Question 1:

```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]

[Classification: Web Application Attack] [Priority: 1]

04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80

TCP TTL:63 TOS:0x0 ID:20054 IpLen: 20 DgmLen:342 DF

***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32

[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts

B. XSS attack against the target webserver

C. brute-force attack against directories and files on the target webserver

D. SQL injection attack against the target webserver

Correct Answer: C

Question 2:
What is a concern for gathering forensics evidence in public cloud environments?

A. High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.

B. Configuration: Implementing security zones and proper network segmentation.

C. Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.

D. Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

Correct Answer: D

Reference:
https://www.researchgate.net/publication/307871954_About_Cloud_Forensics_Challenges_and_Solutions

---

Question 3:
Which scripts will search a log file for the IP address of 192.168.100.100 and create an output file named parsed_host.log while printing results to the console?

A.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "parsed_host.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

B.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_hosts.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "test_log.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

C.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.10\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "parsed_host.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

D.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "test_log.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

A. Option A

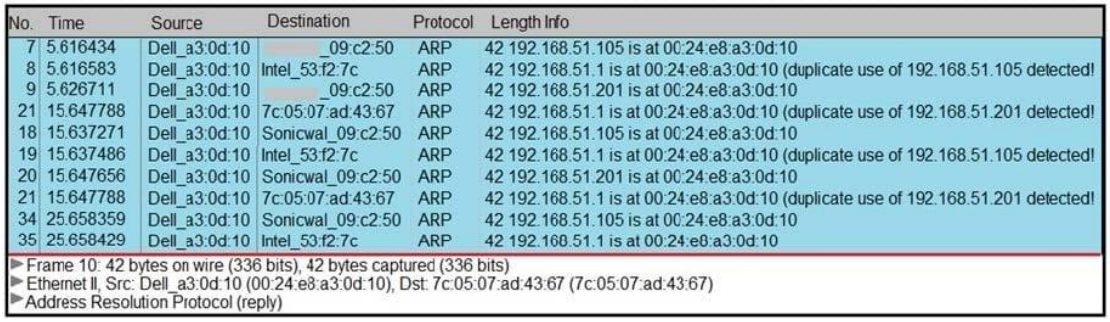
B. Option B

C. Option C

D. Option D

Correct Answer: A

Question 4:



No.	Time	Source	Destination	Protocol	Length Info
7	5.616434	Dell_a3:0d:10	_09:c2:50	ARP	42 192.168.51.105 is at 00:24:e8:a3:0d:10
8	5.616583	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
9	5.626711	Dell_a3:0d:10	_09:c2:50	ARP	42 192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
18	15.637271	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42 192.168.51.105 is at 00:24:e8:a3:0d:10
19	15.637486	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
20	15.647656	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42 192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
34	25.658359	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42 192.168.51.105 is at 00:24:e8:a3:0d:10
35	25.658429	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10

▶ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▶ Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: 7c:05:07:ad:43:67 (7c:05:07:ad:43:67)
▶ Address Resolution Protocol (reply)

Refer to the exhibit. A security analyst notices unusual connections while monitoring traffic. What is the attack vector, and which action should be taken to prevent this type of event?

A. DNS spoofing; encrypt communication protocols

B. SYN flooding, block malicious packets

C. ARP spoofing; configure port security

D. MAC flooding; assign static entries

Correct Answer: C

Question 5:

A website administrator has an output of an FTP session that runs nightly to download and unzip files to a local staging server. The download includes thousands of files, and the manual process used to find how many files failed to download is time-consuming. The administrator is working on a PowerShell script that will parse a log file and summarize how many files were successfully downloaded versus ones that failed. Which script will read the contents of the file one line at a time and return a collection of objects?

A. Get-Content-Folder \\Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"

B. Get-Content –ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked “ERROR”, “SUCCESS”

C. Get-Content –Directory \\Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result “ERROR”, “SUCCESS”

D. Get-Content –Path \\Server\FTPFolder\Logfiles\ftpfiles.log | Select-String “ERROR”, “SUCCESS”

Correct Answer: D

Question 6:

```
<stix:Indicator id= "CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04-
08T00:44:39.970278+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89">
<cybox:Object id= "CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals" >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamp= "2020-04-
08T00:44:39.970417+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox:Object id= "CISA:Object-7728bd69-e724-4917-9550-9ae853becf28">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf" timestamp= "2020-04-
08T00:44:39.970554+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254">
<cybox:Object id= "CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
```

Refer to the exhibit. Which two actions should be taken based on the intelligence information? (Choose two.)

A. Block network access to all .shop domains

B. Add a SIEM rule to alert on connections to identified domains.

C. Use the DNS server to block hole all .shop requests.

D. Block network access to identified domains.

E. Route traffic from identified domains to block hole.

Correct Answer: BD

Question 7:
A security team receives reports of multiple files causing suspicious activity on users\' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

A. Inspect registry entries

B. Inspect processes.

C. Inspect file hash.

D. Inspect file type.

E. Inspect PE header.

Correct Answer: BC

Reference:
https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

---

Question 8:

```
<indicator:Observable id= "example:Observable-9c9869a2-f822-4682-bda4-e89d31b18704">
        <cybox:Object id= "example:EmailMessage-9d56af8e-5588-4ed3-affd-bd769ddd7fe2">
          <cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
            <EmailMessageObj:Attachments>
                <EmailMessageObj:File object_reference= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"/>
            </EmailMessageObj:Attachments>
      </cybox:Properties>
      <cybox:Related_Objects>
        <cybox:Related_Object id= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"
          <cybox:Properties xsi:type= "FileObj:FileObjectType">
                <FileObj:File_Name condition= "StartsWith">Final Report</FileObj:File_Name>
                <FileObj:File_Extension condition= "Equals">doc.exe</FileObj:File_Extension>
          </cybox:Properties>
        <cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelationshipVocab-1.1">Contains</cybox:Relationship>
      </cybox:Related_Object>
    </cybox:Related_Objects>
  </cybox:Object>
</indicator:Observable>
```

Refer to the exhibit. Which determination should be made by a security analyst?

A. An email was sent with an attachment named "Grades.doc.exe".

B. An email was sent with an attachment named "Grades.doc".

C. An email was sent with an attachment named "Final Report.doc".

D. An email was sent with an attachment named "Final Report.doc.exe".

Correct Answer: D

Question 9:

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 10:

```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= 'cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
1.0">Contains</cybox:Relationship>
 </cybox:Related_Object>|
 </cybox:Related_Objects>
 </cybox:Object>
 </indicator:Observable>
```

Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

B. Block all emails sent from an @state.gov address.

C. Block all emails with pdf attachments.

D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB

Question 11:
An attacker embedded a macro within a word processing file opened by a user in an organization\'s legal department. The attacker used this technique to gain access to confidential financial data. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)

A. controlled folder access

B. removable device restrictions

C. signed macro requirements

D. firewall rules creation

E. network access control

Correct Answer: AC

Question 12:

Refer to the exhibit. Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

A. The attacker used r57 exploit to elevate their privilege.

B. The attacker uploaded the word press file manager trojan.

C. The attacker performed a brute force attack against word press and used sql injection against the backend database.

D. The attacker used the word press file manager plugin to upoad r57.php.

E. The attacker logged on normally to word press admin page.

Correct Answer: CD

Question 13:
What are YARA rules based upon?

A. binary patterns

B. HTML code

C. network artifacts

D. IP addresses

Correct Answer: A

Reference:
https://en.wikipedia.org/wiki/YARA#:~:text=YARA%20is%20the%20name%20of,strings%20and%20a%20boolean%20expression.

Question 14:
An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

A. Upload the file signature to threat intelligence tools to determine if the file is malicious.

B. Monitor processes as this a standard behavior of Word macro embedded documents.

C. Contain the threat for further analysis as this is an indication of suspicious activity.

D. Investigate the sender of the email and communicate with the employee to determine the motives.

Correct Answer: A

Question 15:


service

June 3, 2020 at 5:33 PM

Credit Card Refund #186913

To: [removed]

Received: from ([202.142.155.218]) by [removed] for [removed]; Wed, 03 Jub 2020 15:33:03 +0000 (UTC)

Received: from [53.183.109.56] (helo=WEEOWED.lu) by with esmtpa (Exim 4.85) (envelope-from) id 08A56E158516 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Received: from [54.198.90.184] (account cobblergs8@o4.e.notification.intuit.com HELO RUFINEF.GYPUBOT.mcg) by (Postfix) with ESMTPA id mXDmHhpAEoD7.233 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Content-Type: multipart/mixed; boundary="- -_Part_6483125_09335162.9435849616646"

1

Cash Refund

Date	**6/03/2020**
Refund #	**186913**
Payment Method	**Website Payment**
Check #	**3000679700**
Project	
Department	
Phone Number	
Shipping Method	**UPS 2nd Day Air®**
Credit Card #	**********
Transaction Next Approver	

Item	Quantity	Description	Options	Rate	Amount	Gross Amt	Tax Amount	Tax Details	Reference
3795326-44	1	2020		1,397.11	1,397.11	1,397.11			97810761_1
				Subtotal	1,397.11				
				Shipping Cost (UPS 2nd Day Air®)	0.00				
				Total	$1,397.11				

********CREDIT WILL BE ISSUED TO YOUR CREDIT CARD USED FOR ORIGINAL PURCHASE********

Card_Refund_186913.xlsm

Refer to the exhibit. Which element in this email is an indicator of attack?

A. IP Address: 202.142.155.218

B. content-Type: multipart/mixed

C. attachment: "Card-Refund"

D. subject: "Service Credit Card"

Correct Answer: C