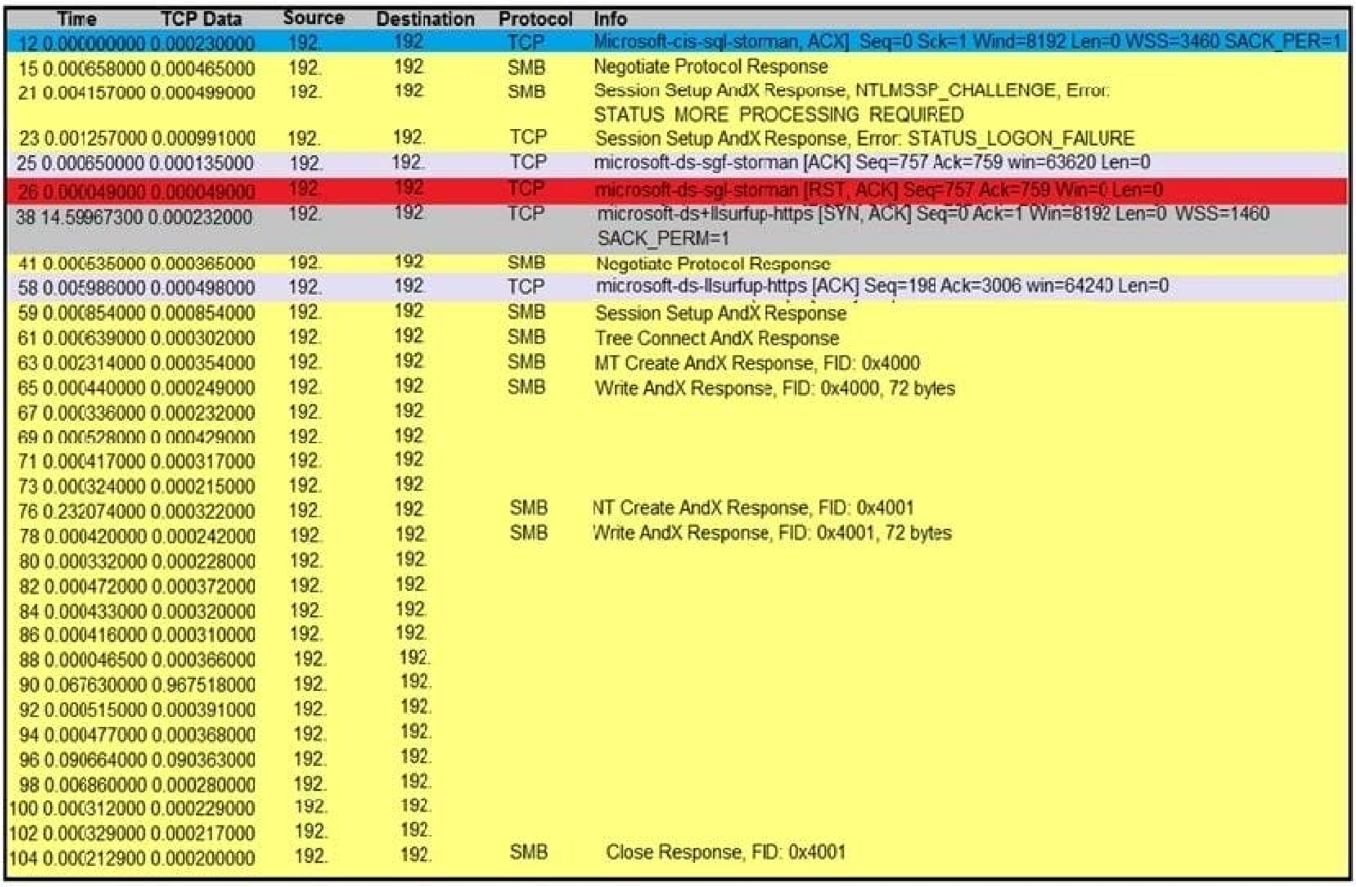
300-215 Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Pass Cisco 300-215 Exam with 100% Guarantee

QUESTION 1



	Time	TCP Data	Source	Destination	Protocol	Info
12	0.000000000	0.000230000	192.	192	TCP	Microsoft-cis-sql-storman, ACX] Seq=0 Sck=1 Wind=8192 Len=0 WSS=3460 SACK_PER=1
15	0.000658000	0.000465000	192.	192	SMB	Negotiate Protocol Response
21	0.004157000	0.000499000	192.	192	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS MORE PROCESSING REQUIRED
23	0.001257000	0.000991000	192.	192.	TCP	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
25	0.000650000	0.000135000	192.	192.	TCP	microsoft-ds-sgf-storman [ACK] Seq=757 Ack=759 win=63620 Len=0
26	0.000049000	0.000049000	192	192	TCP	microsoft-ds-sgl-storman [RST, ACK] Seq=757 Ack=759 Win=0 Len=0
38	14.59967300	0.000232000	192.	192	TCP	microsoft-ds+llsurfup-https [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 WSS=1460 SACK_PERM=1
41	0.000535000	0.000365000	192.	192	SMB	Negotiate Protocol Response
58	0.005986000	0.000498000	192.	192	TCP	microsoft-ds-llsurfup-https [ACK] Seq=198 Ack=3006 win=64240 Len=0
59	0.000854000	0.000854000	192.	192	SMB	Session Setup AndX Response
61	0.000639000	0.000302000	192.	192	SMB	Tree Connect AndX Response
63	0.002314000	0.000354000	192.	192	SMB	MT Create AndX Response, FID: 0x4000
65	0.000440000	0.000249000	192.	192	SMB	Write AndX Response, FID: 0x4000, 72 byles
67	0.000336000	0.000232000	192.	192		
69	0.000528000	0.000429000	192.	192		
71	0.000417000	0.000317000	192.	192		
73	0.000324000	0.000215000	192.	192		
76	0.232074000	0.000322000	192.	192	SMB	NT Create AndX Response, FID: 0x4001
78	0.000420000	0.000242000	192.	192	SMB	Write AndX Response, FID: 0x4001, 72 bytes
80	0.000332000	0.000228000	192.	192		
82	0.000472000	0.000372000	192.	192		
84	0.000433000	0.000320000	192.	192		
86	0.000416000	0.000310000	192.	192		
88	0.000046500	0.000366000	192.	192.		
90	0.067630000	0.967518000	192.	192.		
92	0.000515000	0.000391000	192.	192.		
94	0.000477000	0.000368000	192.	192.		
96	0.090664000	0.090363000	192.	192.		
98	0.006860000	0.000280000	192.	192.		
100	0.000312000	0.000229000	192.	192.		
102	0.000329000	0.000217000	192.	192.		
104	0.000212900	0.000200000	192.	192.	SMB	Close Response, FID: 0x4001

Refer to the exhibit. An engineer is analyzing a TCP stream in a Wireshark after a suspicious email with a URL. What should be determined about the SMB traffic from this stream?

A. It is redirecting to a malicious phishing website,

B. It is exploiting redirect vulnerability C. It is requesting authentication on the user site.

D. It is sharing access to files and printers.

Correct Answer: B

QUESTION 2

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

A. Introduce a priority rating for incident response workloads.

B. Provide phishing awareness training for the fill security team.

C. Conduct a risk audit of the incident response workflow.

D. Create an executive team delegation plan.

E. Automate security alert timeframes with escalation triggers.

Correct Answer: AE

QUESTION 3

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

A. An engineer should check the list of usernames currently logged in by running the command $ who | cut –d' ' -f1| sort | uniq

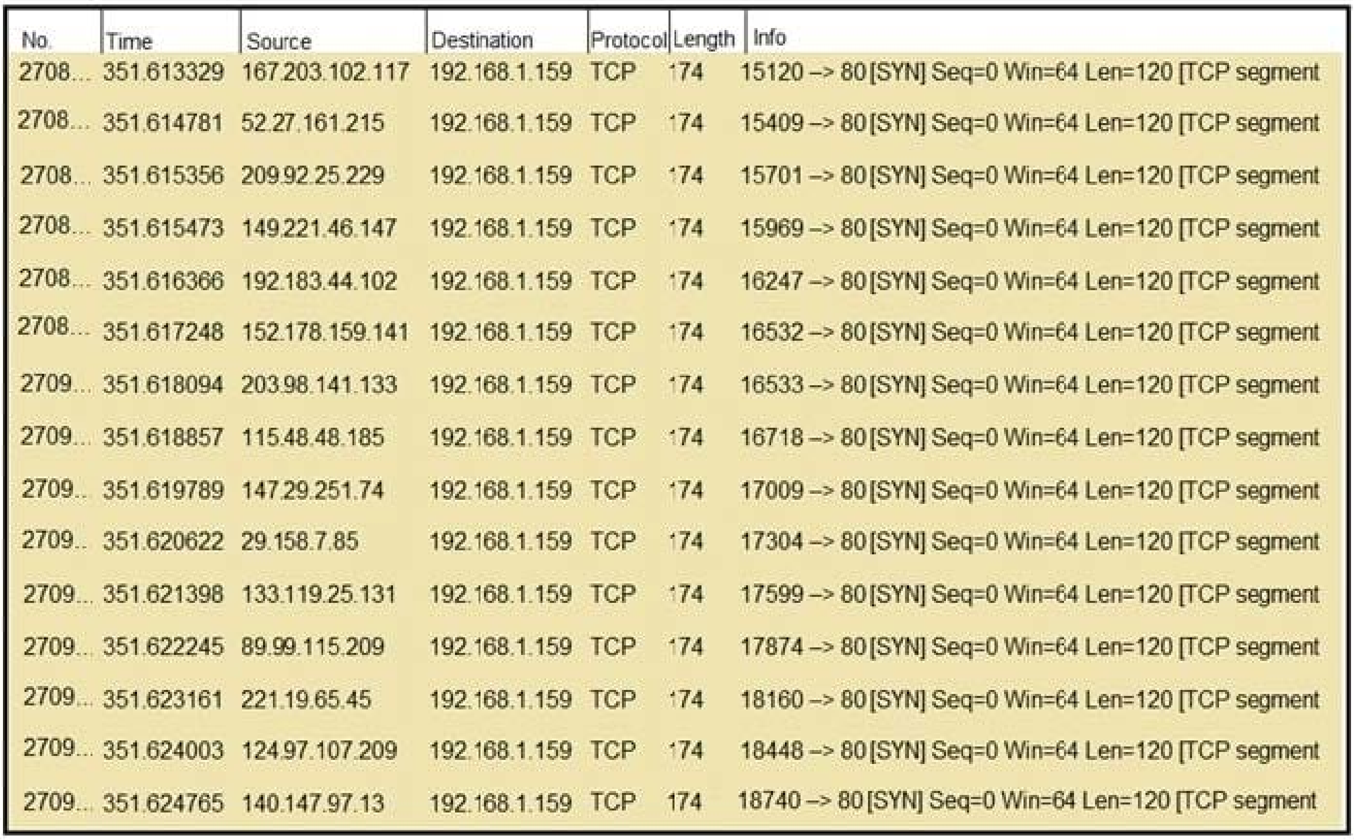
B. An engineer should check the server\\'s processes by running commands ps -aux and sudo ps -a.

C. An engineer should check the services on the machine by running the command service -status-all.

D. An engineer should check the last hundred entries of a web server with the command sudo tail -100 /var/log/apache2/access.log.

Correct Answer: D

QUESTION 4



No.	Time	Source	Destination	Protocol	Length	Info
2708...	351.613329	167.203.102.117	192.168.1.159	TCP	174	15120 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.614781	52.27.161.215	192.168.1.159	TCP	174	15409 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615356	209.92.25.229	192.168.1.159	TCP	174	15701 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615473	149.221.46.147	192.168.1.159	TCP	174	15969 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.616366	192.183.44.102	192.168.1.159	TCP	174	16247 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.617248	152.178.159.141	192.168.1.159	TCP	174	16532 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618094	203.98.141.133	192.168.1.159	TCP	174	16533 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618857	115.48.48.185	192.168.1.159	TCP	174	16718 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709..	351.619789	147.29.251.74	192.168.1.159	TCP	174	17009 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709..	351.620622	29.158.7.85	192.168.1.159	TCP	174	17304 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.621398	133.119.25.131	192.168.1.159	TCP	174	17599 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.622245	89.99.115.209	192.168.1.159	TCP	174	17874 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.623161	221.19.65.45	192.168.1.159	TCP	174	18160 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624003	124.97.107.209	192.168.1.159	TCP	174	18448 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624765	140.147.97.13	192.168.1.159	TCP	174	18740 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment

Refer to the exhibit. What should an engineer determine from this Wireshark capture of suspicious network traffic?

A. There are signs of SYN flood attack, and the engineer should increase the backlog and recycle the oldest half-open TCP connections.

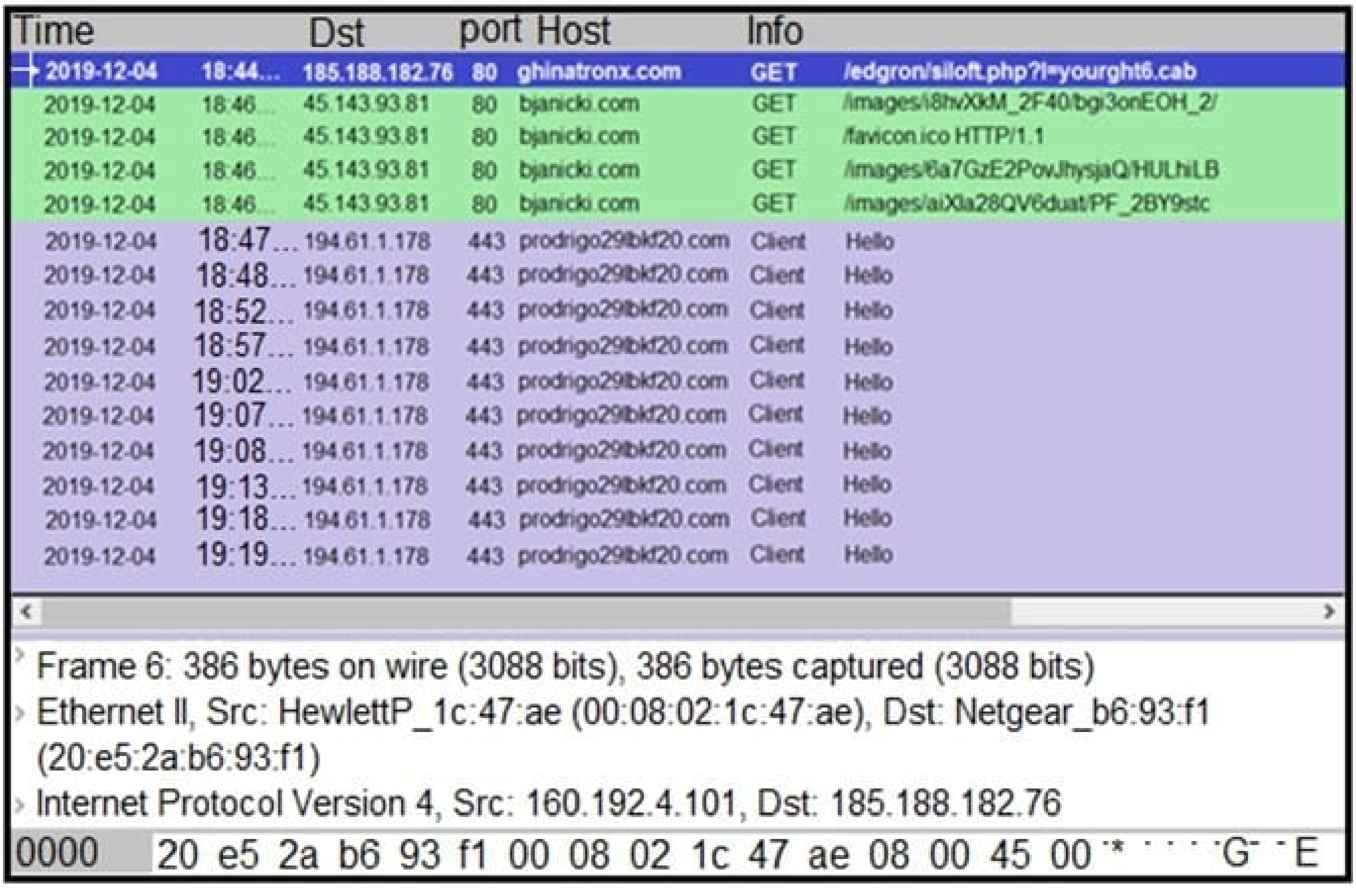
B. There are signs of a malformed packet attack, and the engineer should limit the packet size and set a threshold of bytes as a countermeasure.

C. There are signs of a DNS attack, and the engineer should hide the BIND version and restrict zone transfers as a countermeasure.

D. There are signs of ARP spoofing, and the engineer should use Static ARP entries and IP address-to-MAC address mappings as a countermeasure.

Correct Answer: A

QUESTION 5



```
Time                 Dst             port Host                  Info
2019-12-04  18:44...  185.188.182.76  80   ghinatronx.com        GET     /edgron/siloft.php?l=yourght6.cab
2019-12-04  18:46...  45.143.93.81    80   bjanicki.com          GET     /images/i8hvXkM_2F40/bgi3onEOH_2/
2019-12-04  18:46...  45.143.93.81    80   bjanicki.com          GET     /favicon.ico HTTP/1.1
2019-12-04  18:46...  45.143.93.81    80   bjanicki.com          GET     /images/6a7GzE2PovJhysjaQ/HULhiLB
2019-12-04  18:46...  45.143.93.81    80   bjanicki.com          GET     /images/aiXla28QV6duat/PF_2BY9stc
2019-12-04  18:47...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  18:48...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  18:52...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  18:57...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  19:02...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  19:07...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  19:08...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  19:13...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  19:18...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello
2019-12-04  19:19...  194.61.1.178    443  prodrigo29lbkf20.com  Client  Hello

> Frame 6: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1
  (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 160.192.4.101, Dst: 185.188.182.76
0000   20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00   *    G  E
```

Refer to the exhibit. A network engineer is analyzing a Wireshark file to determine the HTTP request that caused the initial Ursnif banking Trojan binary to download. Which filter did the engineer apply to sort the Wireshark traffic logs?

A. http.request.un matches

B. tls.handshake.type ==1

C. tcp.port eq 25

D. tcp.window_size ==0

Correct Answer: B

Reference:

https://www.malware-traffic-analysis.net/2018/11/08/index.html

https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/

[Latest 300-215 Dumps](#) [300-215 Study Guide](#) [300-215 Exam Questions](#)