Chapter

4

Operations and Incident Response

THE COMPTIA SECURITY+ EXAM SY0-601 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **4.1 Given a scenario, use the appropriate tool to assess organizational security**
- ✓ **4.2 Summarize the importance of policies, processes, and procedures for incident response**
- ✓ **4.3 Given an incident, utilize appropriate data sources to support an investigation**
- ✓ **4.4 Given an incident, apply mitigation techniques or controls to secure an environment**
- ✓ **4.5 Explain the key aspects of digital forensics**

1. Mila wants to generate a unique digital fingerprint for a file, and needs to choose between a checksum and a hash. Which option should she choose and why should she choose it?
   - **A.** A hash, because it is unique to the file
   - **B.** A checksum, because it verifies the contents of the file
   - **C.** A hash, because it can be reversed to validate the file
   - **D.** A checksum, because it is less prone to collisions than a hash

2. Which of the following would prevent a user from installing a program on a company-owned mobile device?
   - **A.** An allow list
   - **B.** A deny list
   - **C.** ACL
   - **D.** HIDS

3. Liam is responsible for monitoring security events in his company. He wants to see how diverse events may connect using his security information and event management (SIEM). He is interested in identifying different indicators of compromise that may point to the same breach. Which of the following would be most helpful for him to implement?
   - **A.** NIDS
   - **B.** PKI
   - **C.** A correlation dashboard
   - **D.** A trend dashboard

4. Emily wants to capture HTTPS packets using `tcpdump`. If the service is running on its default port and her Ethernet adapter is `eth0`, which `tcpdump` command should she use?
   - **A.** `tcpdump eth0 -proto https`
   - **B.** `tcpdump -i eth0 -proto https`
   - **C.** `tcpdump tcp https eth0`
   - **D.** `tcpdump -i eth0 tcp port 443`

5. Mila gives her team a scenario, and then asks them questions about how they would respond, what issues they expect they might encounter, and how they would handle those issues. What type of exercise has she conducted?
   - **A.** A tabletop exercise
   - **B.** A walk-through
   - **C.** A simulation
   - **D.** A drill

6. Murali is preparing to acquire data from various devices and systems that are targets in a forensic investigation. Which of the following devices is the least volatile according to the order of volatility?
   - **A.** Backups
   - **B.** CPU cache

C. Local disk

D. RAM

7. Henry has been asked for vulnerability scan results by an incident responder. He is curious to know why the responder needs scan results. What answer would you provide to him to explain why scan results are needed and are useful?

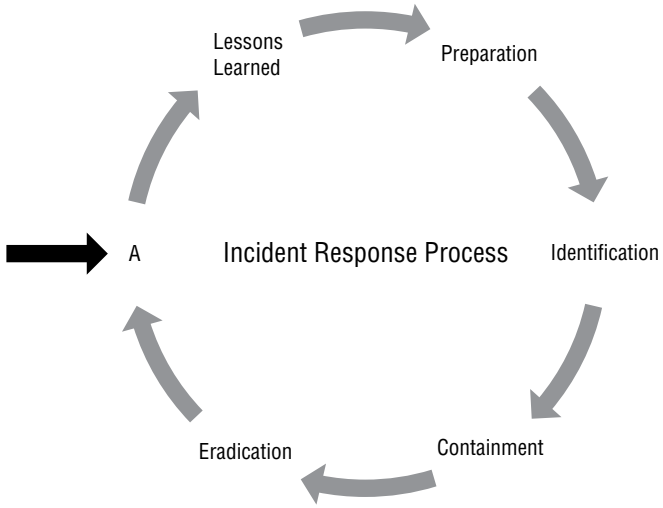
A. The scans will show the programs the attackers used.

B. The scans will show the versions of software installed before the attack.

C. Vulnerable services will provide clues about what the attackers may have targeted.

D. The scans will show where firewalls and other network devices were in place to help with incident analysis.

8. What phase of the incident response process should be placed at point A in the following image?



A. Simulations

B. Review

C. Recovery

D. Patching

9. Nick is reviewing commands run on a Windows 10 system and discovers that the `route` command was run with the `-p` flag. What occurred?

A. Routes were discovered using a `ping` command.

B. The route's path will be displayed.

C. A route was added that will persist between boots.

D. A route was added that will use the path listed in the command.

10. Lucca wants to acquire open source intelligence information using an automated tool that can leverage search engines and tools like Shodan. Which of the following tools should he select?
    A. `curl`
    B. `hping`
    C. `netcat`
    D. `theHarvester`

11. Brent wants to use a tool to help him analyze malware and attacks and wants to cover a broad range of tactics and tools that are used by adversaries. Which of the following is broadly implemented in technical tools and covers techniques and tactics without requiring a specific order of operations?
    A. The Diamond Model of Intrusion Analysis
    B. The Cyber Kill Chain
    C. The MITRE ATT&CK framework
    D. The CVSS standard

12. Ted needs to preserve a server for forensic purposes. Which of the following should he not do?
    A. Turn the system off to ensure that data does not change.
    B. Remove the drive while the system is running to ensure that data does not change.
    C. Leave the machine connected to the network so that users can continue to use it.
    D. All of the above

13. What mitigation technique is used to limit the ability of an attack to continue while keeping systems and services online?
    A. Segmentation
    B. Isolation
    C. Nuking
    D. Containment

14. Jessica wants to review the network traffic that her Windows system has sent to determine if a file containing sensitive data was uploaded from the system. What Windows log file can she use to find this information?
    A. The application log
    B. The network log
    C. The security log
    D. None of the above

15. What term is used to describe the documentation trail for control, analysis, transfer, and final disposition of evidence for digital forensic work?
    A. Evidence log
    B. Paper trail

C. Chain of custody

D. Digital footprint

16. Henry wants to determine what services are on a network that he is assessing. Which of the following tools will provide him with a list of services, ports, and their status?

A. `nmap`

B. `route`

C. `hping`

D. `netstat`

17. Nathan needs to know how many times an event occurred and wants to check a log file for that event. Which of the following `grep` commands will tell him how many times the event happened if each occurrence is logged independently in the `logfile.txt` log file, and uses a unique event ID: `event101`?

A. `grep logfile.txt -n 'event101'`

B. `grep -c 'event101' logfile.txt`

C. `grep logfile.txt -c 'event101'`

D. `grep -c event101 -i logfile.txt`

18. Jacob wants to ensure that all of the areas that are impacted by an incident are addressed by his incident response team. What term is used to describe the relationship and communications process that teams use to ensure that all of those involved are treated appropriately?

A. COOP

B. Stakeholder management

C. PAM

D. Communications planning

19. While Susan is conducting a forensic review of logs from two servers hosted in the same datacenter, she notices that log items on the first server occurred exactly an hour before matching events on the second server. What is the most likely cause of such exact occurrences?

A. The attack took an hour to complete, providing the attacker with access to the second machine an hour later.

B. The log entries are incorrect, causing the events to appear at the wrong time.

C. The attacker used a script causing events to happen exactly an hour apart.

D. A time offset is causing the events to appear to occur at different times.

20. What is the primary usage of Domain Name System (DNS) data in incident investigations and operational security monitoring?

A. DNS data is used to capture network scans.

B. DNS data can be used to identify domain transfer attacks.

C. DNS log information can be used to identify malware going to known malicious sites.

D. DNS log information can be used to identify unauthorized logins.

21. Dani generates an OpenSSL certificate using the following command. What has she set with the flag `-rsa:2048`?

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048
-keyout privateKey.key -out mycert.crt
```

A. The year that the certificate will expire
B. The key length in bytes
C. The year that the root certificate will expire
D. The key length in bits

22. Theresa wants to view the last 10 lines of a log file and to see it change as modifications are made. What command should she run on the Linux system she is logged in to?

A. `head -f -end 10 logfile.log`
B. `tail -f logfile.log`
C. `foot -watch -l 10 logfile.log`
D. `follow -tail 10 logfile.log`

23. Henry wants to acquire the firmware from a running system. What is the most likely technique that he will need to use to acquire the firmware?

A. Connect using a serial cable.
B. Acquire the firmware from memory using memory forensics tools.
C. Acquire the firmware from disk using disk forensic tools.
D. None of the above

24. Eric wants to determine how much bandwidth was used during a compromise and where the traffic was directed to. What technology can he implement before the event to help him see this detail and allow him to have an effective bandwidth monitoring solution?

A. A firewall
B. NetFlow
C. packetflow
D. A DLP

25. Naomi has acquired an image of a drive as part of a forensic process. She wants to ensure that the drive image matches the original. What should she create and record to validate this?

A. A third image to compare to the original and new image
B. A directory listing to show that the directories match
C. A photographic image of the two drives to show that they match
D. A hash of the drives to show that their hashes match

26. Ryan has been asked to run Nessus on his network. What type of tool has he been asked to run?

A. A fuzzer
B. A vulnerability scanner

C. A WAF

D. A protocol analyzer

27. Jason wants to ensure that the digital evidence he is collecting during his forensic investigation is admissible. Which of the following is a common requirement for admissibility of evidence?

A. It must be relevant.

B. It must be hearsay.

C. It must be timely.

D. It must be public.

28. Which of the following key elements is not typically included in the design of a communication plan?

A. Incident severity

B. Customer impact

C. Employee impact

D. Cost to the organization

29. Rick runs the following command:

```
cat file1.txt file2.txt
```

What will occur?

A. The contents of `file1.txt` will be appended to `file2.txt`.

B. The contents of `file1.txt` will be displayed, and then the contents of `file2` will be displayed.

C. The contents of `file2.txt` will be appended to `file1.txt`.

D. The contents of both files will be combined line by line.

30. Michelle wants to check for authentication failures on a CentOS Linux–based system. Where should she look for these event logs?

A. `/var/log/auth.log`

B. `/var/log/fail`

C. `/var/log/events`

D. `/var/log/secure`

31. A web page's title is considered what type of information about the page?

A. Summary

B. Metadata

C. Header data

D. Hidden data

32. Nelson has discovered malware on one of the systems he is responsible for and wants to test it in a safe environment. Which of the following tools is best suited to that testing?

A. `strings`

B. `scanless`

C. `Cuckoo`

D. Sn1per

33. Lucca wants to view metadata for a file so that he can determine the author of the file. What tool should he use from the following list?

A. Autopsy

B. `strings`

C. `exiftool`

D. `grep`

34. Isaac wants to acquire an image of a system that includes the operating system. What tool can he use on a Windows system that can also capture live memory?

A. `dd`

B. FTK Imager

C. Autopsy

D. WinDump

35. Jason is conducting a forensic investigation and has retrieved artifacts in addition to drives and files. What should he do to document the artifacts he has acquired?

A. Image them using `dd` and ensure that a valid MD5sum is generated.

B. Take a picture of them, label them, and add them to the chain of custody documentation.

C. Contact law enforcement to properly handle the artifacts.

D. Engage legal counsel to advise him how to handle artifacts in an investigation.

36. Gary wants to check for the mail servers for `example.com`. What tool and command can he use to determine this?

A. `nslookup -query =mx example.com`

B. `ping -email example.com`

C. `smtp -mx example.com`

D. `email -lookup -mx example.com`

37. Which of the following is best suited to analyzing live SIP traffic?

A. Log files

B. Wireshark

C. Nessus

D. SIPper

38. Andrea wants to identify services on a remote machine and wants the services to be labeled with service names and other common details. Which of the following tools will not provide that information?

A. `netcat`

B. Sn1per

C. Nessus

D. `nmap`

39. Joseph is writing a forensic report and wants to be sure he includes appropriate detail. Which of the following would not typically be included while discussing analysis of a system?

A. Validation of the system clock's time settings

B. The operating system in use

C. The methods used to create the image

D. A picture of the person from whom the system was taken

40. Greg believes an attacker has been using a brute-force password attack against a Linux system he is responsible for. What command could he use to determine if this is the case?

A. `grep "Failed password" /var/log/auth.log`

B. `tail /etc/bruteforce.log`

C. `head /etc/bruteforce.log`

D. `grep "Failed login" /etc/log/auth.log`

41. Elaine wants to determine what websites a user has recently visited using the contents of a forensically acquired hard drive. Which of the following locations would not be useful for her investigation?

A. The browser cache

B. The browser history

C. The browser's bookmarks

D. Session data

42. Jason wants to acquire network forensic data. What tool should he use to gather this information?

A. `nmap`

B. Nessus

C. Wireshark

D. SNMP

43. Ananth has been told that attackers sometimes use `ping` to map networks. What information returned by `ping` could be most effectively used to determine network topology?

A. TTL

B. Packets sent

C. Packets received

D. Transit time

44. Susan has discovered evidence of a compromise that occurred approximately five months ago. She wants to conduct an incident investigation but is concerned about whether the data will exist. What policy guides how long logs and other data are kept in most organizations?

A. The organization's data classification policy

B. The organization's backup policy

C. The organization's retention policy

D. The organization's legal hold policy

45. Selah executes the following command on a system. What has she accomplished?

```
dd if=/dev/zero of=/dev/sda bs=4096
```

A. Copying the disk `/dev/zero` to the disk `/dev/sda`

B. Formatting `/dev/sda`

C. Writing zeroes to all of `/dev/sda`

D. Cloning `/dev/sda1`

46. Jim is preparing a presentation about his organization's incident response process and wants to explain why communications with involved groups and individuals across the organization are important. Which of the following is the primary reason that organizations communicate with and involve staff from affected areas throughout the organization in incident response efforts?

A. Legal compliance

B. Retention policies

C. Stakeholder management

D. A COOP

47. Elle is conducting an exercise for her organization and wants to run an exercise that is as close to an actual event as possible. What type of event should she run to help her organization get this type of real-world practice?

A. A simulation

B. A tabletop exercise

C. A walk-through

D. A wargame

48. Erin wants to determine what devices are on a network but cannot use a port scanner or vulnerability scanner. Which of the following techniques will provide the most data about the systems that are active on the network?

A. Run Wireshark in promiscuous mode.

B. Query DNS for all A records in the domain.

C. Review the CAM tables for all the switches in the network.

D. Run `netstat` on a local workstation.

49. What SIEM component collects data and sends it to the SIEM for analysis?

A. An alert level

B. A trend analyzer

C. A sensor

D. A sensitivity threshold

50. Alaina sets her antimalware solution to move infected files to a safe storage location without removing them from the system. What type of setting has she enabled?

A. Purge

B. Deep-freeze

C. Quarantine

D. Retention

51. A senior vice president in the organization that Chuck works in recently lost a phone that contained sensitive business plans and information about suppliers, designs, and other important materials. After interviewing the vice president, Chuck finds out that the phone did not have a passcode set and was not encrypted, and that it could not be remotely wiped. What type of control should Chuck recommend for his company to help prevent future issues like this?

A. Use containment techniques on the impacted phones.

B. Deploy a DLP system.

C. Deploy an MDM system.

D. Isolate the impacted phones.

52. The school that Gabby works for wants to prevent students from browsing websites that are not related to school work. What type of solution is best suited to help prevent this?

A. A content filter

B. A DLP

C. A firewall

D. An IDS

53. Frank knows that forensic information he is interested in is stored on a system's hard drive. If he wants to follow the order of volatility, which of the following items should be forensically captured after the hard drive?

A. Caches and registers

B. Backups

C. Virtual memory

D. RAM

54. Greg runs the following command. What occurs?

```
chmod -R 755 /home/greg/files
```

A. All of the files in `/home/greg/` are set to allow the group to read, write, and execute them, and Greg and the world can only read them.

B. The read, write, and execute permissions will be removed from all files in the `/home/greg/files` directory.

C. All of the files in `/home/greg/files` are set to allow Greg to read, write, and execute them, and the group and the world can only read them.

D. A new directory will be created with read, write, and execute permissions for the world and read-only permissions for Greg and the group he is in.

55. Charles wants to ensure that the forensic work that he is doing cannot be repudiated. How can he validate his attestations and documentation to ensure nonrepudiation?

A. Encrypt all forensic output.

B. Digitally sign the records.

C. Create a MD5 checksum of all images.

D. All of the above

56. Diana wants to capture the contents of physical memory using a command-line tool on a Linux system. Which of the following tools can accomplish this task?

A. `ramdump`

B. `system -dump`

C. `memcpy`

D. `memdump`

57. Valerie wants to capture the pagefile from a Windows system. Where can she find the file for acquisition?

A. `C:\Windows\swap`

B. `C:\pagefile.sys`

C. `C:\Windows\users\swap.sys`

D. `C:\swap\pagefile.sys`

58. Megan needs to conduct a forensic investigation of a virtual machine (VM) hosted in a VMware environment as part of an incident response effort. What is the best way for her to collect the VM?

A. As a snapshot using the VMware built-in tools

B. By using `dd` to an external drive

C. By using `dd` to an internal drive

D. By using a forensic imaging device after removing the server's drives

59. What forensic concept is key to establishing provenance for a forensic artifact?

A. Right to audit

B. Preservation

C. Chain of custody

D. Timelines

60. What role do digital forensics most often play in counterintelligence efforts?

A. They are used to determine what information was stolen by spies.

B. They are used to analyze tools and techniques used by intelligence agencies.

C. They are required for training purposes for intelligence agents.

D. They do not play a role in counterintelligence.

61. Which of the following groups is not typically part of an incident response team?

A. Law enforcement

B. Security analysts

C. Management

D. Communications staff

62. Bob needs to block Secure Shell (SSH) traffic between two security zones. Which of the following Linux `iptables` firewall rules will block that traffic from the 10.0.10.0/24 network to the system the rule is running on?

A. `iptables -A INPUT -p tcp --dport 22 -i eth0 -s 10.0.10.0/24 -j DROP`

B. `iptables -D OUTPUT -p udp -dport 21 -i eth0 -s 10.0.10.255 -j DROP`

C. `iptables -A OUTPUT -p udp --dport 22 -i eth0 -s 10.0.10.255 -j BLOCK`

D. `iptables -D INPUT -p udp --dport 21 -I eth0 -s 10.0.10.0/24 -j DROP`

63. Maria wants to add entries into the Linux system log so that they will be sent to her security information and event management (SIEM) device when specific scripted events occur. What Linux tool can she use to do this?

A. `cat`

B. `slogd`

C. `logger`

D. `tail`

64. Amanda's organization does not currently have an incident response plan. Which of the following reasons is not one she should present to management in support of creating one?

A. It will prevent incidents from occurring.

B. It will help responders react appropriately under stress.

C. It will prepare the organization for incidents.

D. It may be required for legal or compliance reasons.

65. Which of the following scenarios is least likely to result in data recovery being possible?

A. A file is deleted from a disk.

B. A file is overwritten by a smaller file.

C. A hard drive is quick-formatted.

D. A disk is degaussed.

66. Henry records a video of the removal of a drive from a system as he is preparing for a forensic investigation. What is the most likely reason for Henry to record the video?

A. To meet the order of volatility

B. To establish guilt beyond a reasonable doubt

C. To ensure data preservation

D. To document the chain of custody and provenance of the drive

67. Adam wants to use a tool to edit the contents of a drive. Which of the following tools is best suited to that purpose?

A. Autopsy

B. WinHex

C. `dd`

D. FTK Imager

68. Jill wants to build a checklist that includes all the steps to respond to a specific incident. What type of artifact should she create to do so in her security orchestration, automation, and response (SOAR) environment?

A. A BC plan

B. A playbook

C. A DR plan

D. A runbook

69. Alaina wants to use a password cracker against hashed passwords. Which of the following items is most important for her to know before she does this?

A. The length of the passwords

B. The last date the passwords were changed

C. The hashing method used for the passwords

D. The encryption method used for the passwords

70. Vincent wants to ensure that his staff does not install a popular game on the workstations they are issued. What type of control could he deploy as part of his endpoint security solution that would most effectively stop this?

A. An application approved list

B. A DLP

C. A content filter

D. An application block list

71. Charlene wants to set up a tool that can allow her to see all the systems a given IP address connects to and how much data is sent to that IP by port and protocol. Which of the following tools is not suited to meet that need?

A. IPFIX

B. IPSec

C. sFlow

D. NetFlow

72. A system that Sam is responsible for crashed, and Sam suspects malware may have caused an issue that led to the crash. Which of the following files is most likely to contain information if the malware was a file-less, memory-resident malware package?

A. The swapfile

B. The Windows system log

C. A dump file

D. The Windows security log

73. Which of the following commands can be used to show the route to a remote system on a Windows 10 workstation?

A. `traceroute`

B. `arp`

C. `tracert`

D. `netstat`

74. Tools like PRTG and Cacti that monitor SNMP information are used to provide what type of information for an incident investigation?

A. Authentication logs

B. Bandwidth monitoring

C. System log information

D. Email metadata

75. Which of the following is not a key consideration when considering on-premises versus cloud forensic investigations?

A. Data breach notification laws

B. Right-to-audit clauses

C. Regulatory requirements

D. Provenance

76. The company Charles works for has recently had a stolen company cell phone result in a data breach. Charles wants to prevent future incidents of a similar nature. Which of the following mitigation techniques would be the most effective?

A. Enable FDE via MDM.

B. A firewall change

C. A DLP rule

D. A new URL filter rule

77. Henry runs the following command:

```
dig @8.8.8.8 example.com
```

What will it do?

A. Search `example.com`'s DNS server for the host `8.8.8.8`.

B. Search `8.8.8.8`'s DNS information for `example.com`.

C. Look up the hostname for `8.8.8.8`.

D. Perform open source intelligence gathering about `8.8.8.8` and `example.com`.

78. Greg is collecting a forensic image of a drive using FTK Imager, and he wants to ensure that he has a valid copy. What should he do next?

A. Run the Linux `cmp` command to compare the two files.

B. Calculate an AES-256 hash of the two drives.

C. Compare an MD5 or SHA-1 hash of the drive to the image.

D. Compare the MD5 of each file on the drive to the MD5 of each file in the image.

79. Adam needs to search for a string in a large text file. Which of the following tools should he use to most efficiently find every occurrence of the text he is searching for?

A. `cat`

B. `grep`

C. `head`

D. `tail`

80. Angela wants to use segmentation as part of her mitigation techniques. Which of the following best describes a segmentation approach to network security?

A. Removing potentially infected or compromised systems from the network

B. Using firewalls and other tools to limit the spread of an active infection

C. Partitioning the network into segments based on user and system roles and security requirements

D. Adding security systems or devices to prevent data loss and exposure'

81. Charlene has been asked to write a business continuity (BC) plan for her organization. Which of the following will a business continuity plan best handle?

A. How to respond during a person-made disaster

B. How to keep the organization running during a system outage

C. How to respond during a natural disaster

D. All of the above

82. Brad wants to create a self-signed x.509 certificate. Which of the following tools can be used to perform this task?

A. `hping`

B. Apache

C. OpenSSL

D. `scp`

83. Cameron wants to test for commonly used passwords in his organization. Which of the following commands would be most useful if he knows that his organization's name, mascot, and similar terms are often used as passwords?

A. `john --wordlist "mywords.txt" --passwordfile.txt`

B. `ssh -test -"mascotname, orgname"`

C. `john -show passwordfile.txt`

D. `crack -passwords -wordlist "mascotname, orgname"`

84. Which of the following capabilities is not built into Autopsy?

A. Disk imaging

B. Timeline generation

C. Automatic image filtering

D. Communication visualization

85. Alaina's company is considering signing a contract with a cloud service provider, and wants to determine how secure their services are. Which of the following is a method she is likely to be able to use to assess it?

A. Ask for permission to vulnerability scan the vendor's production service.

B. Conduct an audit of the organization.

C. Review an existing SOC audit.

D. Hire a third party to audit the organization.

86. Erin is working through the Cyber Kill Chain and has completed the exploitation phase as part of a penetration test. What step would come next?

A. Lateral movement

B. Privilege escalation

C. Obfuscation

D. Exfiltration

87. Dana wants to use an exploitation framework to perform a realistic penetration test of her organization. Which of the following tools would fit that requirement?

A. Cuckoo

B. theHarvester

C. Nessus

D. Metasploit

88. Cynthia has been asked to build a playbook for the SOAR system that her organization uses. What will she build?

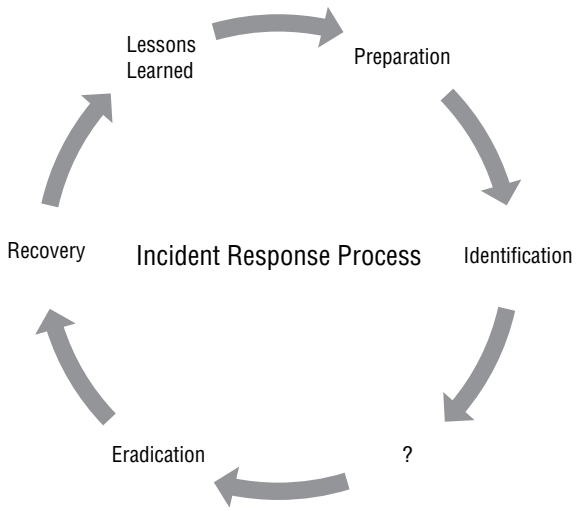
A. A set of rules with actions that will be performed when an event occurs using data collected or provided to the SOAR system

B. An automated incident response process that will be run to support the incident response (IR) team

C. A trend analysis–driven script that will provide instructions to the IR team

D. A set of actions that the team will perform to use the SOAR to respond to an incident

89. What incident response step is missing in the following image?



A. Business continuity

B. Containment

C. Response

D. Discovery

90. Gurvinder's corporate datacenter is located in an area that FEMA has identified as being part of a 100-year flood plain. He knows that there is a chance in any given year that his datacenter could be completely flooded and underwater, and he wants to ensure that his organization knows what to do if that happens. What type of plan should he write?

A. A Continuity of Operations Plan

B. A business continuity plan

C. A flood insurance plan

D. A disaster recovery plan

91. Frank wants to identify where network latency is occurring between his computer and a remote server. Which of the following tools is best suited to identifying both the route used and which systems are responding in a timely manner?

A. `ping`

B. `tracert`

C. `pathping`

D. `netcat`

92. Derek wants to see what DNS information can be queried for his organization as well as what hostnames and subdomains may exist. Which of the following tools can provide both DNS query information and Google search information about hosts and domains through a single tool?

A. `dnsenum`

B. `dig`

C. `host`

D. `dnscat`

93. Jill has been asked to perform data recovery due to her forensic skills. What should she tell the person asking to perform data recovery to give her the best chance of restoring lost files that were accidentally deleted?

A. Immediately reboot using the reset switch to create a lost file memory dump.

B. Turn off "secure delete" so that the files can be more easily recovered.

C. Do not save any files or make any changes to the system.

D. All of the above

94. What phase follows lateral movement in the Cyber Kill Chain?

A. Exfiltration

B. Exploitation

C. Anti-forensics

D. Privilege escalation

95. Veronica has completed the recovery phase of her organization's incident response plan. What phase should she move into next?

A. Preparation

B. Lessons learned

C. Recovery

D. Documentation

96. Michelle has been asked to sanitize a number of drives to ensure that sensitive data is not exposed when systems are removed from service. Which of the following is not a valid means of sanitizing hard drives?

A. Physical destruction

B. Degaussing

C. Quick-formatting the drives

D. Zero-wiping the drives

97. Bart is investigating an incident, and needs to identify the creator of a Microsoft Office document. Where would he find that type of information?

A. In the filename

B. In the Microsoft Office log files

C. In the Windows application log

D. In the file metadata

98. Nathaniel wants to allow Chrome through the Windows Defender firewall. What type of firewall rule change will he need to permit this?

A. Allow TCP 80 and 443 traffic from the system to the Internet.

B. Add Chrome to the Windows Defender Firewall allowed applications.

C. Allow TCP 80 and 443 traffic from the Internet to the system.

D. All of the above

99. Nathan wants to perform whois queries on all the hosts in a class C network. Which of the following tools can do that and also be used to discover noncontiguous IP blocks in an automated fashion?

A. `netcat`

B. `dnsenum`

C. `dig`

D. `nslookup`

100. What key forensic tool relies on correctly set system clocks to work properly?

A. Disk hashing

B. Timelining

C. Forensic disk acquisition

D. File metadata analysis

101. Valerie is writing her organization's forensic playbooks and knows that the state that she operates in has a data breach notification law. Which of the following key items is most likely to be influenced by that law?

A. Whether Valerie calls the police for forensic investigation help

B. The maximum amount of time until she has to notify customers of sensitive data breaches

C. The certification types and levels that her staff have to maintain

D. The maximum number of residents that she can notify about a breach

102. As part of a breach response, Naomi discovers that Social Security numbers (SSNs) were sent in a spreadsheet via email by an attacker who gained control of a workstation at her company's headquarters. Naomi wants to ensure that more SSNs are not sent from her environment. What type of mitigation technique is most likely to prevent this while allowing operations to continue in as normal a manner as possible?

A. Antimalware installed at the email gateway

B. A firewall that blocks all outbound email

C. A DLP rule blocking SSNs in email

D. An IDS rule blocking SSNs in email

103. Troy wants to review metadata about an email he has received to determine what system or server the email was sent from. Where can he find this information?

A. In the email message's footer

B. In the to: field

C. In the email message's headers

D. In the from: field

104. Henry is working with local police on a forensic case and discovers that he needs data from a service provider in another state. What issue is likely to limit their ability to acquire data from the service provider?

A. Jurisdiction

B. Venue

C. Legislation

D. Breach laws

105. Olivia wants to test the strength of passwords on systems in her network. Which of the following tools is best suited to that task?

A. John the Ripper

B. Rainbow tables

C. Crack.it

D. TheHunter

106. What U.S. federal agency is in charge of COOP?

A. The USDA

B. FEMA

C. The NSA

D. The FBI

107. Elaine wants to write a series of scripts to gather security configuration information from Windows 10 workstations. What tool should she use to perform this task?

A. Bash

B. PowerShell

C. Python

D. SSH

108. As part of his incident response, Ramon wants to determine what was said on a Voice over IP (VoIP) call. Which of the following data sources will provide him with the audio from the call?

A. Call manager logs

B. SIP logs

C. A Wireshark capture of traffic from the phone

D. None of the above

109. Isabelle wants to gather information about what systems a host is connecting to, how much traffic is sent, and similar details. Which of the following options would not allow her to perform that task?

A. IPFIX

B. NetFlow

C. NXLog

D. sFlow

110. As part of an incident response process, Pete puts a compromised system onto a virtual LAN (VLAN) that he creates that only houses that system and does not allow it access to the Internet. What mitigation technique has he used?

A. Isolation

B. Containment

C. Segmentation

D. Eradication

111. Lucca needs to conduct a forensic examination of a live virtual machine (VM). What forensic artifact should he acquire?

A. An image of live memory using FTK Imager from the VM

B. A `dd` image of the virtual machine disk image

C. A snapshot of the VM using the underlying virtualization environment

D. All of the above

112. James has a PCAP file that he saved while conducting an incident response exercise. He wants to determine if his intrusion prevention system (IPS) could detect the attack after configuring new detection rules. What tool will help him use the PCAP file for his testing?

A. `hping`

B. `tcpreplay`

C. `tcpdump`

D. Cuckoo

113. What type of file is created when Windows experiences a blue screen of death?

A. A security log

B. A blue log

C. A dump file

D. A tcpdump

114. Ed wants to ensure that a compromise on his network does not spread to parts of the network with different security levels. What mitigation technique should he use prior to the attack to help with this?

A. Isolation

B. Fragmentation

C. Tiering

D. Segmentation

115. Derek has acquired over 20 hard drives as part of a forensic investigation. What key process is important to ensure that each drive is tracked and managed properly over time?

A. Tagging the drives

B. Taking pictures of each drive

C. Labeling each drive with its order of volatility

D. Interviewing each person whose drive is imaged

116. What term describes the ownership, custody, and acquisition of digital forensic artifacts and images?

A. E-discovery

B. Provenance

C. Jurisdiction

D. Volatility

117. Elle wants to acquire the live memory (RAM) from a machine that is currently turned on. Which of the following tools is best suited to acquiring the contents of the system's memory?

A. Autopsy

B. The Volatility framework

C. `dd`

D. `netcat`

118. Randy believes that a misconfigured firewall is blocking traffic sent from some systems in his network to his web server. He knows that the traffic should be coming in as HTTPS to his web server, and he wants to check to make sure the traffic is received. What tool can he use to test his theory?

A. `tracert`

B. Sn1per

C. `traceroute`

D. Wireshark

119. Ryan wants to implement a flexible and reliable remote logging environment for his Linux systems. Which of the following tools is least suited to that requirement?

A. rsyslog

B. syslog

C. NXLog

D. syslog-ng

120. Susan has been reading about a newly discovered exploit, and wants to test her IPS rules to see if the sample code will work. In order to use the exploit, she needs to send a specifically crafted UDP packet to a DHCP server. What tool can she use to craft and send this test exploit to see if it is detected?

A. `hping`

B. `scanless`

C. `curl`

D. `pathping`

121. Valerie wants to check to see if a SQL injection attack occurred against her web application on a Linux system. Which log file should she check for this type of information?

A. The security log

B. The DNS log

C. The auth log

D. The web server log

122. Olivia's company has experienced a breach and believes that the attackers were able to access the company's web servers. There is evidence that the private keys for the certificates for the server were exposed and that the passphrases for the certificates were kept in the same directory. What action should Olivia take to handle this issue?

A. Revoke the certificates.

B. Change the certificate password.

C. Change the private key for the certificate.

D. Change the public key for the certificate.

123. Jean's company is preparing for litigation with another company that they believe has caused harm to Jean's organization. What type of legal action should Jean's lawyer take to ensure that the company preserves files and information related to the legal case?

A. A chain of custody demand letter

B. An e-discovery notice

C. A legal hold notice

D. An order of volatility

124. Cynthia wants to display all of the active connections on a Windows system. What command can she run to do so?

A. `route`

B. `netstat -a`

C. `netstat -c`

D. `hping`

125. What type of mitigation places a malicious file or application in a safe location for future review or study?

A. Containment

B. Quarantine

C. Isolation

D. Deletion

126. What location is commonly used for Linux swap space?

A. `\root\swap`

B. `\etc\swap`

C. `\proc\swap`

D. A separate partition

127. Marco is conducting a forensic investigation and is preparing to pull eight different storage devices from computers that he will analyze. What should he use to track the drives as he works with them?

A. Tags with system, serial number, and other information

B. MD5 checksums of the drives

C. Timestamps gathered from the drives

D. None of the above; the drives can be identified by the data they contain

128. Isaac executes the following command using `netcat`:

```
nc -v 10.11.10.1 1-1024
```

What has he done?

A. Opened a web page

B. Connected to a remote shell

C. Opened a local shell listener

D. Performed a port scan

129. Tony works for a large company with multiple sites. He has identified an incident in progress at one site that is connected to the organization's multisite intranet. Which of the following options is best suited to preserving the organization's function and protecting it from issues at that location?

A. Isolation

B. Containment

C. Segmentation

D. None of the above

130. Which of the following environments is least likely to allow a right-to-audit clause in a contract?

A. A datacenter co-location facility in your state

B. A rented facility for a corporate headquarters

C. A cloud server provider

D. A datacenter co-location facility in the same country but not the same state

131. Alaina's organization has been suffering from successful phishing attacks, and Alaina notices a new email that has arrived with a link to a phishing site. What response option from the following will be most likely to stop the phishing attack from succeeding against her users?

A. A WAF

B. A patch

C. An allow list

D. A URL filter

132. Ben writes down the checklist of steps that his organization will perform in the event of a cryptographic malware infection. What type of response document has he created?

A. A playbook

B. A DR plan

C. A BC plan

D. A runbook

133. Which of the following is not information that can be gathered from a system by running the `arp` command?

A. The IP address of the local system

B. The MAC addresses of recently resolved external hosts

C. Whether the IP address is dynamic or static

D. The MAC addresses of recently resolved local hosts

134. What log will `journalctl` provide Selah access to?

A. The event log

B. The auth log

C. The systemd journal

D. The authentication journal

135. What phase of the incident response process often involves adding firewall rules and patching systems to address the incident?

A. Preparation

B. Eradication

C. Recovery

D. Containment

136. Gary wants to use a tool that will allow him to download files via HTTP and HTTPS, SFTP, and TFTP from within the same script. Which command-line tool should he pick from the following list?

A. `curl`

B. `hping`

C. theHarvester

D. `nmap`

137. Tim wants to check the status of malware infections in his organization using the organization's security information and event management (SIEM) device. What SIEM dashboard will tell him about whether there are more malware infections in the past few days than normal?

A. The alerts dashboard

B. The sensors dashboard

C. The trends dashboard

D. The bandwidth dashboard

138. Warren is gathering information about an incident and wants to follow up on a report from an end user. What digital forensic technique is often used when end users are a key part of the initial incident report?

A. Email forensics

B. Interviews

C. Disk forensics

D. Chain of custody

139. Aaron wants to use a multiplatform logging tool that supports both Windows and Unix/Linux systems and many log formats. Which of the following tools should he use to ensure that his logging environment can accept and process these logs?

A. IPFIX

B. NXLog

C. syslog

D. `journalctl`

140. Which of the following is not a common type of incident response exercise?

A. Drills

B. Simulations

C. Tabletop

D. Walk-throughs

141. Susan needs to run a port scan of a network. Which of the following tools would not allow her to perform that type of scan?

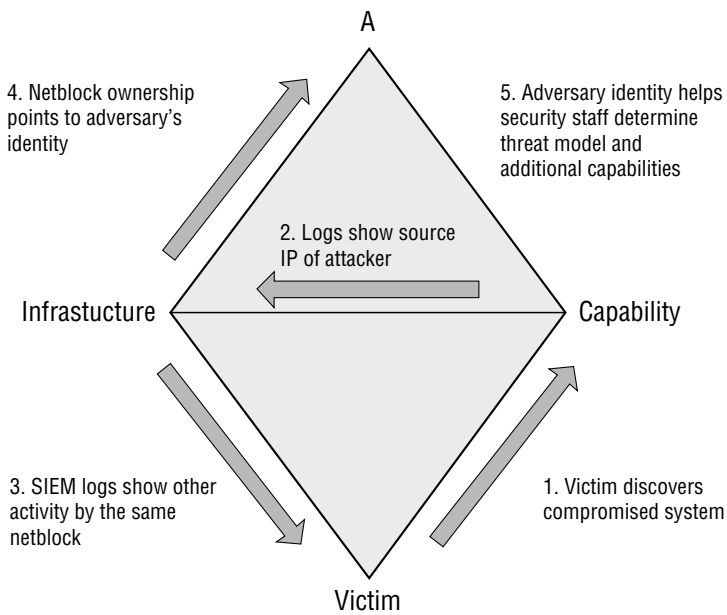
A. `netstat`

B. `netcat`

C. `nmap`

D. Nessus

142. What term belongs at point A on the Diamond Model of Intrusion Analysis shown below?



A. Opponent

B. Target

C. Adversary

D. System

143. The government agency that Vincent works for has received a Freedom of Information Act (FoIA) request and needs to provide the requested information from its email servers. What is this process called?

A. Email forensics

B. An inquisition

C. e-discovery

D. Provenance