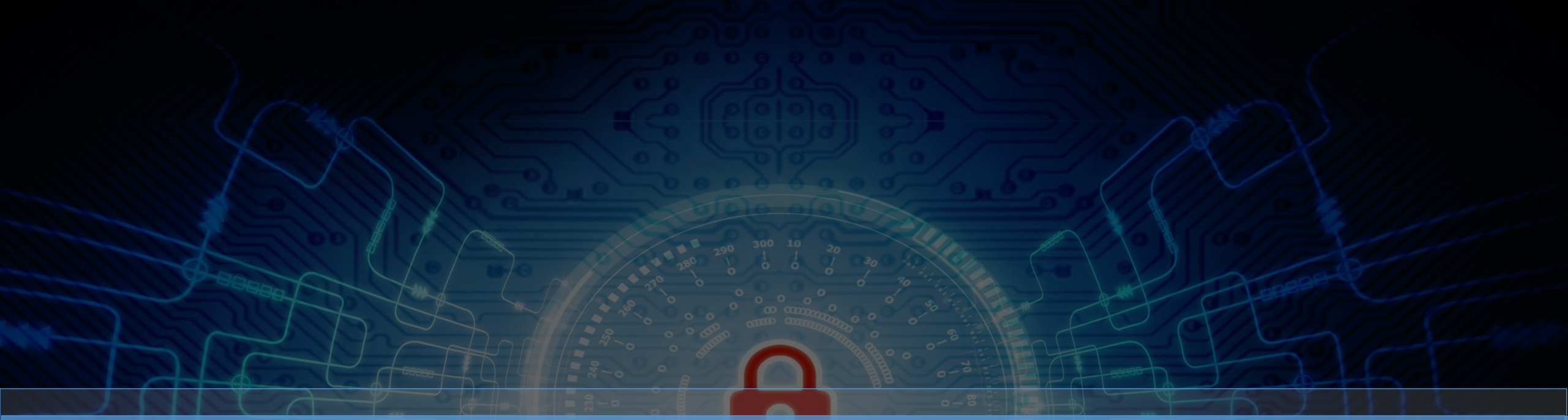
CHAPTER 6

Attacking the Cloud



Episode 6.01 - Cloud Attacks, Part 1

Objective 3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies

CLOUD ATTACKS

- Credential harvesting
  - Using different techniques to compromise credentials used to access cloud resources
- Privilege escalation
  - Leveraging application or service vulnerabilities to carry out unauthorized actions

CLOUD ATTACKS

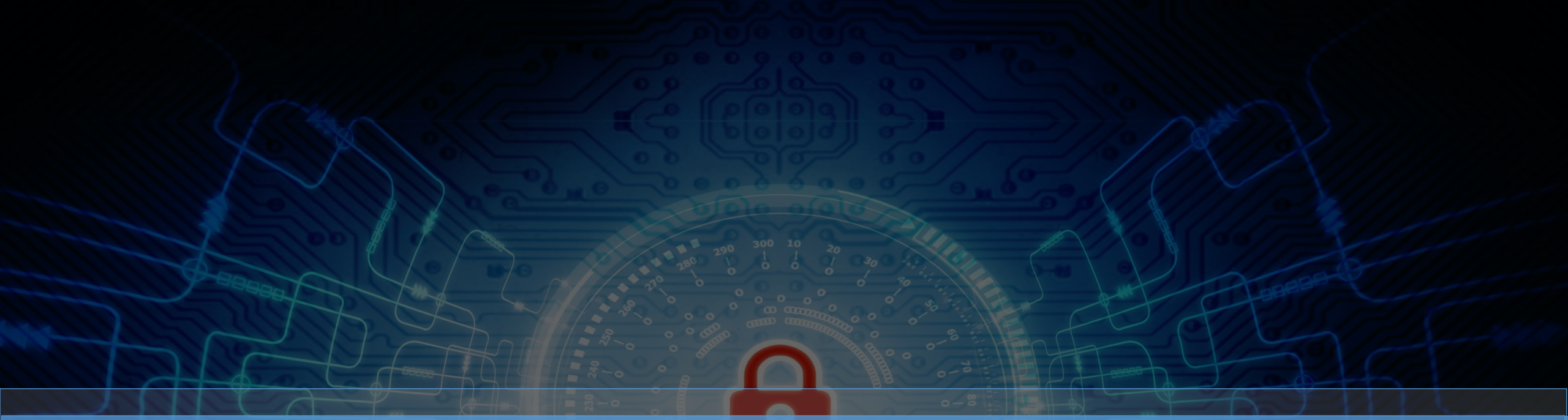
- Account takeover
  - After compromising credentials, attacker changes access configuration to deny the rightful owner access
- Metadata service attack
  - Service that provides information about how to access hosted services
  - Compromised metadata service could report malicious service information

CLOUD ATTACKS

- Misconfigured cloud assets
  - Identity and access management (IAM)
    - Incorrect/malicious authentication/authorization
  - Federation misconfigurations
    - Deny access to authorized subjects or allow access to unauthorized subjects
    - Potential to leak credentials
  - Object storage
    - Improper settings could allow unauthorized access
  - Containerization technologies
    - Improper container configurations can allow unauthorized connections
    - Could lead to further compromise

QUICK REVIEW

- Moving data and functionality outside the traditional trust boundary can lead to vulnerabilities
- A lack of visibility and control can expose resources to abuse
- Many cloud attacks start with spoofing a privileged identity



Episode 6.02 - Cloud Attacks, Part 2

Objective 3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies

CLOUD ATTACKS

- Resource exhaustion
  - Similar to classic DoS/DDoS attacks
  - Threat to service and server availability

CLOUD ATTACKS

- Cloud malware injection attacks
  - Delivering malware to cloud-based VMs and containers
  - Similar to malware delivery for physical servers
- Denial-of-service attacks
  - Saturate network or CPU with traffic/work to leave no capability for authorized processes

CLOUD ATTACKS

- Side-channel attacks
  - Generally carried out by a malicious VM that sample system performance during cryptographic operations to disclose key information
- Direct-to-origin attacks
  - Attacks that penetrate layers of devices intended to protect the true network's addresses
  - Two-step attack – first find the real network, then attack it directly

QUICK REVIEW

- Many cloud attacks are based on traditional on-premises attacks
- Virtualization makes some VM or container escape attacks possible
- Cloud environment security often depends on hiding true addresses