Exam questions, with keywords - which are examples of the subjects in this question.

You should prepare a 10 minute talk about the subject, but don't try to include every keyword!

1) Overview of Enterprise Attacks

- Mitre ATT&CK
- Common Vulnerabilities and Exposures (CVE)
- OWASP Top-10
- Common Weakness Enumeration CWE
- Hacker tools, SATAN, Scanning, Nmap
- Pentesting
- Confidentiality, Integrity and Availability
- Cost-Benefit Analysis
- Risk Analysis
- Human Issues

2) Confidentiality, Integrity and Availability

- Confidentiality, Integrity and Availability
- Deadlocks, DBMS, databases, Postgresql
- Availability and flooding attacks, Protection against TCP Synfloods
- Trust models

3) Real-life Policies

- Policies in general
- Chinese Wall model - Confidentiality and Integrity in the real world
- Clinical Information Systems security model
- Role-based Access Control (RBAC), example Github
- Break-the-glass Policies
- Side Channels and Deducibility
- Memory Errors and Row hammer - explaining row hammer outside of curriculum

4) Basic Cryptography

- Basic Cryptography
- **Symmetric Cryptosystems**
- Data Encryption Standard (DES) / **Advanced Encryption Standard (AES)**
- **Public Key Cryptography**
- Stream and Block Ciphers
- **Hashing**
- Diffie Hellman exchange
- Elliptic-curve cryptography (ECC)
- **Transport Layer Security (TLS)**
- Example cryptosystems OpenPGP, IPsec, Transport Layer Security (TLS)
- Authentication and Password security, NIST guidelines
- Example sslscan scan various sites for TLS settings, Qualys SSLLabs

5) Malware, Intrusion, Vulnerabilities

- Trojan horses, Rootkits, computer viruses

- Computer worms, from Morris Worm to today
- Bots and botnets
- Ransomware
- Phishing and spear phishing
- Sandboxing, Java and browsers
- Penetration testing
- Common Vulnerabilities and Exposure CVE
- Common Weakness Enumeration CWE
- Examples: Smashing The Stack For Fun And Profit, Bypassing non-executable-stack during exploitation using return-to-libc, Basic Integer Overflows, Return-Oriented Programming

6) Secure Systems Design and Implementation

- Security Principles: Principle of least privilege, fail-safe defaults, separation of privilege etc. - dont try to go over ALL of them in 10mins
- Files, objects, users, groups and roles
- Naming and Certificates
- Access Control Lists
- Domain Name System Security Extensions DNSSEC
- Capabilities, Capsicum, Wedge, Jails, chroot, Pledge, and Unveil, in OpenBSD

Other examples: Email security DNSSEC, SPF, DMARC, Email servers vulns in Exim, OpenSMTPD, Firewalls

7) Auditing and Intrusion Detection (Forensics 1)

- Auditing and logging
- Volatility and file systems
- Intrusion Detection
- Host and Networks Based Intrusion Detection (HIDS/NIDS)
- Network Security Monitoring
- Netflow

Examples used:

- Centralized syslogging and example system
- Create Kibana Dashboard
- ENISA papers

8) Incident Response (Forensics 2)

- Attack and Response
- Attack graphs
- Attack surfaces, and reducing them
- Intrusion Handling, phases
- Incident Response
- Digital forensics / Computer Forensics
- Honeypots

Examples:

- Checklist from NIST.SP.800-61r2.pdf
  Incident Handler’s Handbook by Patrick Kral, SANS Information Security Reading Room
  https://www.sans.org/reading-room/whitepapers/incident/paper/33901
- Computer Security Incident Handling Guide, NIST Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

9) Benchmarking and Auditing Recap CIS controls

- Benchmarking standards
- CIS controls Center for Internet Security
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019</li>
- Payment Card Industry Data Security Standard