# CySA+

## Cybersecurity Analyst

**CCI**
**Post Office Box 9627**
**Mississippi State, MS 39762**

# CySA+

## Part 1
## Threat Management

# Responding to Network-Based Threats

## Chapter 3

# Outline

- Network Segmentation
- Honeypots and Honeynets
- Endpoint Security
- Group Policies
- Device Hardening
- Network Access Control

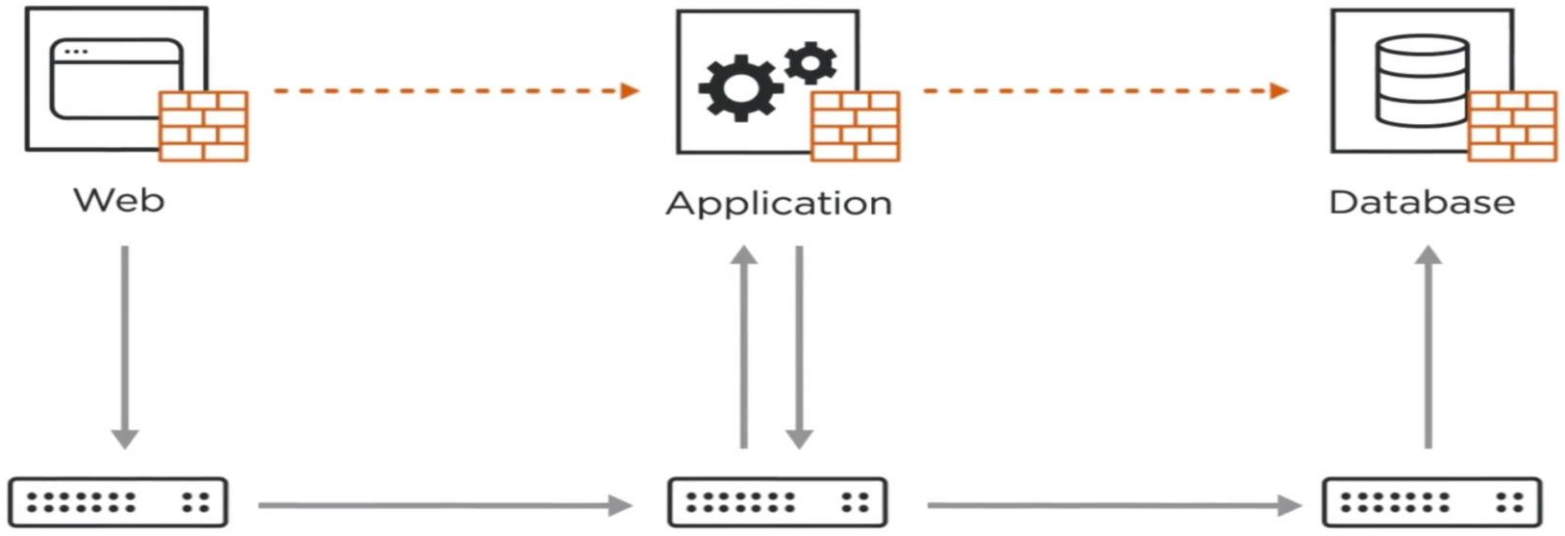
# Network Segmentation

- **Network Segmentation**
  - The practice of splitting up different parts of the network into subordinate zones
- **Goal of Network Segmentation**
  - Increase the difficulty level for advisories
  - Better management of traffic
  - Maintain sensitive data in a secure zone of the network
- **Network Segmentation Implementation**
  - Can be implemented in the physical layer and each layer up to the application layer
  - For example, it is common to use virtual local area networks (VLANs) in the link layer of the network

[1]

# Network Segmentation

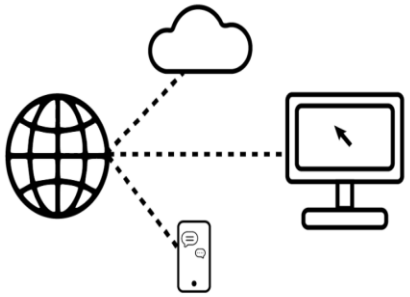
- **Micro-Segmentation**
  - **A network security technique**
  - **Allows detailed security policies to be assigned to data center applications, down to the workload level**
  - **Makes use of containers, software-defined networks, virtualized infrastructure, and cryptographic restrictions**

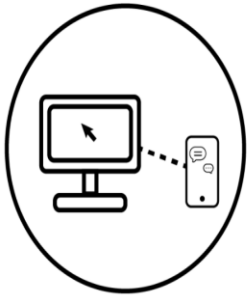



[1,2]

# Network segmentation

- **System Isolation**
  - **Air gap**
    - **Physically separating a machine or a group of machines from outside connections**
    - **Use access control lists (ACLs) to set rules to deny or allow access to the air-gapped machines**
      - **Allows and denies access depending on the layer it is operating on**
      - **Most often operating on the network or file system level**





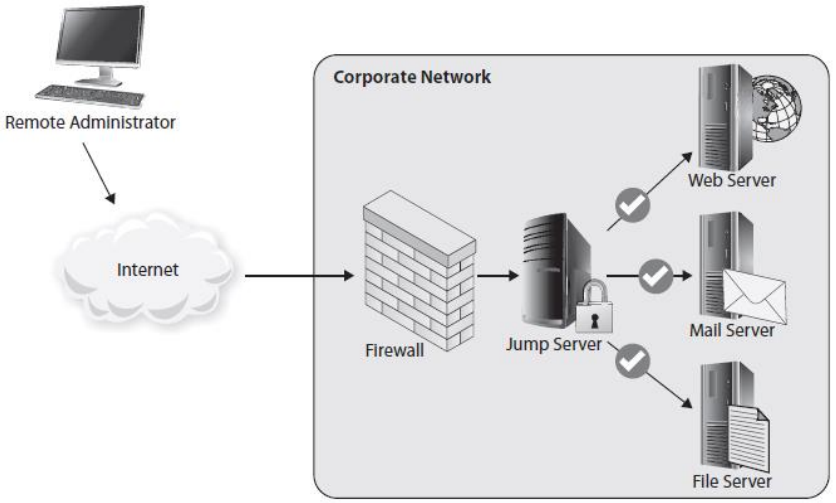
**Air-gapped Network**

Devices included in the air-gapped network are physically isolated and can communicate with each other, but cannot communicate with any other network outside of the air-gap.

[3]

# Network Segmentation

- **Jump Box**
  - **Also known as Jump Server**
  - **A machine that severs as a jumping-off point for external users to access protected parts of a network**
  - **Example use case**
    - **Most often, admin use Jump Boxes to remotely log into sensitive hosts**




[1]

# Network Segmentation

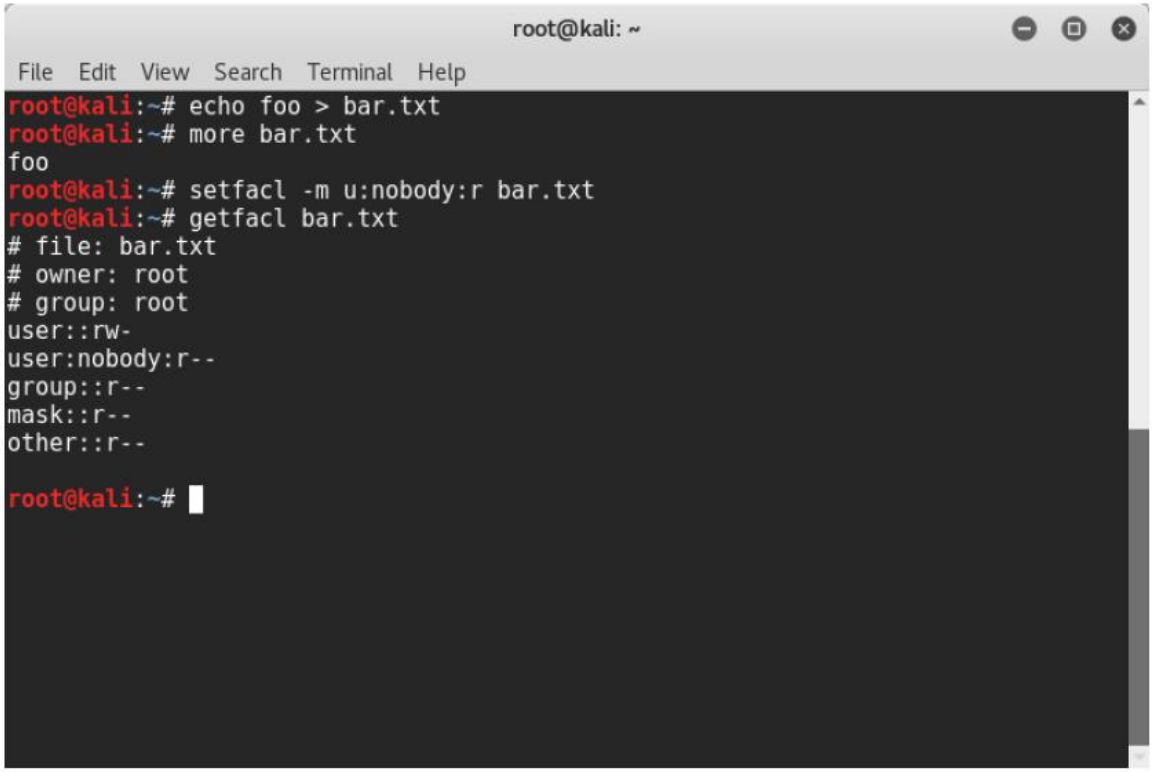
- **Honeypot**
  - **A highly vulnerable machine that is used to attract attackers**
  - **Are made to appear to be a legitimate target**
  - **Isolated from the actual network**
  - **All activity on the honeypot is monitored and logged**
- **Honeynet**
  - **A set of interactive honeypots**
  - **Designed to look like a legitimate network environment**
- **Both are used to**
  - **Gain insight into the attacker's tactics, techniques, and procedures (TTPs)**
  - **Delay and exhaust an attacker's resources**

[1]

# Network Segmentation

- Access Control List ACLs
  - Table of files or networks and the users that can access or modify them.
  - Used to secure networks
- File System ACLs
  - Selectively allow or deny one user or a group of users
  - Was developed to give granular levels of access over a file or directory
- Network ACLs
  - Can selectively accept or deny both inbound and outbound network traffic
  - Access conditions depends on the device
    - Switches are layer 2 devices and use IP and Mac address as access conditions
    - Routers are layers 3 and 4 devices and can use IP, network protocol, or port as access conditions

[1]




# Network ACL Example

**Example listing**

[1]

# Network Segmentation

- **Black Hole**
  - **A device configured to accept all packets from a specific source or destination address and then not respond**
  - **Advisories rely on network probing; if an advisory's IP address is known, a black hole will not return any exploratory information**
- **DNS Sinkholes**
  - **Targets known malicious domains**
  - **Can be used to find machines infected with malware**
  - **Example**
    - **When an infected machine tries to connect to a malicious site to download needed tools, the DNS Sinkhole will return a special server IP address**
    - **If any machine tries to connect to that IP address, it will be logged, and the admin will know which machines are infected**

[1]

# Endpoint Security

- **Endpoint Security**
  - **Fortifying host machines against attacks**
- **Detect and Block**
  - **Signature-based malware detection**
    - **Compares hashes of files on the host machine against known malicious files**
  - **Behavior-based malware detection**
    - **Monitors system processes for expected malware behavior**
  - **Possible Limitations**
    - **Signature-based malware detection does not always work because polymorphic malware files are constantly changing**
    - **Files can be incorrectly identified as malware causing false positives**

[1]

# Endpoint Security

- **Sandbox**
  - **A virtual machine with a realistic OS environment that is used**
    - **To test files for malicious code before running on the host machine**
    - **To observe and research malware**
  - **Advisories will test their malicious code against popular malware detection software in a sandbox**
  - **Advisories have also been known to develop malware that detects a sandbox and will remain dormant to evade detection**

[1]

# Endpoint Security

- **Cloud-Connected Protection**
  - **Cloud computing is used to enhance system security by allowing for quick analysis of files status and behavior**
  - **Cloud-based Security**
    - **Automatic sharing of threat details across a network**
    - **Minimizes risks of infection from known and unknown threats**
- **Trust**
  - **Problem**
    - **Humans make mistakes such as falling for phishing emails or losing devices**
  - **Zero-trust environments**
    - **Admin will try to design and defend the network as if threats are coming from external and internal sources** [1]

# Group Policies

- **Directory Service**
  - **Enterprise devices rely on directory services to great access to shared resources**
- **Active Directory**
  - **Microsoft directory service developed for Windows domain networks**
  - **Provides authentication and authorization services**
  - **Using policies it allows for remote administration**
    - **Admin can force user machines to a baseline setting using a group policy**
    - **Can set security settings for both user accounts and machines at the local, domain or network level using group policies**

[1]

# Device Hardening

- **Device Hardening**
  - The practice of increasing the time and effort for an adversary to make network discoveries
  - This practice can also make it more likely for the adversary to be discovered
  - To be effective, this requires continuous monitoring of the network and local resources
- **Rules to follow**
  - Resources should only be accessed by those who require them to do their work
  - Host machines should only have the required application for the user to perform their job
  - Updates and patch releases should be applied often and as early as possible

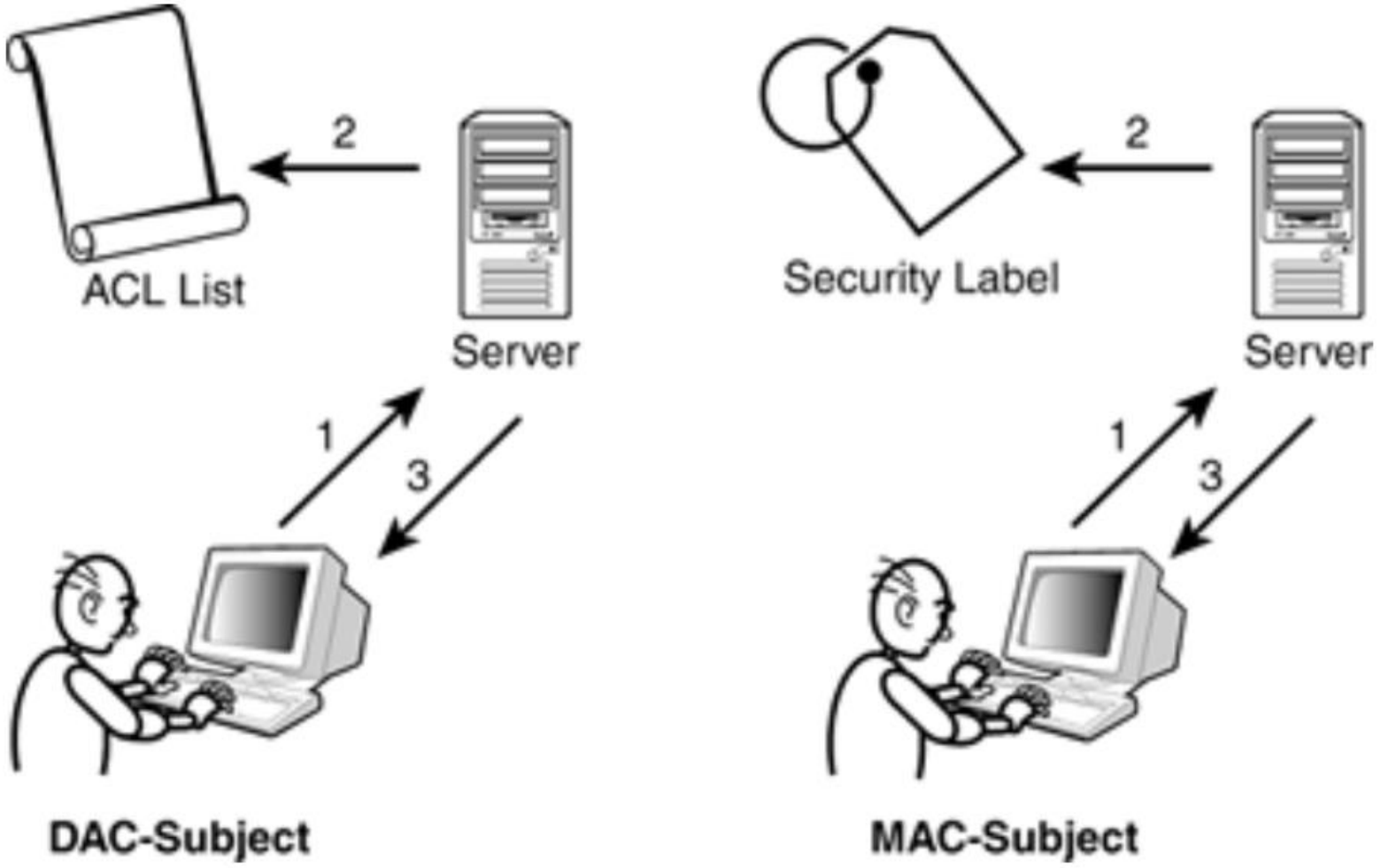
[1]

# Device Hardening

- Discretionary Access Control (DAC)
  - Access is given to the media for a given user or group at the discretion of the admin or the content owner
  - The validation for access occurs at the resource
- Mandatory Access Control (MAC)
  - Access is given with explicit authorization for a given user on a given object
  - This is a model that has additional labels for multi-level security that is applied to both subject and object
    - Unclassified, Confidential, Secret, and Top Secret
  - Classification Level
    - The security label on the file (object)
  - Clearance Level
    - The security level of the user (Subject)

[1]

# (MAC) VS (DAC) illustration




[4]

# (DAC)vs(MAC) Exercise

| Characteristic | MAC | DAC |
|---|---|---|
| Access control enforced by | | |
| Flexibility | | |
| Scalability | | |
| Simplicity | | |
| Maintenance | | |
| Implementation cost | | |
| Granularity | | |
| Easy to use | | |
| Security level | | |
| Useful for | | |

[5]

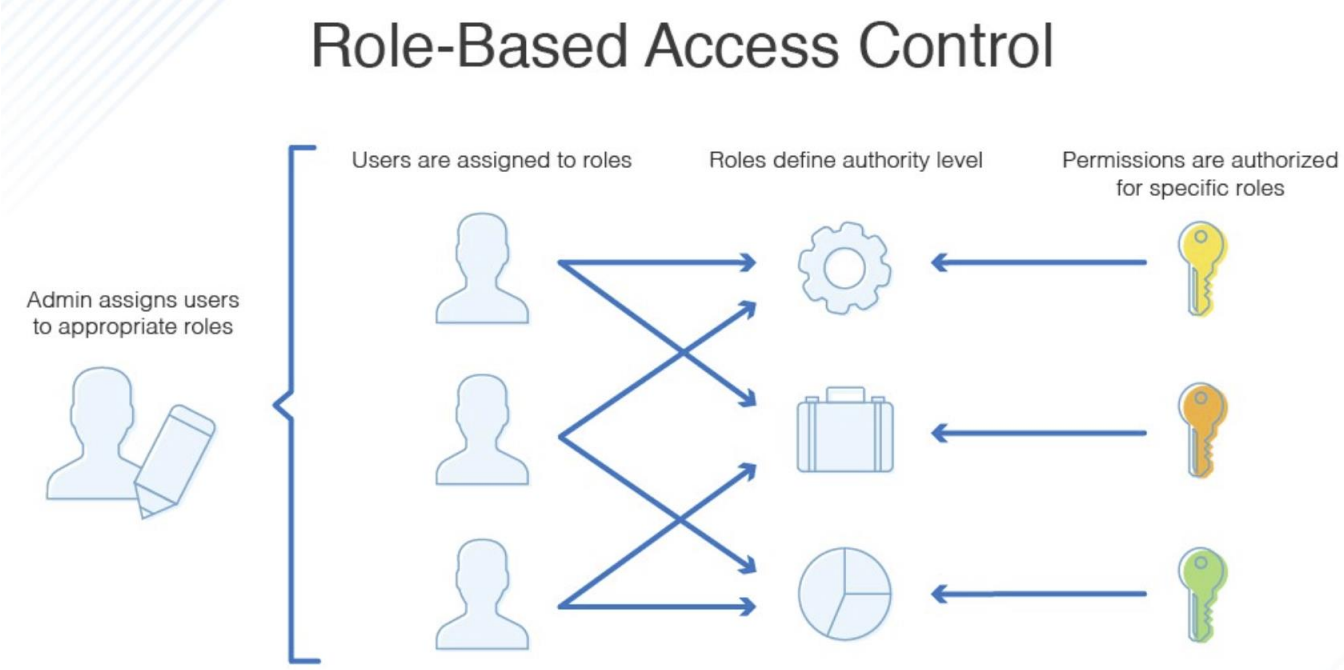
# (DAC) Vs (MAC) Exercise answers

| Characteristic | MAC | DAC |
|---|---|---|
| Access control enforced by | Administrators and operating system | Administrators and users |
| Flexibility | – | ✓ |
| Scalability | – | ✓ |
| Simplicity | – | ✓ |
| Maintenance | Hard | Easy |
| Implementation cost | High | Low |
| Granularity | High (admins adjust clearances for each user and object manually) | High (users can assign access rights for any other user or group) |
| Easy to use | – | ✓ |
| Security level | High | Low |
| Useful for | Government, military, law enforcement | Small and medium-sized companies |

[5]

# Device Hardening

- **Role-Based Access Control (RBAC)**
  - **Grants access based on the user's role or group**
  - **Access is never granted directly to the user**
  - **Regardless of the total amount of users, there should be fewer roles than users making management much easier**




[1,6]

# Device hardening

- **Compensating Controls**
  - **An organization using any means possible to meet security requirements even if they were unable to meet the requirement explicitly due to an unavoidable conflict**
  - **Example**
    - **Problem: A company using the same network for both financial operations and external web**
    - **Compensating Control: The company introducing a Switch that is capable of VLAN management and enforcing ACLs at the switch and router level**

# Device Hardening

- **Blocking Unused Ports/Services**
  - **Consumer products**
    - **Many are designed to be connected to the network that has unnecessary services running**
    - **It is important to disable unnecessary services**
  - **Well-known ports**
    - **UDP and TCP ports between 0 and 1023**
    - **20(FTP), 22(SSH), 25(SMTP), and port 80(HTTP)**
    - **Ports 1024 – 49151 are registered ports**
    - **Ports above 49151 are ephemeral or dynamic ports**
- **Patching**
  - **It is important to patch software to prevent adversaries from exploiting the vulnerable unpatched software**
  - **Major vendors like Microsoft have improved patching by providing automatic updates**

[1]

# Network Access Control

- **Network Access Control (NAC)**
  - **Features**
    - **Endpoint visibility**
    - **Policy enforcement checks before a device can connect to the network**
    - **Utilizes RBAC, verification of endpoint malware protection, and version checks**
  - **Concerns**
    - **Network performance problems**
      - **Version checking and remediation of several hundred non-compliant endpoints requires a lot of resources**
    - **User privacy concerns**
      - **NAC verifies the status of the endpoint's software and system configuration**

[1]

# Network Access Control

- **Time Based**
  - Provides network access for fixed time intervals
  - Can enforce time limits for guest access
  - Can set time policies for different groups
- **Rule Based**
  - Rule-based NAC queries the host machine to verify any criteria that are defined by the list of rules
  - Rules may be software or hardware related
  - Can operate in passive mode and only report rule violations

[1]

# Network Access Control

- **Role Based**
  - Using a role-based NAC solution can prevent unauthorized data disclosure
  - NAC can utilize existing RBAC policies and enforce them across the network
  - Role-Based NAC can serve as a DLP solution
    - Can verify the presence of host-based DPL tools
    - Can more quickly locate sensitive information across various parts of the network
- **Location Based**
  - NAC can grant access to the user depending on the location of their device
  - This provides both identity verification and more accurate asset tracking

[1]

# Quiz

## Chapter 3

# Question #1

- **Which of the following is the correct term for a network device designed to deflect attempts to compromise the security of an information system?**
  - **A. ACL**
  - **B. VLAN**
  - **C. Jump box**
  - **D. Honeypot**

[1]

# Answer #1

- **D**
  - **Honeypots are fake systems developed to lure threat actors to them, effectively deflecting their attacks.**
  - **Once the actors start interacting with the honeypot, it may slow them down and allow defenders to either study their techniques or otherwise prevent them from attacking real systems.**

[1]

# Question #2

- **Network Access Control (NAC) can be implemented using all of the following parameters except which one?**
  - **A. Domain**
  - **B. Time**
  - **C. Role**
  - **D. Location**

[1]

# Answer #2

- **A**
  - **NAC uses time, rules, roles, or location to determine whether a device should be allowed on the network.**
  - **The domain to which the device claims to belong is not used as parameter to make the access decision.**

[1]

# Question #3

- **You are reviewing the access control list (ACL) rules on your edge router. Which of the following ports should normally not be allowed outbound through the device?**
  - **A. UDP 53**
  - **B. TCP 23**
  - **C. TCP 80**
  - **D. TCP 25**

[1]

# Answer #3

- **B**
  - **TCP port 23 is assigned to telnet, which is an inherently insecure protocol for logging onto remote devices.**
  - **Even if you allow telnet within your organization, you would almost certainty want to encapsulate it in a secure connection.**
  - **The other three ports are almost always allowed to travel outbound through a firewall, because DNS (UDP 53), HTTP (TCP 80), and SMTP (TCP 25) are typically required**

[1]

# Question #4

- **What is the likeliest use for a sinkhole?**
  - **A. To protect legitimate traffic from eavesdropping**
  - **B. To preventing malware from contacting command-and-control systems**
  - **C. To provide ICMP messages to the traffic source**
  - **D. Directing suspicious traffic toward production systems**

[1]

# Answer #4

- **B**
  - **Sinkholes are most used to divert traffic away from production systems without notifying the source (that is, without sending ICMP messages to it).**
  - **They do not provide protection from eavesdropping and, quite the opposite, would facilitate analysis of the packets by network defenders.**
  - **A very common application of sinkholes is to prevent malware from using DNS to resolve the names of command-and-control nodes.**

[1]

# Question #5

- **Which of the following is not technique normally used to segregate network traffic in order to thwart the efforts of threat actors?**
  - **A. Micro-segmentation**
  - **B. Virtual LANs**
  - **C. Jump server**
  - **D. NetFlow**

[1]

# Answer #5

- **D**
  - **NetFlow is system designed to provide statistics on network traffic. Micro-segmentation, virtual LANs and jump servers (or jump boxes) all provide ways to isolate or segregate network traffic.**

[1]

# Question #6

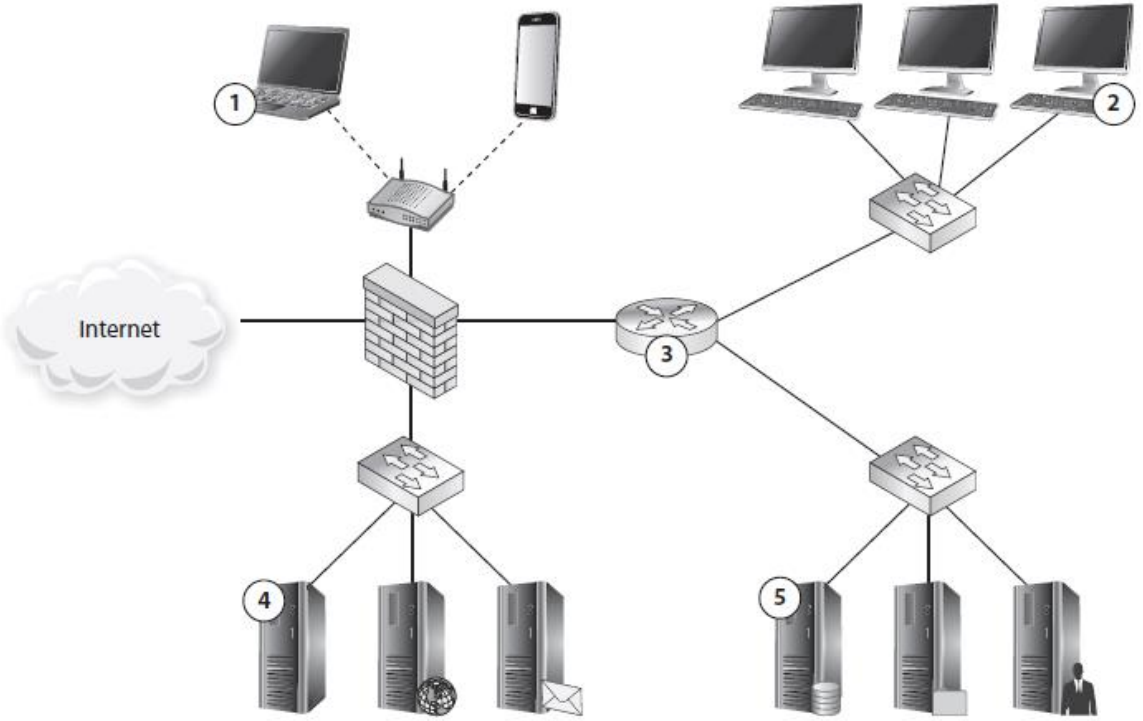
- **Which of the following terms is used fir an access control mechanism whose employment is deliberately optional?**
  - **A. DAC**
  - **B. MAC**
  - **C. RBAC**
  - **D. EBAC**

[1]

# Answer #6

- **A**
  - **The discretionary access control (DAC) model requires no enforcement by design. The other listed approaches are either mandatory (MAC) or agnostic to enforcement (RBAC and EBAC).**

[1]




## Question #7

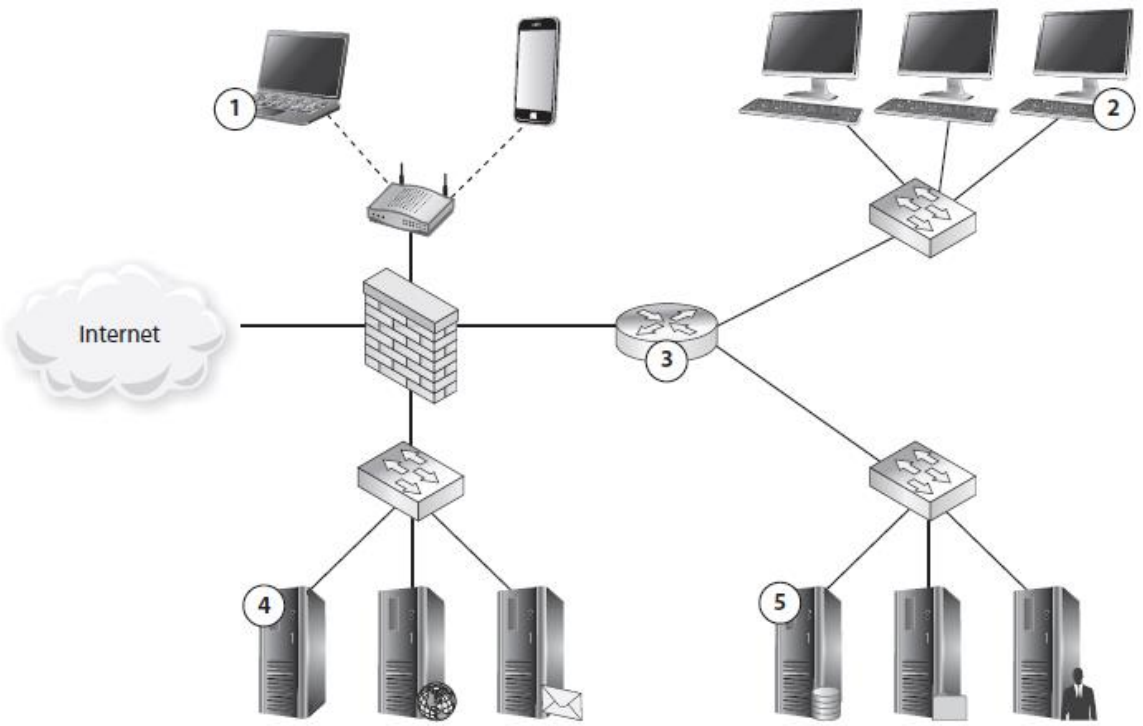
- **Where would be the best location for a honeypot?**
  - **A. Circle 2**
  - **B. Circle 4**
  - **C. Either circle 2 or 5**
  - **D. None of the above**

[1]

# Answer #7

- **B**
  - **Honeypots, sinkholes, and black holes should all be deployed as far from production systems as possible. Therefore, the unlabeled server on the DMZ would be the best option.**

[1]




## Question #8

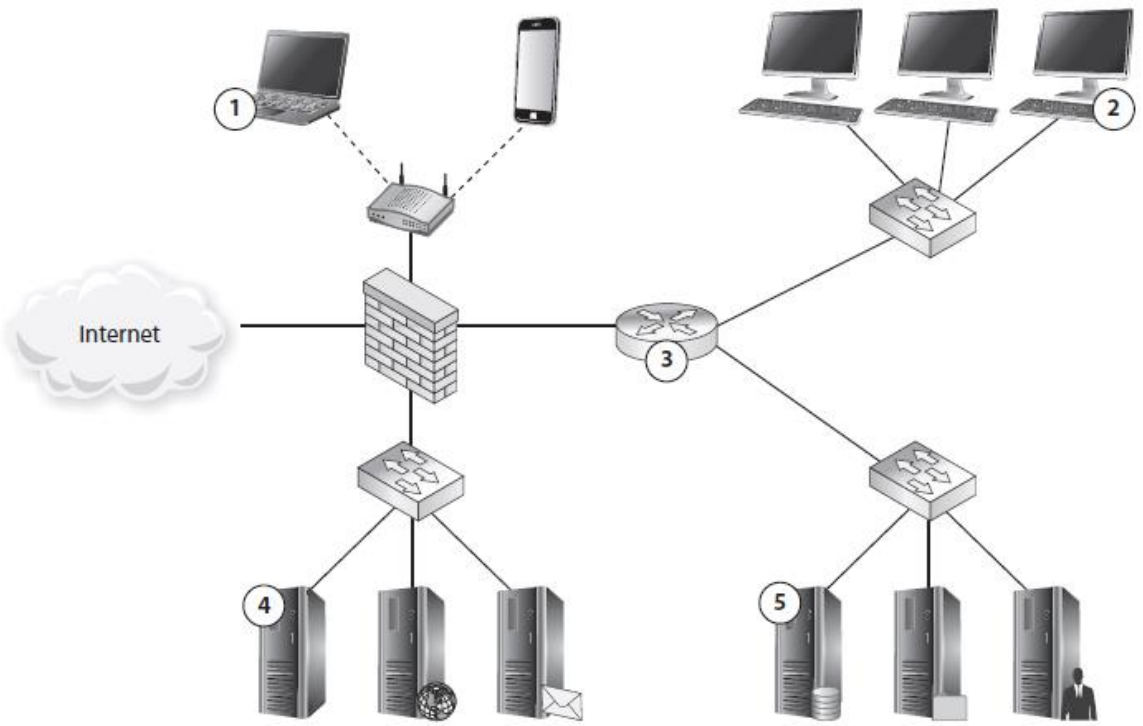
- **Which would be the best location at which to use a sandbox?**
  - **A. Any of the five circled locations**
  - **B. Circle 3**
  - **C. Circles 4 and 5**
  - **D. Circles 1 and 2**

[1]

# Answer #8

- **D**
  - **Sandboxes are typically used at endpoints when executing code that is not known to be benign.**
  - **Circles 1 and 2 are end-user workstations, which is where we would normally deploy sandboxes because the users are prone to run code from unknown sources.**
  - **Because anything running on a router or server should be carefully vetted and approved beforehand, circle 3 and 5 are not where we would normally expect to deploy sandboxes.**
  - **Circle 4 might be a possible location if it were designed solely for that purpose, but it was bundled with the data server at circle 5, which makes it less than ideal.**

[1]




## Question #9

- **Where would you expect to find access control lists being used?**
  - **A. Circle 1 and 2**
  - **B. Circle 3**
  - **C. All the above**
  - **D. None of the above**

[1]

# Answer #9

- **C**
  - **Access control list (ACLs) can be found almost anywhere on a network.**
  - **Endpoints use them to control which users can read, modify, or execute files, while routers can also use them to control the flow of packets across their interfaces.**

[1]

# Scenario For Questions 10 & 11

**Your industry sector is facing a wave of intrusions by an overseas crime organization. Their approach is to persuade end users to click a link that will exploit their browsers or, failing that, will prompt them to download and install an "update" to their Flash Player. Once they compromise a host, they establish contact with the command-and-control (C2) system using DNS to resolve the ever-changing IP addresses of the C2 nodes. You are part of your sector's Information Sharing and Analysis Center (ISAC), which gives you updated access to the list of domain names. Your company's culture is very progressive, so you cannot take any extreme measures to secure your systems, lest you incur the wrath of your young CEO.**

[1]

# Question #10

- **You realize that the first step should be preventing the infection in the first place. Which of the following approaches would best allow you to protect the user workstations?**
  - **A. Using VLANs to segment your network**
  - **B. Deploying a honeypot**
  - **C. Using sandboxing to provide transparent endpoint security**
  - **D. Implementing MAC so users cannot install software downloaded from the Internet**

[1]

# Answer #10

- **C**
  - **Using sandboxes helps protect the endpoints with minimal impact to the users. It would be ideal to prevent them from installing malware, but the organizational culture in the scenario makes that infeasible (for now).**

[1]

# Question #11

- **How can you best prevent compromised hosts from connecting to their C2 nodes?**
  - **A. Force all your network devices to resolve names provided by the ISAC.**
  - **B. Deploy a honeypot to attract traffic from the C2 nodes.**
  - **C. Implement a DNS sinkhole using the domain names provided by the ISAC.**
  - **D. Resolve the domain names provided by the ISAC and implement an ACL on your firewall that prevents connections to those IP addresses.**

[1]

# Answer #11

- C
  - More often than not, malware comes loaded with hostnames and not IP addresses for their C2 nodes.
  - The reason is that a hostname can be mapped to multiple IP addresses over time, making the job of blocking them harder.
  - The DNS sinkhole will resolve all hostnames in a given list of domains to a dead end that simply logs the attempts and alerts the cybersecurity analyst to the infected host.
  - Blocking Ips will not work as well, because those addresses will probably change often.

[1]

# Question #12

- **You start getting reports of successful intrusions in your network. Which technique lets you contain the damage until you can remediate the infected hosts?**
  - **A. Instruct the users to refrain from using their web browser.**
  - **B. Add the infected host to its own isolated VLAN.**
  - **C. Deploy a jump box**
  - **D. Install a sandbox on the affected host.**

[1]

# Answer #12

- **B**
  - **An extreme form of network segmentation can be used to keep infected hosts connected to the network but unable to communicate with anyone but forensic or remediation devices.**

[1]

# References


1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. Illumio, “What is Network Segmentation?,” Illumio. [Online]. Available: https://www.illumio.com/network-segmentation. [Accessed: 01-Oct-2020].
3. Gary DiFazio Gary DiFazio is the Strategic Marketing Director for Industry Cybersecurity at Tripwire. He has been in the technology space for over 26 years, “What is Network Air-gapping?,” Belden, 20-Nov-2019. [Online]. Available: https://www.belden.com/blog/industrial-security/network-air-gapping. [Accessed: 01-Oct-2020].
4. “Data Access Controls,” Data Access Controls | Access-Control Systems and Methodology. [Online]. Available: https://flylib.com/books/en/1.34.1/data_access_controls.html. [Accessed: 01-Oct-2020].

# References


5. “Mandatory Access Control vs Discretionary Access Control: Which to Choose?,” *Mandatory Access Control vs Discretionary Access Control | MAC vs DAC*, 10-Apr-2020. [Online]. Available: https://www.ekransystem.com/en/blog/mac-vs-dac. [Accessed: 02-Oct-2020].
6. “RBAC vs. ABAC Access Control: What's the Difference?,” DNSstuff, 07-Jul-2020. [Online]. Available: https://www.dnsstuff.com/rbac-vs-abac-access-control. [Accessed: 04-Oct-2020].