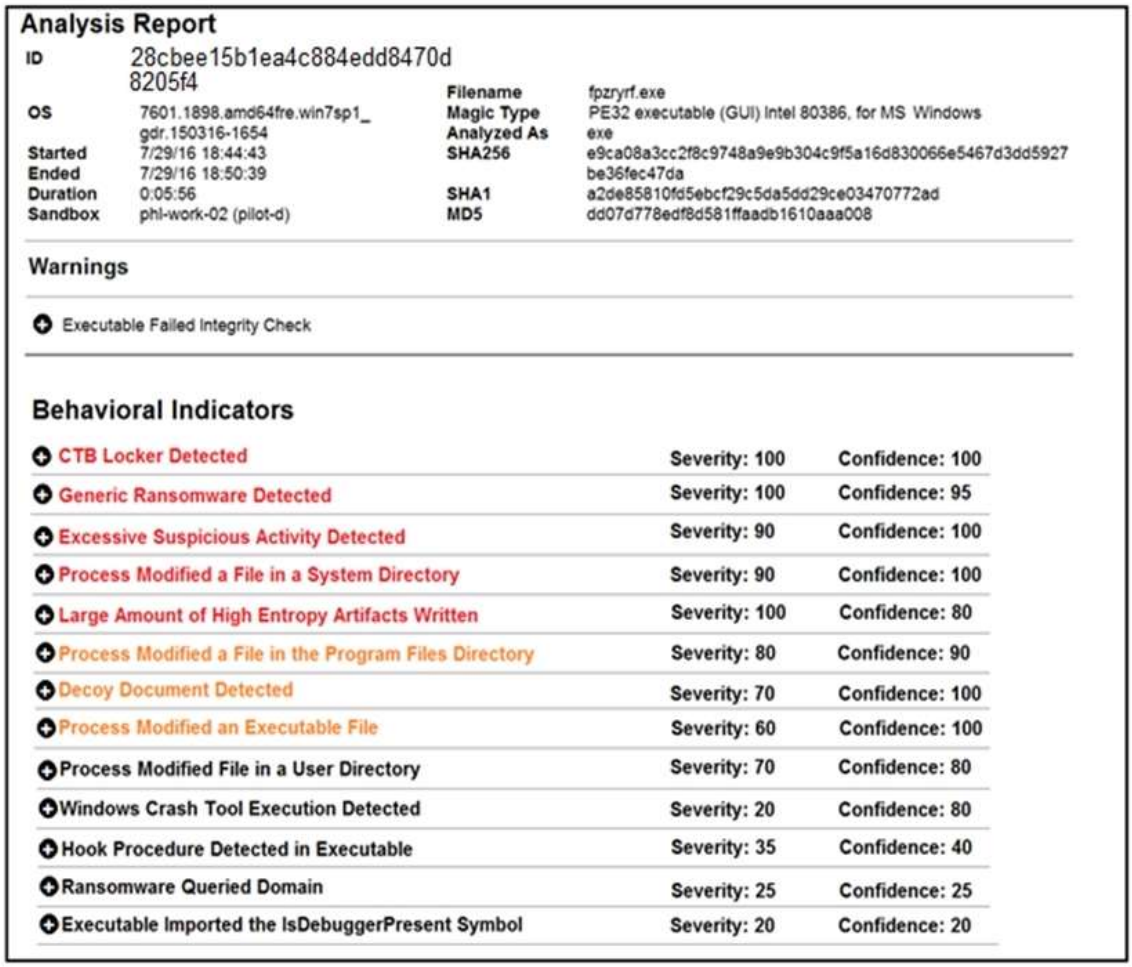
QUESTION 43
Refer to the exhibit. A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A. packet sniffer
B. malware analysis
C. SIEM
D. firewall manager

Answer: A

QUESTION 44
Refer to the exhibit. Cisco Advanced Malware Protection installed on an end-user desktop has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?



Analysis Report

ID	28cbee15b1ea4c884edd8470d8205f4		
		Filename	fpzryrf.exe
OS	7601.1898.amd64fre.win7sp1_gdr.150316-1654	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
		Analyzed As	exe
Started	7/29/16 18:44:43	SHA256	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
Ended	7/29/16 18:50:39		
Duration	0:05:56	SHA1	a2de85810fd5ebcf29c5da5dd29ce03470772ad
Sandbox	phl-work-02 (pilot-d)	MD5	dd07d778edf8d581ffaadb1610aaa008

Warnings

- Executable Failed Integrity Check

Behavioral Indicators

CTB Locker Detected	Severity: 100	Confidence: 100
Generic Ransomware Detected	Severity: 100	Confidence: 95
Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100
Process Modified a File in a System Directory	Severity: 90	Confidence: 100
Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80
Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
Decoy Document Detected	Severity: 70	Confidence: 100
Process Modified an Executable File	Severity: 60	Confidence: 100
Process Modified File in a User Directory	Severity: 70	Confidence: 80
Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80
Hook Procedure Detected in Executable	Severity: 35	Confidence: 40
Ransomware Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

A. The prioritized behavioral indicators of compromise do not justify the execution of the "ransomware" because the scores do not indicate the likelihood of malicious ransomware.
B. The prioritized behavioral indicators of compromise do not justify the execution of the "ransomware" because the scores are high and do not indicate the likelihood of malicious ransomware.
C. The prioritized behavioral indicators of compromise justify the execution of the "ransomware" because the scores are high and indicate the likelihood that malicious ransomware has been detected.
D. The prioritized behavioral indicators of compromise justify the execution of the "ransomware" because the scores are low and indicate the likelihood that malicious ransomware has been detected.

Answer: C

QUESTION 45
The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

A. Determine the assets to which the attacker has access
B. Identify assets the attacker handled or acquired
C. Change access controls to high risk assets in the enterprise

D. Identify movement of the attacker in the enterprise

Answer: D

QUESTION 46
A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

A. incident response playbooks
B. asset vulnerability assessment
C. report of staff members with asset relations
D. key assets and executives
E. malware analysis report

Answer: BE
Explanation:
https://cloudogre.com/risk-assessment/

QUESTION 47
Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

A. exploitation
B. actions on objectives
C. delivery
D. reconnaissance

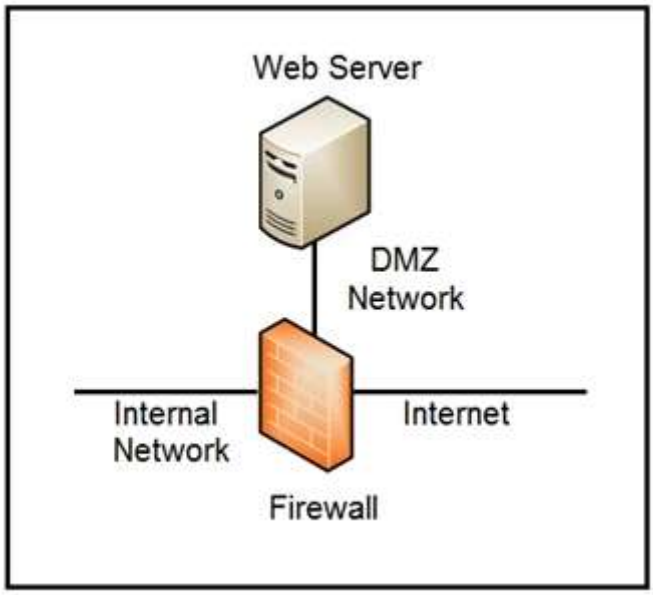
Answer: C
Explanation:
https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf

QUESTION 48
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic
B. Tapping interrogations detect and block malicious traffic
C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

QUESTION 49
Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)



A. Create an ACL on the firewall to allow only TLS 1.3
B. Implement a proxy server in the DMZ network
C. Create an ACL on the firewall to allow only external connections
D. Move the webserver to the internal network
E. Move the webserver to the external network

Answer: BD

QUESTION 50
According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

A. Perform a vulnerability assessment
B. Conduct a data protection impact assessment
C. Conduct penetration testing
D. Perform awareness testing

Answer: B
Explanation:
https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

QUESTION 51
A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

A. Classify the criticality of the information, research the attacker's motives, and identify missing patches
B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

Answer: B

QUESTION 52
A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets
B. Update software to patch third-party software
C. Validate CSRF by executing exploits within Metasploit
D. Fix applications according to the risk scores

Answer: D

QUESTION 53
An engineer is analyzing a possible compromise that happened a week ago when the company database servers unexpectedly went down. The analysis reveals that attackers tampered with Microsoft SQL Server Resolution Protocol and launched a DDoS attack. The engineer must act quickly to ensure that all systems are protected. Which two tools should be used to detect and mitigate this type of future attack? (Choose two.)

A. firewall
B. Wireshark
C. autopsy
D. SHA512
E. IPS

Answer: AB

QUESTION 54
A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

A. HIPAA
B. PCI-DSS
C. Sarbanes-Oxley
D. GDPR

Answer: D
Explanation:
https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/

QUESTION 55
An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates
B. Update the IDS/IPS signatures and reimage the affected hosts
C. Identify the systems that have been affected and tools used to detect the attack
D. Identify the traffic with data capture using Wireshark and review email filters

Answer: C

QUESTION 56
An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?

A. Investigate the vulnerability to prevent further spread

B. Acknowledge the vulnerabilities and document the risk
C. Apply vendor patches or available hot fixes
D. Isolate the assets affected in a separate network

Answer: D

QUESTION 57
A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs.
Which technology should be used to accomplish this task?

A. application whitelisting/blacklisting
B. network NGFW
C. host-based IDS
D. antivirus/antispyware software

Answer: A

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: B

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

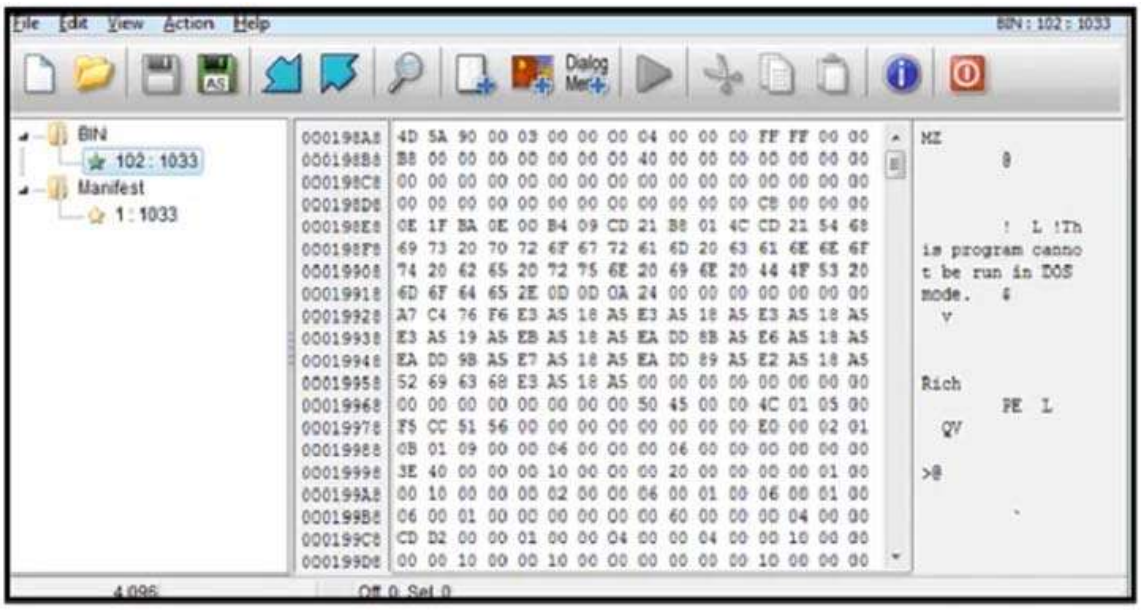
QUESTION 62
Refer to the exhibit. What results from this script?

```
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: D