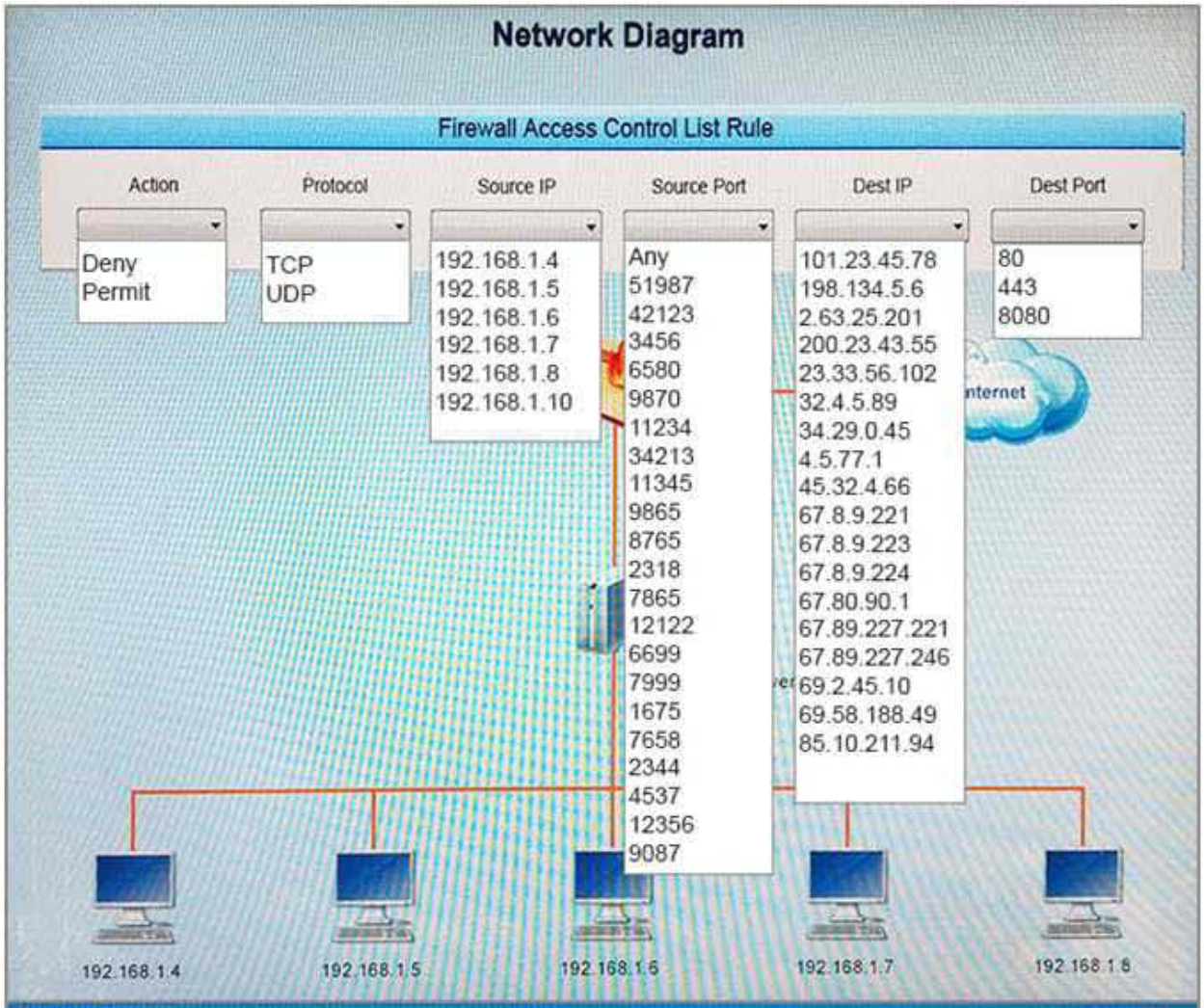


Solution

WEB_SERVER01: VALID – IMPLEMENT SSL/TLS
WEB_SERVER02: VALID – SET SECURE ATTRIBUTE WHEN COOKIE SHOULD SENT VIA HTTPS ONLY
WEB_SERVER03: VALID – IMPLEMENT CA SIGNED CERTIFICATE

Question: 2

HOTSPOT
A security analyst suspects that a workstation may be beaconing to a command and control server. Inspect the logs from the company's web proxy server and the firewall to determine the best course of action to take in order to neutralize the threat with minimum impact to the organization.
Instructions:
Modify the firewall ACL, using the Firewall ACL form to mitigate the issue.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button.



Web Logs

Time	SIP	Sport	DIP	Dport	Request Code	URL
12:01:00	192.168.1.4	2344	67.89.227.246	443	GET	company.cn
12:01:01	192.168.1.5	7658	67.89.227.221	443	GET	google.ru
12:01:02	192.168.1.7	9087	85.10.211.94	80	GET	provider.il
12:01:03	192.168.1.6	3456	2.63.25.201	80	POST	bqtest2.ru
12:01:04	192.168.1.8	12356	69.58.188.49	80	POST	testsite.jp
12:01:05	192.168.1.5	42123	198.134.5.6	443	POST	network.org
12:01:06	192.168.1.4	2318	4.5.77.1	443	GET	mynews.com
12:01:07	192.168.1.8	9865	32.4.5.89	80	GET	catala.com
12:01:08	192.168.1.6	9870	2.63.25.201	80	POST	bqtest2.ru
12:01:09	192.168.1.8	4537	69.2.45.10	80	POST	lillte.cn
12:01:10	192.168.1.5	7865	45.32.4.66	80	POST	portal.co.jp
12:01:11	192.168.1.6	51987	101.23.45.78	443	POST	malware.com
12:01:12	192.168.1.5	34213	200.23.43.55	443	GET	vortex.net
12:01:13	192.168.1.6	11234	2.63.25.201	80	POST	bqtest2.ru
12:01:14	192.168.1.6	8765	34.29.0.45	80	GET	colocation.com
12:01:15	192.168.1.4	1675	67.80.90.1	443	GET	johnson.com
12:01:16	192.168.1.7	11345	23.33.56.102	80	POST	college.edu
12:01:17	192.168.1.7	12122	67.8.9.221	443	GET	lalala.gov
12:01:18	192.168.1.6	6580	2.63.25.201	80	POST	bqtest2.ru
12:01:19	192.168.1.7	6699	67.8.9.223	80	POST	mystuff.ac.jp
12:01:20	192.168.1.5	7999	67.8.9.224	8080	GET	erdas.com

Deny TCP 192.168.1.6 Any 2.63.25.201 80

Question: 3

Which of the following BEST describes the offensive participants in a tabletop exercise?

A. Red team
B. Blue team
C. System administrators
D. Security analysts
E. Operations team

Answer: A

Question: 4

After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of:

A. privilege escalation.
B. advanced persistent threat.
C. malicious insider threat.
D. spear phishing.

Answer: B

Question: 5

A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

A. Succession planning
B. Separation of duties
C. Mandatory vacation
D. Personnel training
E. Job rotation

Answer: B,D

Question: 6

Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

A. Blue team training exercises
B. Technical control reviews
C. White team training exercises
D. Operational control reviews

Answer: A

Question: 7

A cybersecurity analyst is reviewing log data and sees the output below:

```
POST:// payload.php HTTP/1.1
HOST: localhost
Accept: */*
Referrer: http://localhost
**********
HTTP /1.1 403 Forbidden
connection : close
```

Which of the following technologies MOST likely generated this log?

A. Stateful inspection firewall
B. Network-based intrusion detection system
C. Web application firewall
D. Host-based intrusion detection system

Answer: C

Question: 8

A security analyst is reviewing a report from the networking department that describes an increase in network utilization, which is causing network performance issues on some systems. A top talkers report over a five-minute sample is included.

Source	Destination	Application	Packets	Volume(Kbps)
8.4.4.100	172.16.1.25	SMTP	4386	6141
96.23.114.14	172.16.1.1	IPSec	7734	10827
172.16.1.101	100.15.25.34	HTTP	3412	4776
96.23.114.18	172.16.1.1	IPSec	2723	3812
172.16.1.101	100.15.25.34	SSL	8697	12176
172.16.1.222	203.67.121.12	Quicktime	1302	1822
172.16.1.197	113.121.12.15	8180/tcp	6045	8463
172.16.1.131	172.16.1.67	DHCP	25	35
172.16.1.25	172.16.1.53	DNS	66	93

Given the above output of the sample, which of the following should the security analyst accomplish FIRST to help track down the performance issues?

A. Perform reverse lookups on each of the IP addresses listed to help determine if the traffic is necessary.
B. Recommend that networking block the unneeded protocols such as Quicktime to clear up some of the congestion.
C. Put ACLs in place to restrict traffic destined for random or non-default application ports.
D. Quarantine the top talker on the network and begin to investigate any potential threats caused by the excessive traffic.

Answer: A

Question: 9

A security analyst received a compromised workstation. The workstation's hard drive may contain evidence of criminal activities. Which of the following is the FIRST thing the analyst must do to ensure the integrity of the hard drive while performing the analysis?

A. Make a copy of the hard drive.
B. Use write blockers.
C. Run rm –R command to create a hash.
D. Install it on a different machine and explore the content.

Answer: B

Question: 10

File integrity monitoring states the following files have been changed without a written request or approved change. The following change has been made:
chmod 777 –Rv /usr
Which of the following may be occurring?

A. The ownership pf /usr has been changed to the current user.

B. Administrative functions have been locked from users.
C. Administrative commands have been made world readable/writable.
D. The ownership of/usr has been changed to the root user.

Answer: C