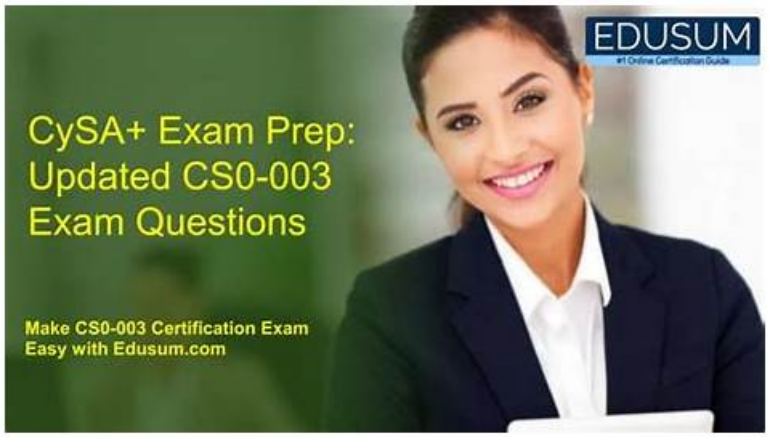
CS0-003 Exam - CS0-003 Schulungsangebot



Übrigens, Sie können die vollständige Version der PrüfungFrage CS0-003 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1-kxdIztUXrjdYW56004UCciE_r3OSrHc

Kein Wunder, dass die Schulungsunterlagen zur CompTIA CS0-003 Prüfungs von PrüfungFrage von der Mehrheit der Kandidaten gelobt werden. Das zeigt, dass unsere Schulungsunterlagen doch zuverlässig sind und den Kandidaten tatsächlich Hilfe leisten können. Die Kandidaten sind in der Lage, die CS0-003 Prüfung unbesorgt zu bestehen. Im vergleich zu anderen Websites ist PrüfungFrage immer noch der Best-Seller auf dem Market. Unter den Kunden hat der PrüfungFrage einen guten Ruf und wird von vielen anerkannt. Wenn Sie an der CompTIA CS0-003 Prüfung teilnehmen wollen, klicken Sie doch schnell PrüfungFrage. Ich glaube, Sie werden sicher was bekommen, was Sie wollen. Sonst würden Sie sicher bereuen. Wenn Sie ein professionelle IT-Experte werden wollen, dann fügen Sie es schnell in den Warenkorb hinzu.

Die Comptia Cybersecurity Analyst (CYSA+) -Zertifizierung, auch als CS0-003-Prüfung bezeichnet, ist eine global anerkannte Zertifizierung, die das Wissen und die Fähigkeiten einer Person auf dem Gebiet der Cybersicherheitsanalyse validiert. Diese Zertifizierung ist für Fachleute konzipiert, die sich auf den Bereich der Cybersicherheit spezialisieren möchten und ihre Fähigkeiten beim Erkennen, Verhinderung und Reagieren von Cybersicherheitsbedrohungen verbessern möchten.

>> CS0-003 Exam <<

Die anspruchsvolle CS0-003 echte Prüfungsfragen von uns garantiert Ihre bessere Berufsaussichten!

PrüfungFrage ist eine Website, die den Traum der IT-Fachleute erfüllen kann. PrüfungFrage bietet den Kandidaten die gewünschte Materialien, mit den Sie die Prüfung bestehen können. Machen Sie sich noch Sorgen um die CompTIA CS0-003 Zertifizierungsprüfung?Haben Sie schon mal gedacht, die relevanten Kurse von PrüfungFrage zu kaufen?Die Schulungsunterlagen von PrüfungFrage wird Ihnen helfen, die Prüfung effizienter zu bestehen. Die Fragen von PrüfungFrage sind den realen Prüfungsfragen ähnlich, fast mit ihnen identisch. Mit den genauen Prüfungsfragen und Antworten zur CompTIA CS0-003 Zertifizierungsprüfung können Sie die Prüfung leicht bestehen.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam CS0-003 Prüfungsfragen mit Lösungen (Q149-Q154):

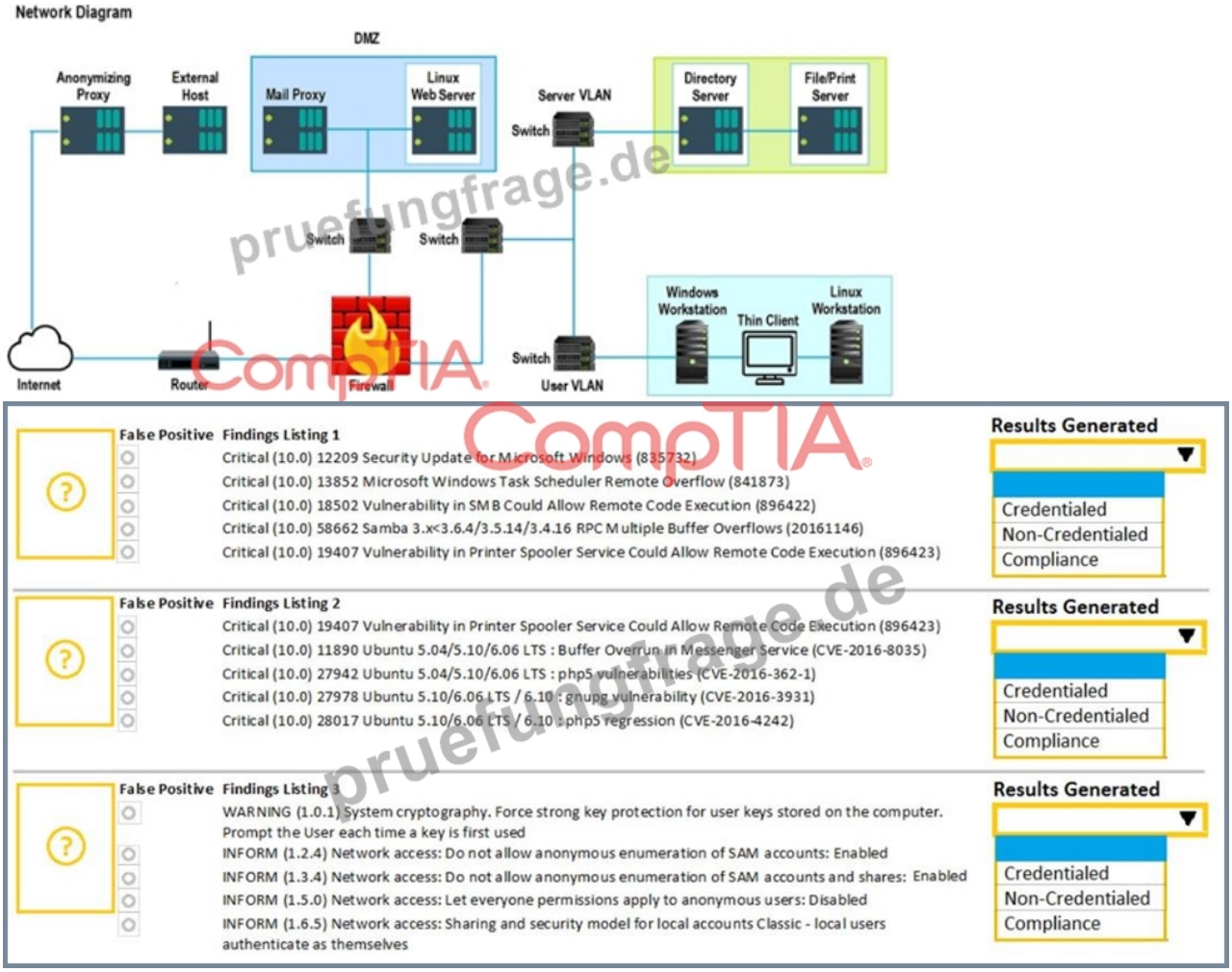
149. Frage
A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

- A. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H
- B. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L
- C. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
- D. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H

Antwort: B

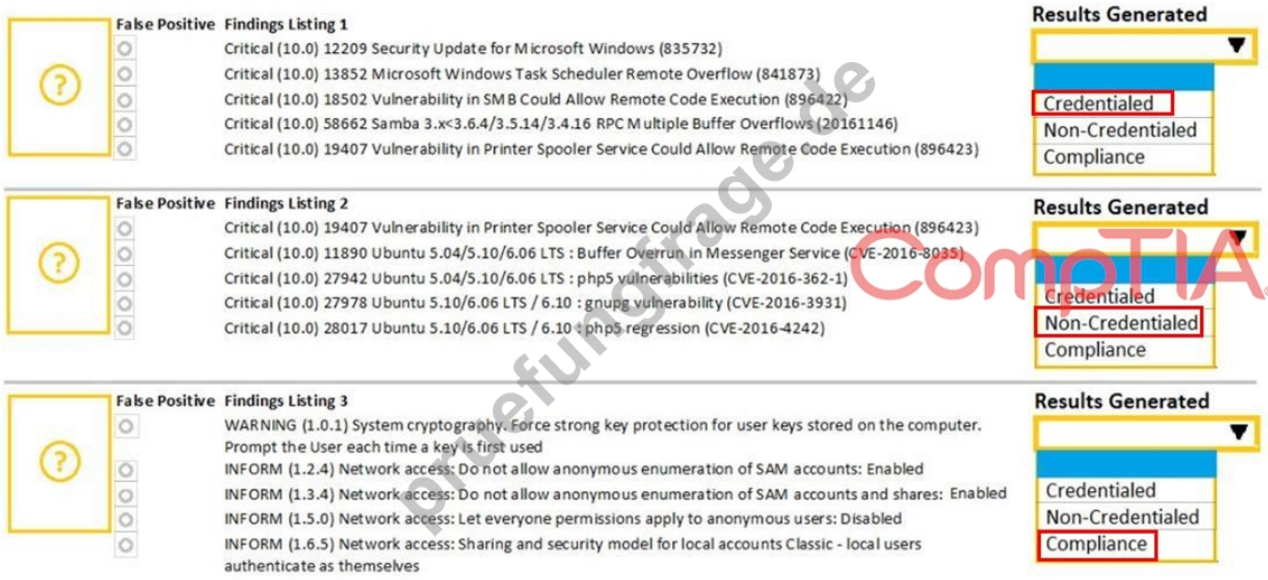
Begründung:
This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official Reference: https://nvd.nist.gov/vuln-metrics/cvss

150. Frage
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.
The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Antwort:

Begründung:



151. Frage
During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

- A. The risk would decrease because a web application firewall is in place.
- B. The risk would decrease because RDP is blocked by the firewall.
- C. The risk would increase because the host is external facing.
- D. The risk would not change because network firewalls are in use.

Antwort: B

Begründung:
Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.
References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 2: Software and Systems Security, page 67; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 3: Software and Systems Security, page 103.

152. Frage
Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

```
Nmap scan report for officerokuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerokuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
80/tcp    open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```


Which of the following choices should the analyst look at first?

- A. lan (192.168.86.22)
- B. imaging.lan (192.168.86.150)
- C. p4wnp1_aloa.lan (192.168.86.56)
- D. wh4dc-748gy.lan (192.168.86.152)
- E. xlaptop.lan (192.168.86.249)

Antwort: C

Begründung:
The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official Reference: https://github.com/mame82/P4wnP1_aloa

153. Frage
A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:

Log entry #	Message
Log entry 1	comptia.org/${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='../index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

Which of the following log entries provides evidence of the attempted exploit?

- A. Log entry 3
- B. Log entry 4
- C. Log entry 1
- D. Log entry 2

Antwort: B

Begründung:
Log entry 4 shows an attempt to exploit the zero-day command injection vulnerability by appending a malicious command (;cat /etc/passwd) to the end of a legitimate request (/cgi-bin/index.cgi?name=John). This command would try to read the contents of the /etc/passwd file, which contains user account information, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official Reference:
https://www.imperva.com/learn/application-security/command-injection/
https://www.zerodayinitiative.com/advisories/published/

154. Frage
.....

Die Schulungsunterlagen zur CompTIA CS0-003 Zertifizierungsprüfung aus unserem PrüfungFrage kann Ihren Traum - die CS0-003 Prüfung bestehen - verwirklichen, denn sie alle Dinge für den Durchlauf der CompTIA CS0-003 Zertifizierungsprüfung enthalten. Wählen Sie PrüfungFrage, können sie bestimmt die CompTIA CS0-003 Zertifizierungsprüfung bestehen, so werden Sie auch ein Mitglied der Eliten im IT-Bereich. Worauf warten Sie? Bitte beeilen Sie sich!

www.itzert.com Suchen Sie 「 CS0-003 」 Kostenloser Download CS0-003 Fragen Und Antworten

- Hohe Qualität von CS0-003 Prüfung und Antworten Suchen Sie auf ➥ www.pruefungfrage.de nach kostenlosem Download von ➡ CS0-003 CS0-003 Examengine
- iachm.com, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, lms.ait.edu.za, myportal.utt.edu.tt, study.stcs.edu.np, Disposable vapes

Übrigens, Sie können die vollständige Version der PrüfungFrage CS0-003 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1-kxdIztUXrjdYW56004UCciE_r3OSrHc