Welcome to the CoGrammar

Setting up for Cyber Security: Kali Linux, HTTP, and SSH

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

Regularly audit and review your third-party vendors and service providers for security risks.

Make sure to regularly evaluate the security practices of anyone with access to your data or systems, including reviewing contracts for security clauses and asking for up-to-date audits or certifications.

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar

Setting up for Cyber Security: Kali Linux, HTTP, and SSH

November 2024

Learning Objectives & Outcomes

By the end of the lecture, everyone should be able to:

- Recognize the purpose and features of Kali Linux in the context of cybersecurity and penetration testing.
- Explain client-server architecture.
- Define HTTP protocol in security.
- Configure SSH for secure communications.

Learning Objectives & Outcomes

In your own words, can you explain what a Virtual Machine or VirtualBox is and how it can be useful in a cybersecurity or IT environment?

Polls

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

In a client/server architecture, which statement is correct?

A. The client provides resources, and the server requests them.
B. The server provides resources or services, and the client requests them.
C. Both the client and server are resource providers.
D. The client and server operate without any communication

Polls

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

What is the primary purpose of HTTPs in a client/server communication?

A. To make the website load faster
B. To encrypt the data exchanged between client and server.
C. To prevent server-side errors
D. To ensure the server is always online

Kali linux overview

- **What is Kali linux?**
  - A linux distribution designed for penetration testing and security auditing.
  - Pre-installed tools for network analysis, exploitation, forensics and more.
- **Features**
  - Open source
  - Supports a wide range of wireless and wired networking tools
  - Customisable and flexible for various environment

Kali linux overview

- **Installation:**
  - Follow the additional resources guide:
    - https://drive.google.com/file/d/1NS2csE66v59cmdolkxmgz1KYos6HfnES/view

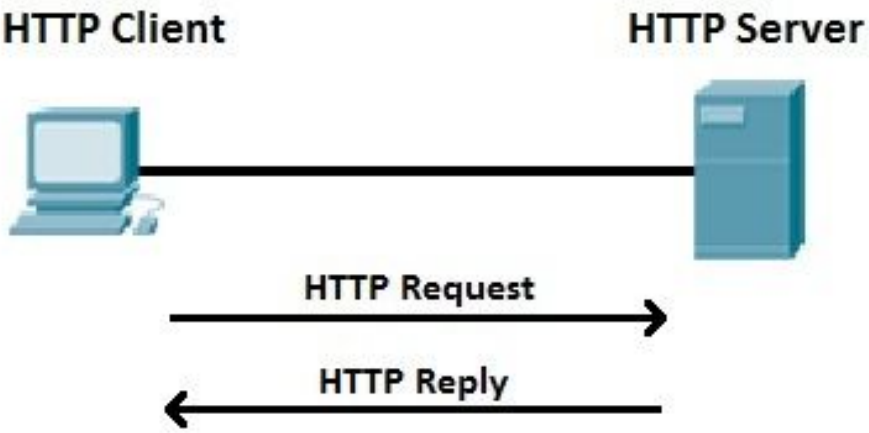
HTTP

- **What is HTTP?**
  - HyperText Transfer Protocol (HTTP) is the foundation of any data exchange on the web.
- **HTTP Status Codes:**
  - HTTP status codes are like short notes from a server that get tacked onto a web page.
- **Status Codes Cheat sheet:**
  - https://www.oxitsolutions.co.uk/blog/http-status-code-cheat-sheet-infographic

MIME TYPES

- **MIME TYPES:**
  - Helps the browser open the file with the appropriate extension or plugin and also helps a server identify how to process a specific file if it is sent from client to server.
- **List of available mime-types:**
  - https://www.iana.org/assignments/media-types/media-types.xhtml

HTTP: Request/Response Cycle



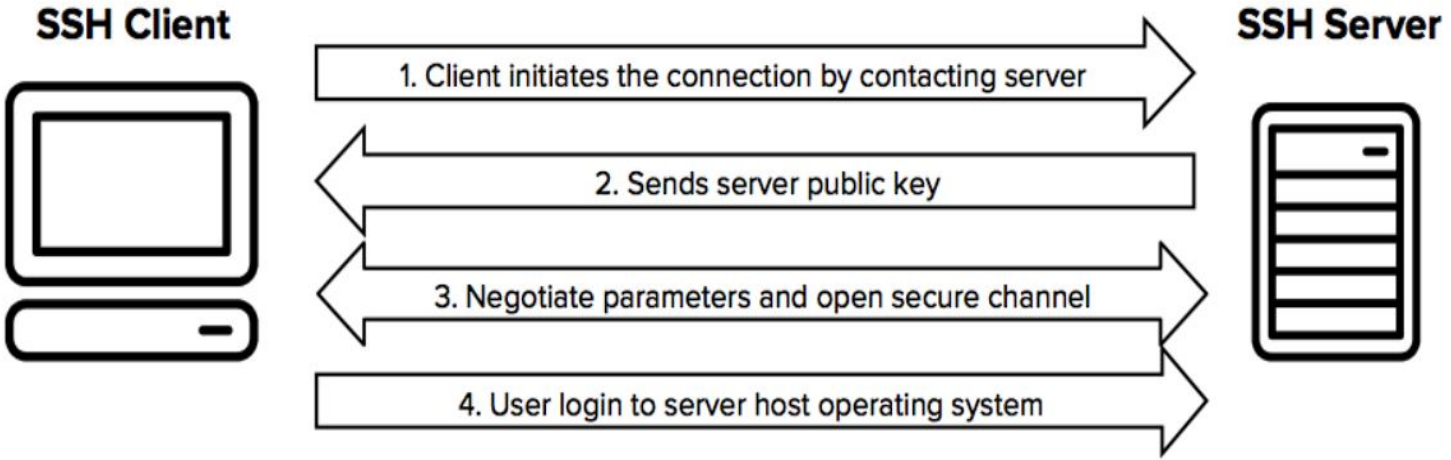
Configuring HTTP Services in kali

- **Install apache:**
  - sudo apt update
  - sudo apt install apache2
- **Start Apache service:**
  - sudo systemctl start apache2
  - sudo systemctl enable apache2
- **Test HTTP Server:**
  - Access the server by visiting http://localhost/ or http://<your_ip_address>/.
  - Check that Apache is serving the default “It works!” page.

Configuring HTTP Services in kali

- **What is SSH?**
  - A network protocol used for securely accessing remote systems over an unsecured network.
  - Provides encrypted communication for shell access, file transfers and more.
- **Common uses of SSH:**
  - Remote administration of servers.
  - Secure file transfer.
  - Tunneling and port forwarding.

SSH


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

Configuring HTTP Services in kali

- **Install OpenSSH Server:**
  - sudo apt update
  - sudo apt install openssh-server
- **Start ssh service:**
  - sudo systemctl enable ssh
  - sudo systemctl start ssh
- **Test SSH Connection:**
  - ssh user@<your_ip_address>

HOMEWORK

- **Securing HTTP traffic with HTTPS:**
  - Secure the HTTP traffic by setting up SSL/TLS and configuring HTTPS on the server.
- **Securing SSH**
  - Implement SSH key-based authentication for more secure access.
  - Optionally disable password authentication to further enhance SSH security.

Polls

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

Which of the following is NOT a use case for SSH?

A. Secure remote login to a server
B. Transfer files securely between client and server
C. Encrypt web page data for a browser
D. Create secure tunnels for port forwarding.

Polls

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

What key difference distinguishes HTTPS from HTTP?

A. HTTPS uses port 80, while HTTP uses port 443
B. HTTPS provides encryption via SSL/TLS, while HTTP does not
C. HTTPS requires a faster internet connection
D. HTTP is used for secure communication, while HTTPS is not.

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar