Welcome to the CoGrammar

Server Configuration

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.

Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(Fundamental British Values: Mutual Respect and Tolerance)**
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: **Questions**

Cyber Security Session Housekeeping cont.

- For all **non-academic questions**, please submit a query: **www.hyperiondev.com/support**
- We would love your **feedback** on lectures: **Feedback on Lectures**
- Find all the lecture **content** in you **Lecture Backpack** on GitHub.
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Nurhaan Snyman

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

CoGrammar HyperionDev

Stay Safe Series:

Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the *Stay Safe Series* will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Security Tip

"Enable login alerts for all your online accounts."

Why?
Login alerts notify you immediately if your account is accessed from an unrecognized device or location. This early warning system allows you to take quick action—such as changing your password or enabling multi-factor authentication (MFA)—to secure your account before further damage is done.

How to Enable:

- Check your account security settings for an option like "Login Alerts" or "Account Activity Notifications."
- Ensure the alerts are sent to a secure email or phone number that only you can access.

Stay proactive and keep hackers out by staying informed!

Server Configuration

December 2024

Learning Objectives & Outcomes

- Define key server security concepts, such as authentication, encryption, and access control.
- Explain the purpose and functionality of server security features, including firewalls and user access controls.
- Configure server settings to implement security measures such as SSL/TLS encryption and role-based access control.
- Identify and assess potential security vulnerabilities in a server environment and recommend corrective actions.
- Develop a comprehensive server security strategy that includes configuration, monitoring, and incident response measures.

Polls

Please have a look at the poll notification and select an option.

What do you think is the primary cause of server security breaches?

A) Weak passwords

B) Outdated software

C) Lack of monitoring

D) Insider threats

Polls

Please have a look at the poll notification and select an option.

What is the primary purpose of a firewall in server security?

- A) To encrypt data
- B) To block unauthorized access
- C) To monitor user activity
- D) To create backups

Introduction to Server Configuration

- **What is Server Configuration?**
  a. The process of setting up and maintaining server systems to ensure optimal performance, reliability and security
  b. Focuses on hardware, software and security measures to protect data and services.

Why it matters

- Protects sensitive data from unauthorized access
- Ensures smooth and uninterrupted server operations
- Mitigates risks from cyber threats

Key Security Features to configure.

- **Access control:**
  - Use role-based access control (RBAC)
  - Implement strong password policies
- **Firewalls**
  - Configure rules to allow only necessary traffic
  - Monitor and log firewall security
- **Encryption**
  - Enable SSL/TLS for secure data transmission
  - Encrypt sensitive data at rest and in transit

Best practices for server security

- **Regular updates and patching**
  - Keep OS and software up to date
  - Apply security patches as soon as they are released
- **System Monitoring**
  - Use intrusion detection and preventions systems
  - Analyze logs regularly for suspicious activities
- **Backup strategy**
  - Schedule regular automated backups
  - Test backup recovery processes periodically
- **Principle of least privilege**
  - Grant minimum access required for tasks
  - Revoke unused permissions immediately

Protecting server data

- **Network security:**
  - Use VPNs for remote access
- **Data protection:**
  - Use data loss prevention (DLP) tools
- **Physical security:**
  - Protect server hardware in secure facilities
- **Security policies and training:**
  - Create clear server security policies

Troubleshooting server security issues

- **Unauthorized access attempts:**
  - Check logs for failed login attempts
  - Block suspicious IP addresses
- **Data breaches:**
  - Identify and isolate affected systems
  - Notify stakeholders and mitigate further risks
- **Malware infections:**
  - Run antivirus scans and remove threats
  - Patch vulnerabilities exploited by malware
- **Performance issues linked to security**
  - Analyze load balancers and firewalls
  - Optimize configurations to avoid bottlenecks

Practical Example

Performing User Creation in Kali Linux and Role-Based Access Control (RBAC)

Polls

Please have a look at the poll notification and select an option.

Which encryption protocol is most commonly used to secure data transmitted over the internet?

A) TLS

B) HTTP

C) FTP

D) SSL

Polls

Please have a look at the poll notification and select an option.

What is the first step you would take to troubleshoot a suspected server security issue?

A) Check server logs

B) Scan for malware

C) Block suspicious IP addresses

D) Notify stakeholders

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar