QUESTION 58
Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

A. chmod 666
B. chmod 774
C. chmod 775
D. chmod 777

Answer: D
Explanation:
https://www.pluralsight.com/blog/it-ops/linux-file-permissions

QUESTION 59
A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network.
What is the next step in handling the incident?

A. Block the source IP from the firewall
B. Perform an antivirus scan on the laptop
C. Identify systems or services at risk
D. Identify lateral movement

Answer: C

QUESTION 60
A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

A. Determine the systems involved and deploy available patches
B. Analyze event logs and restrict network access
C. Review access lists and require users to increase password complexity
D. Identify the attack vector and update the IDS signature list

Answer: A

QUESTION 61
A patient views information that is not theirs when they sign in to the hospital's online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue.

An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real- time. What is the first step the analyst should take to address this incident?

A. Evaluate visibility tools to determine if external access resulted in tampering
B. Contact the third-party handling provider to respond to the incident as critical
C. Turn off all access to the patient portal to secure patient records
D. Review system and application logs to identify errors in the portal code

Answer: C

QUESTION 62
Refer to the exhibit. What results from this script?

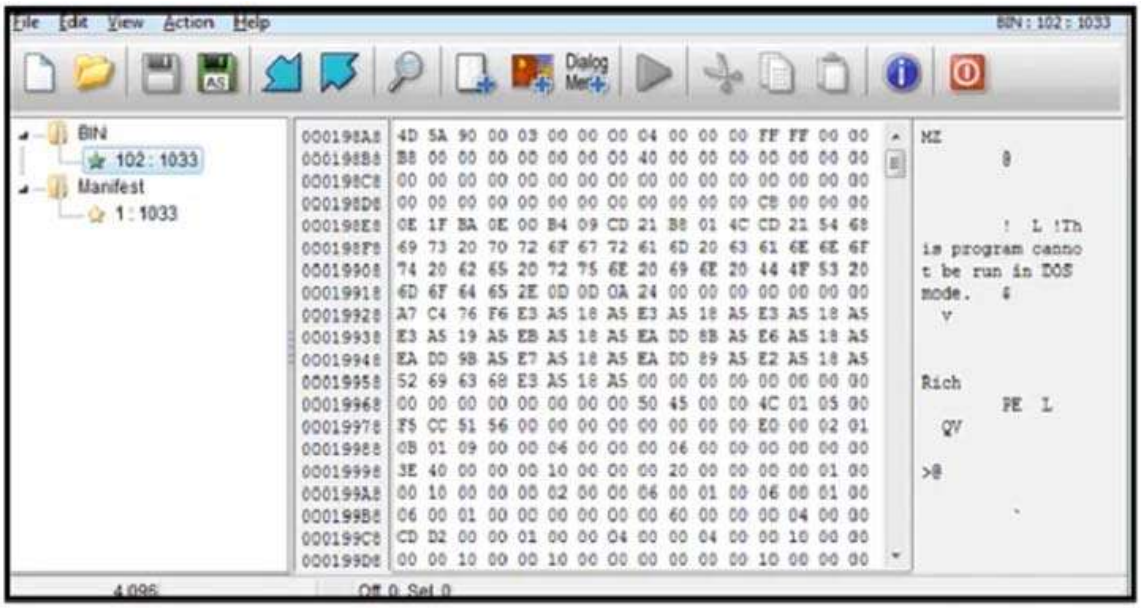
```
def map_to_lowercase_letter(s):
  return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
  dl = [ord(x) for x in list(domain)]
  dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
  dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
  dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
  dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
  return ''.join([chr(x) for x in dl])
def isBanjoriTail(seed):
 for c0 in xrange(97,123):
  for c1 in xrange(97, 123):
   for c2 in xrange(97,123):
    for c3 in xrange (97,123):
        domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
        domain = next_domain(domain)
        if seed.startswith(domain):
         return False
 return True
seeds = {
"nhcisatformalisticirekb.com",
"egfesatformalisticirekb.com",
"qwfusatformalisticirekb.com",
"eijhsatformalisticirekb.com",
"siowsatformalisticirekb.com",
"dhansatformalisticirekb.com",
"zvogsatformalisticirekb.com",
"yaewsatformalisticirekb.com",
"wgxfsatformalisticirekb.com",
"vfxlsatformalisticirekb.com",
"usjssatformalisticirekb.com",
"selzsatformalisticirekb.com",
"nzjqsatformalisticirekb.com",
"kencsatformalisticirekb.com",
"fzkxsatformalisticirekb.com",
"babysatformalisticirekb.com",
}
for seed in seeds:
  print seed,isBanjonTail(seed)
```

A. Seeds for existing domains are checked
B. A search is conducted for additional seeds

C. Domains are compared to seed rules
D. A list of domains as seeds is blocked

Answer: B

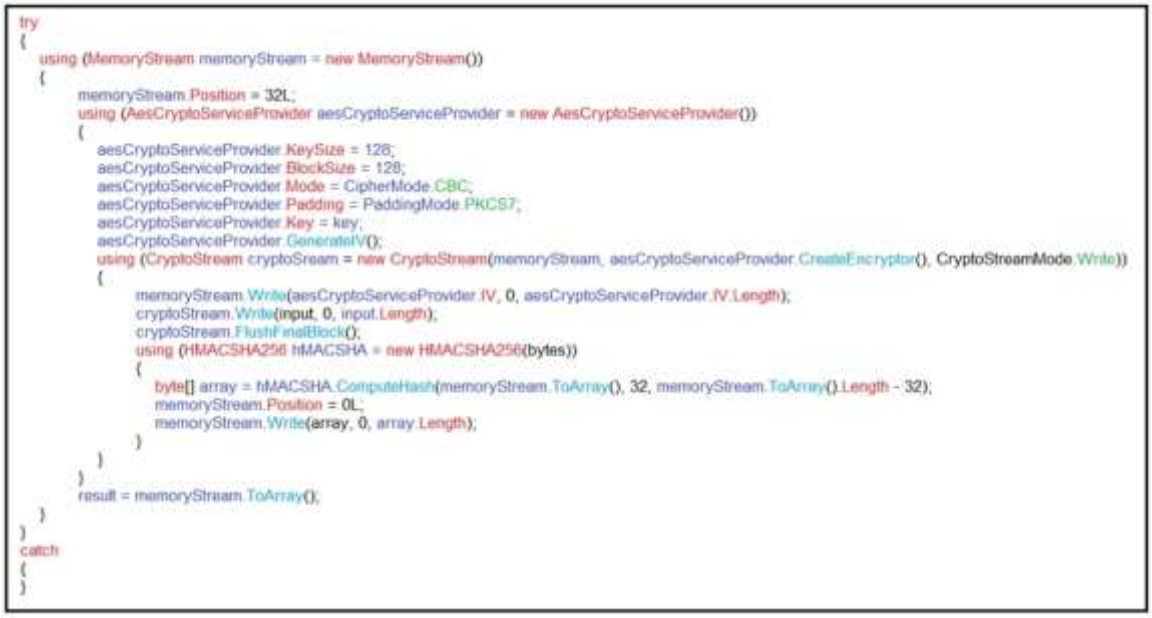
QUESTION 63
Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?



A. a DOS MZ executable format
B. a MS-DOS executable archive
C. an archived malware
D. a Windows executable file

Answer: A
Explanation:
The DOS MZ executable format is the executable file format used for. EXE files in DOS. The file can be identified by the ASCII string "MZ" (hexadecimal: 4D 5A) at the beginning of the file (the "magic number").

QUESTION 64
Refer to the exhibit. An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?



```
try
{
    using (MemoryStream memoryStream = new MemoryStream())
    {
        memoryStream.Position = 32L;
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoSream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
                memoryStream.Write(aesCryptoServiceProvider.IV, 0, aesCryptoServiceProvider.IV.Length);
                cryptoStream.Write(input, 0, input.Length);
                cryptoStream.FlushFinalBlock();
                using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
                {
                    byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                    memoryStream.Position = 0L;
                    memoryStream.Write(array, 0, array.Length);
                }
            }
        }
        result = memoryStream.ToArray();
    }
}
catch
{
}
```

A. The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.
B. The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.
C. The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.
D. The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

Answer: D
Explanation:
https://gist.github.com/yetanotherchris/810c5900616b6c76f78dedda9bf3be85

QUESTION 65
An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

A. HIPAA
B. FISMA
C. COBIT
D. PCI DSS

Answer: D
Explanation:
https://upserve.com/restaurant-insider/restaurant-pos-pci-compliance-checklist/

QUESTION 66
A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?

A. SNMPv2
B. TCP small services
C. port UDP 161 and 162
D. UDP small services

Answer: A
Explanation:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-snmp

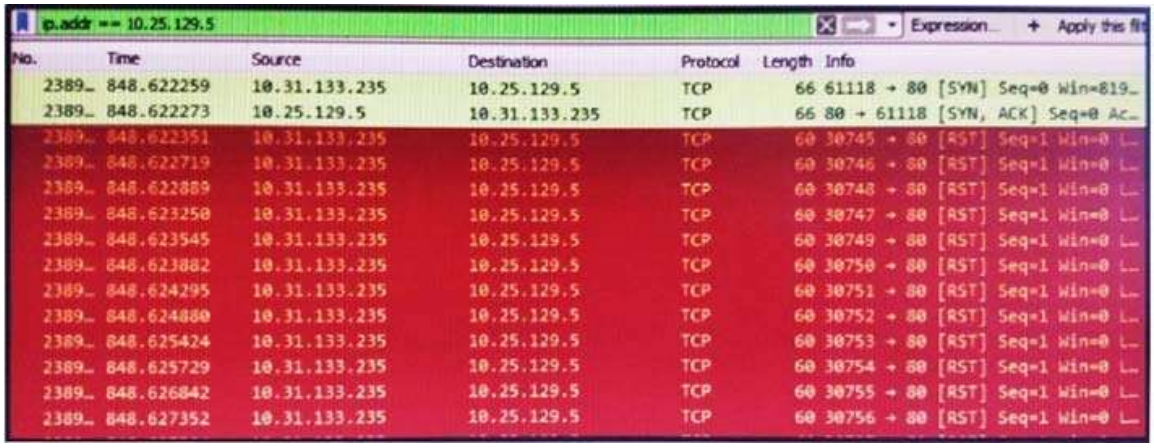
QUESTION 67
Refer to the exhibit. Which indicator of compromise is represented by this STIX?


```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
      {
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
        "created": "2020-08-10T13:49:37.079Z",
        "modified": "2020-08-10T13:49:37.079Z",
        "name": "Malicious site hosting downloader",
        "indicator_types":[
            "malicious-activity"
        ],
        "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
        "pattern_type": "stix",
        "valid_from": "2020-08-10T13:49:37.079Z"
      },
      {
        "type": "malware",
        "spec_version": "2.1",
        "id": "malware--162d917e-766f-4611-b5d6-652791454fca",
        "created": "2020-08-13T09:15:17.182Z",
        "modified": "2020-08-13T09:15:17.182Z",
        "name": "y2z7atc backdoor",
        "malware_types": [
            "backdoor",
            "remote-access-trojan"
        ],
        "is_family": false,
        "kil_chain_phases": [
            {
              "kill_chain_name": "mandant-attack-lifecycle-model",
              "phase_name": "establish-foothold"
            }
        ]
      },
      {
        "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--864af2ea-46f9-4d23-b3a2-1c2adf81c265",
        "created": "2020-08-15T18:03:58.029Z",
        "modified": "2020-08-15T18:03:58.029Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
        "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
      }
  ]
}
```


A. website redirecting traffic to ransomware server
B. website hosting malware to download files
C. web server vulnerability exploited by malware
D. cross-site scripting vulnerability to backdoor server

Answer: B

QUESTION 68
Refer to the exhibit. What is occurring in this packet capture?



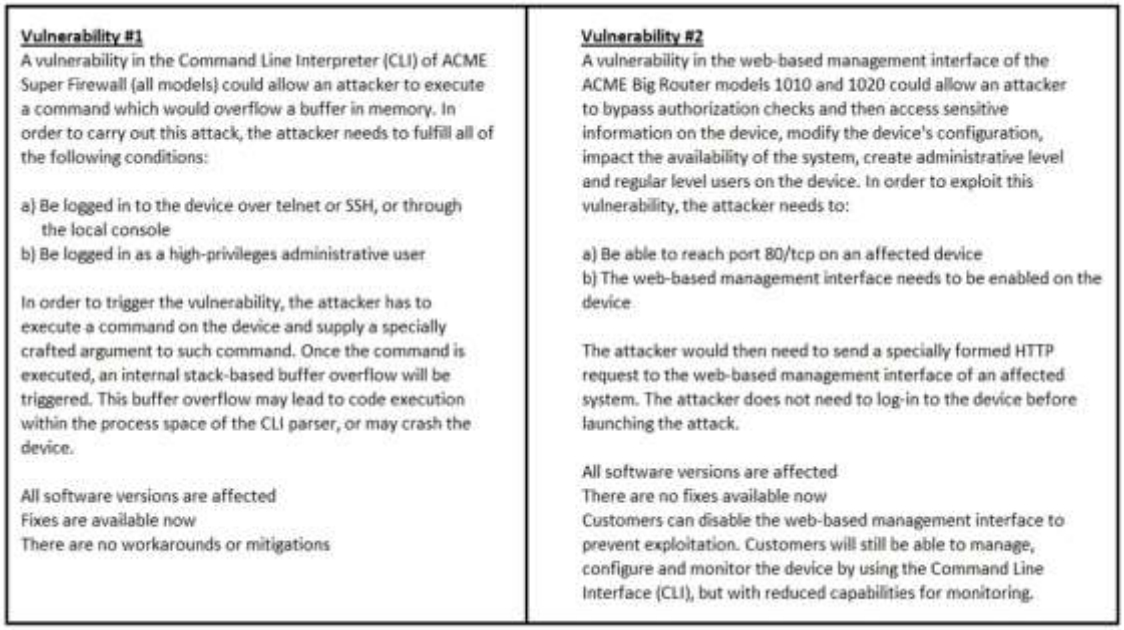
ip.addr == 10.25.129.5

No.	Time	Source	Destination	Protocol	Length	Info
2389...	848.622259	10.31.133.235	10.25.129.5	TCP	66	61118 → 80 [SYN] Seq=0 Win=819...
2389...	848.622273	10.25.129.5	10.31.133.235	TCP	66	80 → 61118 [SYN, ACK] Seq=0 Ac...
2389...	848.622351	10.31.133.235	10.25.129.5	TCP	60	30745 → 80 [RST] Seq=1 Win=0 L...
2389...	848.622719	10.31.133.235	10.25.129.5	TCP	60	30746 → 80 [RST] Seq=1 Win=0 L...
2389...	848.622889	10.31.133.235	10.25.129.5	TCP	60	30748 → 80 [RST] Seq=1 Win=0 L...
2389...	848.623250	10.31.133.235	10.25.129.5	TCP	60	30747 → 80 [RST] Seq=1 Win=0 L...
2389...	848.623545	10.31.133.235	10.25.129.5	TCP	60	30749 → 80 [RST] Seq=1 Win=0 L...
2389...	848.623882	10.31.133.235	10.25.129.5	TCP	60	30750 → 80 [RST] Seq=1 Win=0 L...
2389...	848.624295	10.31.133.235	10.25.129.5	TCP	60	30751 → 80 [RST] Seq=1 Win=0 L...
2389...	848.624880	10.31.133.235	10.25.129.5	TCP	60	30752 → 80 [RST] Seq=1 Win=0 L...
2389...	848.625424	10.31.133.235	10.25.129.5	TCP	60	30753 → 80 [RST] Seq=1 Win=0 L...
2389...	848.625729	10.31.133.235	10.25.129.5	TCP	60	30754 → 80 [RST] Seq=1 Win=0 L...
2389...	848.626842	10.31.133.235	10.25.129.5	TCP	60	30755 → 80 [RST] Seq=1 Win=0 L...
2389...	848.627352	10.31.133.235	10.25.129.5	TCP	60	30756 → 80 [RST] Seq=1 Win=0 L...

A. TCP port scan
B. TCP flood
C. DNS flood
D. DNS tunneling

Answer: B

QUESTION 69
Refer to the exhibit. How must these advisories be prioritized for handling?



Vulnerability #1
A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:

a) Be logged in to the device over telnet or SSH, or through the local console
b) Be logged in as a high-privileges administrative user

In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.

All software versions are affected
Fixes are available now
There are no workarounds or mitigations

Vulnerability #2
A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to:

a) Be able to reach port 80/tcp on an affected device
b) The web-based management interface needs to be enabled on the device

The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack.

All software versions are affected
There are no fixes available now
Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.

A. The highest priority for handling depends on the type of institution deploying the devices
B. Vulnerability #2 is the highest priority for every type of institution
C. Vulnerability #1 and vulnerability #2 have the same priority
D. Vulnerability #1 is the highest priority for every type of institution

Answer: B
Explanation:
All that is needed is port 80 access on #2 whereas #1 requires a login by a privileged account to exploit.

QUESTION 70
The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

A. Conduct a risk assessment of systems and applications
B. Isolate the infected host from the rest of the subnet
C. Install malware prevention software on the host
D. Analyze network traffic on the host's subnet

Answer: B
Explanation:
Short-term containment - limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.

QUESTION 71
An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

A. diagnostic
B. qualitative
C. predictive
D. statistical

Answer: C
Explanation:
What Is Predictive Analytics?
When you know what happened in the past and understand why it happened, you can then begin to predict what is likely to occur in the future based on that information. Predictive analytics takes the investigation a step further, using statistics, computational modeling, and machine learning to determine the probability of various outcomes.
What Is Diagnostic Analytics?
Once you know what happened, you'll want to know why it happened. That's where diagnostic analytics comes in. Understanding why a trend is developing or why a problem occurred will make your business intelligence actionable. It prevents your team from making inaccurate guesses, particularly related to confusing correlation and causality.

QUESTION 72
A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

A. Assess the network for unexpected behavior
B. Isolate critical hosts from the network
C. Patch detected vulnerabilities from critical hosts
D. Perform analysis based on the established risk factors

Answer: B

QUESTION 73
Refer to the exhibit. Cisco Advanced Malware Protection installed on an end-user desktop automatically submitted a low prevalence file to the Threat Grid analysis engine. What should be concluded from this report?

Analysis Report

ID	5c723eb4d706of70875ddtb69009d8fc	Filename	ee482400446236cb3f5ad7ed035bd77ad40140058b6d0e6ffe639ec9bfebc8f2.eml
OS	Windows 7 64-bit	Magic Type	SMTP mail, ASCII text
		Analyzed As	eml
Started	10/13/20 06:22:43	SHA256	ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639, ec9bfebc8f2
Ended	10/13/20 06:29:19		
Duration	0:06:36	SHA1	d700bca5b65aaf0c613d702d9a28a6084692224
Sandbox	rcn-work-042 (pilot-d)	MD5	58d1163715089192a8177a5244b9658f

Behavioral Indicators

Email References Localhost in Received Message Trace	Severity: 40	Confidence: 100
Document Contains Embedded Material and Minimal Content	Severity: 50	Confidence: 80
Download Forced Open/Save Prompt	Severity: 50	Confidence: 75
Email With Different Sender and Return-Path Detected	Severity: 60	Confidence: 60
Process Users Very Large Command-Line	Severity: 40	Confidence: 80
File Downloaded to Disk	Severity: 30	Confidence: 90
Potential Code Injection Detected	Severity: 50	Confidence: 50
HTTP Client Error Response	Severity: 50	Confidence: 50
Sample Communicates With Only Benign Domains	Severity: 20	Confidence: 95
Executable with Encrypted Sections	Severity: 30	Confidence: 30
Outbound Communications to Nginx Web Server	Severity: 25	Confidence: 25
Outbound HTTP POST Communications	Severity: 25	Confidence: 25
Document Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

A. Threat scores are high, malicious ransomware has been detected, and files have been modified
B. Threat scores are low, malicious ransomware has been detected, and files have been modified
C. Threat scores are high, malicious activity is detected, but files have not been modified
D. Threat scores are low and no malicious file activity is detected

Answer: D

QUESTION 74
An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since deploying certificates and tracking them requires searching server owners manually. Which action will improve workflow automation?

A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.
B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.
C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.
D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.

Answer: D
Explanation:
https://www.studocu.com/row/document/arab-academy-for-science-technology-maritime-transport/marketing/top-security-orchestration-use-cases/35519516

QUESTION 75
Refer to the exhibit. Which data format is being used?

```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

A. JSON
B. HTML
C. XML
D. CSV

Answer: C

QUESTION 76
The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

A. Contain the malware
B. Install IPS software
C. Determine the escalation path
D. Perform vulnerability assessment

Answer: A

QUESTION 77
An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

A. ExecutedMalware.ioc
B. Crossrider.ioc
C. ConnectToSuspiciousDomain.ioc
D. W32 AccesschkUtility.ioc

Answer: A
Explanation:
Crossrider is a an Adware variant that targets Mac with the intent of displaying ads. It also changes the default home page of Safari and Chrome browsers.
W32.AccesschkUtility.ioc
Accesscheck is a Windows utility that lets users check for access rights on resources including files, directories, registry keys, global objects and Windows services. This utility could be used by malware or threat actors with malicious intent such as collection of information necessary for privilege escalation on the compromised host. This indicator monitors for accesschk tool used with suspicious options that suppress errors and dialog boxes.
ExecutedMalware.ioc
A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.

QUESTION 78

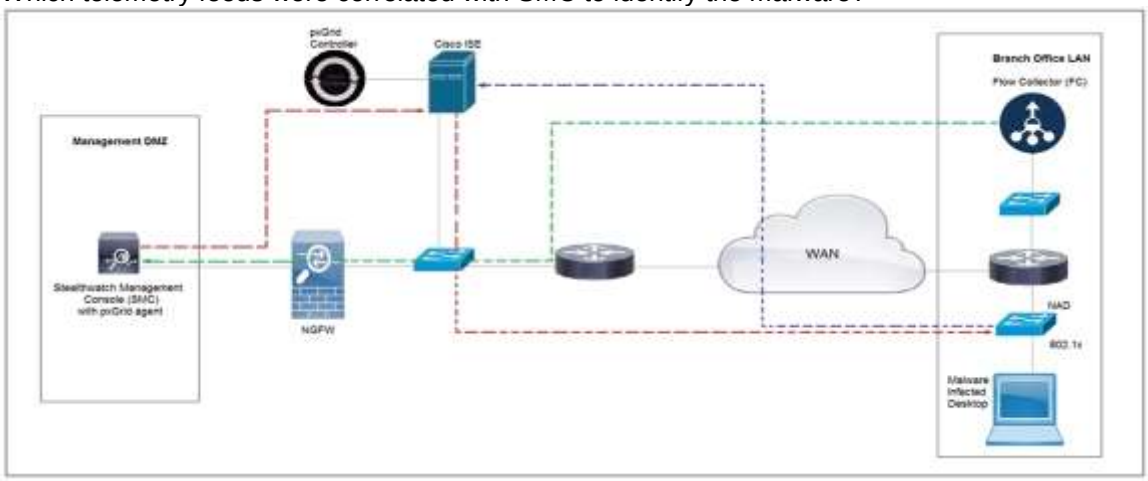
Refer to the exhibit. Which command was executed in PowerShell to generate this log?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. Get-EventLog -LogName*
B. Get-EventLog -List
C. Get-WinEvent -ListLog* -ComputerName localhost
D. Get-WinEvent -ListLog*

Answer: B
Explanation:
This "Get-EventLog -List" command gets a list of event logs along with their properties such as maximum size, retention, overflow action, and the number of entries.

QUESTION 79
Refer to the exhibit. Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy.
Which telemetry feeds were correlated with SMC to identify the malware?



A. NetFlow and event data
B. event data and syslog data
C. SNMP and syslog data
D. NetFlow and SNMP

Answer: B

QUESTION 80
A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

A. DLP for data in motion
B. DLP for removable data
C. DLP for data in use
D. DLP for data at rest

Answer: C
Explanation:
https://www.endpointprotector.com/blog/what-is-data-loss-prevention-dlp/

QUESTION 81
A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
C. Review the server backup and identify server content and data criticality to assess the intrusion risk
D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

Answer: A

QUESTION 82
A security expert is investigating a breach that resulted in a $32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack. Which step was missed that would have prevented this breach?

A. use of the Nmap tool to identify the vulnerability when the new code was deployed
B. implementation of a firewall and intrusion detection system
C. implementation of an endpoint protection system
D. use of SecDevOps to detect the vulnerability during development

Answer: D
Explanation:
https://securityintelligence.com/how-to-prioritize-security-vulnerabilities-in-secdevops/

QUESTION 83
An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

A. Restrict the number of requests based on a calculation of daily averages. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
B. Implement REST API Security Essentials solution to automatically mitigate limit exhaustion. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
C. Increase a limit of replies in a given interval for each API. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
D. Apply a limit to the number of requests in a given time interval for each API. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D
Explanation:
https://www.whoishostingthis.com/resources/http-status-codes/

QUESTION 84
Refer to the exhibit. IDS is producing an increased amount of false positive events about brute force attempts on the organization's mail server. How should the Snort rule be modified to improve performance?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-
IMAP login brute force attempt";
flow:to_server,established,no_stream;
content:"LOGIN",fast_pattern,nocase; detection_filter:track
by_dst, count 5, seconds 900; metadata:ruleset community;
service:imap; reference:url,attack.mitre.org/techniques/T1110;
classtype:suspicious-login; sid:2273; rev:12; )
```

A. Block list of internal IPs from the rule
B. Change the rule content match to case sensitive
C. Set the rule to track the source IP
D. Tune the count and seconds threshold of the rule

Answer: C
Explanation:
Step 1 Identify Potential Locations for Sensors - To properly tune IDS sensors, the first step is to identify network locations where the sensors can be placed for maximum efficiency.
https://www.ccexpert.us/ccie-security/ids-tuning.html

QUESTION 85
Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

A. customer data
B. internal database
C. internal cloud
D. Internet

Answer: D
Explanation:
Threat intelligence tools gather data from a variety of sources across the Internet, including open-source intelligence (OSINT), threat feeds, public and private forums, dark web sites, and other online resources. This wide-ranging data collection helps identify and track malicious activity and emerging threats.

QUESTION 86
An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to "output alert_syslog: output log"
B. Modify the output module rule to "output alert_quick: output filename"
C. Modify the alert rule to "output alert_syslog: output header"
D. Modify the output module rule to "output alert_fast: output filename"

Answer: D
Explanation:
2.6.2 alert_fast
This will print Snort alerts in a quick one-line format to a specified output file. It is a faster alerting method than full alerts because it doesn't need to print all of the packet headers to the output file and because it logs to only 1 file.

QUESTION 87
A company's web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

A. assessment scope
B. event severity and likelihood
C. incident response playbook
D. risk model framework

Answer: B
Explanation:
To conduct an assessment the following steps are required:
1) Identify threat sources and events
2) Identify vulnerabilities and predisposing conditions
3) Determine likelihood of occurrence
4) Determine magnitude of impact
5) Determine risk
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (page 32)

QUESTION 88
An employee who often travels abroad logs in from a first-seen country during non-working hours.
The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out.
The investigation concludes that the external domain belongs to a competitor.
Which two behaviors triggered UEBA? (Choose two.)

A. domain belongs to a competitor
B. log in during non-working hours
C. email forwarding to an external domain
D. log in from a first-seen country
E. increased number of sent mails

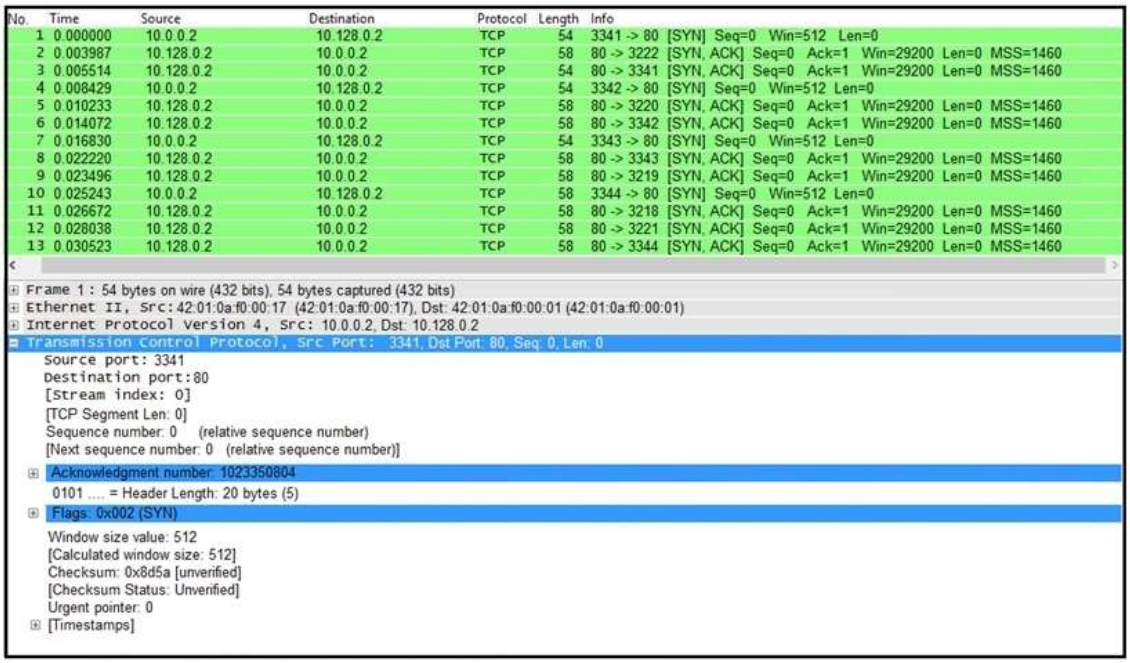
Answer: BD
Explanation:
UEBA (User and Entity Behavior Analytics)
(D). log in from a first-seen country User Behavior
(B). log in during non-working hours User Behavior

QUESTION 89
How is a SIEM tool used?

A. To collect security data from authentication failures and cyber attacks and forward it for analysis
B. To search and compare security data against acceptance standards and generate reports for analysis
C. To compare security alerts against configured scenarios and trigger system responses
D. To collect and analyze security data from network devices and servers and produce alerts

Answer: D
Explanation:
https://www.varonis.com/blog/what-is-siem/

QUESTION 90
Refer to the exhibit. What is the threat in this Wireshark traffic capture?



A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
B. A flood of ACK packets coming from a single source IP to multiple destination IPs
C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs
D. A flood of SYN packets coming from a single source IP to a single destination IP

Answer: D

QUESTION 91
An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering
B. data regression
C. data ingestion
D. data obfuscation

Answer: C
Explanation:
Technically, data ingestion is the process of transferring data from any source. But that's not always the case as businesses have multiple units, each having its own applications, file types, and systems. To make business decisions, companies port-in data from these heterogeneous sources onto a single storage medium, typically a data warehouse or a data mart after passing it through the Extract, Transfer, Load (ETL) process.
https://dataintegrationinfo.com/what-is-data-ingestion

QUESTION 92
What is a benefit of key risk indicators?

A. clear perspective into the risk position of an organization
B. improved visibility on quantifiable information
C. improved mitigation techniques for unknown threats
D. clear procedures and processes for organizational risk

Answer: A
Explanation:
https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time