300-215 Unterlagen mit echte Prüfungsfragen der Cisco Zertifizierung

Die Produkte von PrüfungFrage wird Ihnen nicht nur helfen, die Cisco 300-215 Zertifizierungsprüfung erfolgreich zu bestehen, sondern auch Ihnen einen einjährigen kostenlosen Update-Service bieten. Wir werden den Kunden die neuesten von uns entwickelten Produkte in der ersten Zeit liefern, so dass Sie sich gut auf die Cisco 300-215 Prüfung vorbereiten können. Falls Sie in der Cisco 300-215 Prüfung durchfallen, zahlen wir Ihnen dann die gesammte Summe zurück.

Die CISCO 300-215-Zertifizierungsprüfung richtet sich an Cybersecurity-Fachkräfte, die ihre Fähigkeiten und Kenntnisse in der forensischen Analyse und in der Vorfallreaktion unter Verwendung von Cisco-Technologien verbessern möchten. Diese Prüfung ist Teil des CISCO -zertifizierten Cyberops Professional -Zertifizierungsprogramms, das den Fachleuten die erforderlichen Fähigkeiten zur Bewältigung von ausgefeilten Cyber -Bedrohungen zur Verfügung stellt.

>> 300-215 Zertifizierungsfragen <<

300-215 Prüfungs & 300-215 Demotesten

Nur kontinuierlich zu verbessern kann man immer an der führenden Stelle stehen. Und es ist auch unsere Firmenphilosophie. Deshalb prüfen wir regelmäßig nach, ob die Cisco 300-215 Prüfung aktualisiert hat. Wenn sie aktualisiert hat, informieren wir unsere Kunden sofort darüber. Dadurch lassen Sie die neueste Informationen über Cisco 300-215 Prüfung erfahren. Aller Kundendienst der Aktualisierung nach der Kauf der Cisco 300-215 Software ist kostenlos innerhalb einem Jahr.

Die Prüfung deckt eine Reihe von Themen ab, die sich auf die Reaktion auf Vorfälle und die forensische Analyse beziehen, einschließlich der Reaktionsverfahren, der Erfassung und -analyse, der Bedrohungsanalyse sowie der Netzwerk- und Host-basierten Forensik. Es deckt auch die Verwendung verschiedener Cisco -Technologien wie Cisco Stealthwatch, Cisco Identity Services Engine (ISE) und Cisco Firepower ab, um Sicherheitsvorfälle zu erkennen, zu verhindern und auf Sicherheitsvorfälle zu reagieren.

Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps 300-215 Prüfungsfragen mit Lösungen (Q111-Q116):

111. Frage
Which tool is used for reverse engineering malware?

- A. NMAP
- B. Wireshark
- C. Ghidra
- D. SNORT

Antwort: C

112. Frage
An "unknown error code" is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

- A. var/log/shell.log
- B. /var/log/syslog.log
- C. /var/log/vmksummary.log
- D. var/log/general/log

Antwort: B

113. Frage
Refer to the exhibit.

Time	TCP Data	Source	Destination	Protocol	Info
12 0.000000000	0.000230000	192.	192.	TCP	Microsoft-cis-sql-storman, ACK] 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.[illegible]	[illegible]	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 bytes
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

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

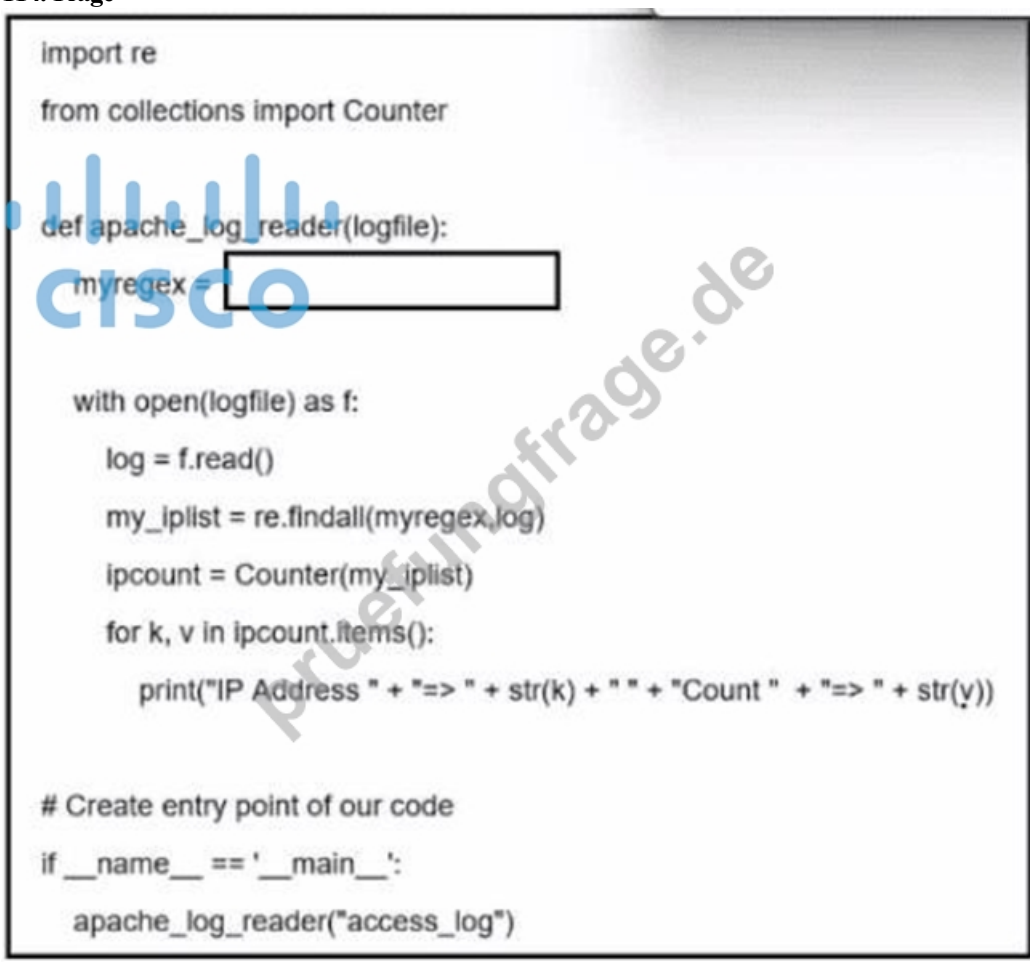
- A. It is requesting authentication on the user site.

- B. It is exploiting redirect vulnerability
- C. It is redirecting to a malicious phishing website
- D. It is sharing access to files and printers.

Antwort: D

Begründung:
The Wireshark output shows SMB protocol transactions, including NT Create AndX Response and Write AndX Response, indicating the transfer of files or objects. SMB (Server Message Block) is a protocol used for file sharing and printer access in Windows networks. The log does not indicate phishing or redirection behavior but rather normal SMB communication such as accessing files or shared resources.
-

114. Frage



Refer to the exhibit. A network administrator creates an Apache log parser by using Python. What needs to be added in the box where the code is missing to accomplish the requirement?

- A. r'*\b'
- B. r'\d(1,3),\d(1.3),\d{13}.df{1,3}'
- C. r'\b{1-9}[0-9}\b'
- D. r'\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}'

Antwort: D

Begründung:
The goal of the given Python code is to parse an Apache access log and extract IP addresses using regular expressions (regex). In this context, the most appropriate regex pattern to extract IPv4 addresses from log data is:
* r'\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}'
This pattern matches typical IPv4 addresses, where each octet consists of 1 to 3 digits separated by periods.
For example, it matches addresses like192.168.1.1or10.0.0.123. The pattern uses:

* \d{1,3}to capture between 1 and 3 digits,
* \.to match the dot (escaped since.is a special character in regex),
* repeated 4 times with proper separation to form the full IPv4 structure.
Options A, B, and C either include incorrect syntax, improper escape sequences, or do not represent a valid IP address pattern.
This type of log analysis and pattern extraction is described in the Cisco CyberOps Associate curriculum under basic scripting and automation techniques used in log and artifact analysis.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Section: "Basic Python Scripting for Security Analysts" and "Log Analysis and Data Extraction using Regex."

115. Frage
A threat intelligence report identifies an outbreak of a new ransomware strain spreading via phishing emails that contain malicious URLs. A compromised cloud service provider, XYZCloud, is managing the SMTP servers that are sending the phishing emails. A security analyst reviews the potential phishing emails and identifies that the email is coming from XYZCloud. The user has not clicked the embedded malicious URL.
What is the next step that the security analyst should take to identify risk to the organization?

- A. Reset the reporting user's account and enable multifactor authentication.
- B. Find any other emails coming from the IP address ranges that are managed by XYZCloud.
- C. Create a detailed incident report and share it with top management.
- D. Delete email from user mailboxes and update the incident ticket with lessons learned.

Antwort: B

Begründung:
Since the phishing email originates from a known compromised cloud provider (XYZCloud), the correct immediate action for the security analyst is to determine the broader scope of exposure. This involves checking whether other users in the organization received similar emails from the same potentially malicious source. Therefore, querying for emails from theIP address rangesorSMTP domainslinked to XYZCloud is essential for identifying other possible attack vectors.
This step aligns with the containment phase of the incident response lifecycle, as outlined in theCyberOps Technologies (CBRFIR) 300-215 study guide, where threat hunting and log analysis are used to determine the extent of compromise and prevent lateral movement or further exposure. Only after the scope is understood should remediation or reporting actions follow.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Email-Based Threats and Containment Strategy during Incident Response.

116. Frage
.....

- 300-215 Schulungsangebot - 300-215 Simulationsfragen - 300-215 kostenlos downloden Öffnen Sie die Webseite “ www.itzert.com ” und suchen Sie nach kostenloser Download von { 300-215 } 300-215 Vorbereitungsfragen
- 300-215 Simulationsfragen 300-215 Vorbereitung 300-215 Fragen Und Antworten Geben Sie ➠ www.zertfragen.com ein und suchen Sie nach kostenloser Download von { 300-215 } 300-215 German
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes