🚨 OPERATION DIGITAL JUSTICE - RAY THE ATTACKER

Cyber Security Assignment: Portray the Attacker

📋 Assignment Submission Details

1. URL of the Site (Single Page)

Live Site URL: `file:///path/to/your/project/index.html`

> **Note:** This is a static website consisting of three files:
> - `index.html`
> - `styles.css`
> - `script.js`
>
> To view the site:
> 1. Download all three files to the same folder
> 2. Open `index.html` in any modern web browser (Chrome, Firefox, Edge, Safari)
> 3. The site is fully responsive and works on desktop and mobile devices

Alternative Hosting Options:

- GitHub Pages: `https://yourusername.github.io/operation-digital-justice/`
- Netlify: `https://operation-digital-justice.netlify.app/`
- Vercel: `https://operation-digital-justice.vercel.app/`

---

2. Attacker Story Script (150-200 Words)

Narration for Presentation:

In November 2025, a decentralized hacktivist collective called Echo Strike launched Operation Digital Justice against TechFlow Industries, a fictional corporation accused of environmental crimes and whistleblower suppression. Their motive was clear: expose corporate wrongdoing and force accountability through digital disruption.

The operation unfolded in three calculated phases. During reconnaissance, Echo Strike spent three weeks gathering intelligence through social media, open-source research, and social engineering tactics targeting employees. They identified vulnerabilities in TechFlow's infrastructure and mapped their digital landscape.

In the delivery phase, the collective launched sophisticated phishing campaigns and exploited an unpatched VPN gateway to gain initial access. Once inside, they established persistence and began exfiltrating sensitive data.

The final impact phase was devastating. Echo Strike leaked fifteen thousand internal documents exposing environmental violations, launched a massive DDoS attack that took down TechFlow's website for three hours, and coordinated a viral social media campaign that reached millions worldwide.

The defender countermeasures displayed on this site—DDoS protection, security monitoring, employee training, strong access controls, and aggressive patch management—represent essential defenses against hacktivist threats. These groups prioritize visibility and disruption, making proactive security and rapid incident response critical for any organization.

Word Count: 197 words

---

3. Attacker Type Declaration

Our attacker type is: Hacktivists

🎯 Project Overview

This project demonstrates a comprehensive understanding of **hacktivist** cyber threats through an immersive, interactive single-page website and accompanying narration.

Key Features:

✅ **Single-page responsive website** (HTML, CSS, vanilla JavaScript only)
✅ **Gen Z cyber aesthetic** (dark mode, neon accents, terminal-inspired design)
✅ **Complete attacker profile** (motive, tactics, target, impact)
✅ **Three realistic mock artifacts** (manifesto, leaked email, social media post)
✅ **Three-phase attack timeline** (reconnaissance → delivery → actions/impact)
✅ **Defender countermeasures** (DDoS protection, SIEM, training, MFA, patching)
✅ **Interactive elements** (smooth scrolling, click-to-expand timeline, hover effects)
✅ **150-200 word narration script** for presentation

🛠️ Technical Stack

- **HTML5 -** Semantic markup and structure
- **CSS3 -** Custom styling with gradients, animations, and responsive design
- **Vanilla JavaScript -** Interactive functionality (no frameworks)

- **Design Philosophy -** Gen Z hacktivist aesthetic with neon purple, cyan, pink, and lime green accents

---

📁 Project Structure

```
operation-digital-justice/
│
├── index.html          # Main HTML structure (single page)
├── styles.css          # All styling and animations
├── script.js           # Interactive functionality
└── README.md           # This file (submission documentation)
```

🎨 Design Elements

Color Palette

- **Background:** Deep charcoal (#0a0a0a)
- **Primary Accent:** Neon Purple (#a855f7)
- **Secondary Accent:** Electric Cyan (#06b6d4)
- **Tertiary Accent:** Hot Pink (#ec4899)
- **Quaternary Accent:** Lime Green (#84cc16)

Typography

- **Headings:** Arial Black, bold, high-impact
- **Body Text:** Segoe UI, clean and readable

Interactive Features

- Smooth scroll navigation
- Expandable timeline sections
- Hover effects on all cards
- Scroll-triggered animations
- Keyboard shortcuts (Press 'T' for timeline)

🎭 Attacker Profile: Echo Strike

Who They Are

Echo Strike is a decentralized collective of digital activists fighting for environmental justice and corporate accountability. United by ideology rather than geography, they operate across encrypted channels and social media platforms.

Motive (WHY)

Expose corporate environmental violations and force accountability through public disruption and data exposure.

Tactics (HOW)

- DDoS attacks using botnets
- Website defacement
- Data exfiltration and leaks
- Coordinated social media campaigns
- Social engineering and phishing

Target (WHO/WHAT)

TechFlow Industries - a fictional multinational corporation accused of illegal waste dumping and silencing whistleblowers.

Impact (SO WHAT)

- 3-hour website outage
- 15,000+ leaked documents
- $2M+ in lost revenue
- Massive PR crisis
- Regulatory investigations
- CEO resignation

📊 Attack Timeline

Phase 1: Reconnaissance (Weeks 1-3)

- Social engineering via LinkedIn
- OSINT gathering from public sources

- Infrastructure vulnerability scanning
- Employee forum monitoring

Phase 2: Delivery / Initial Access (Week 4)

- Phishing campaign targeting employees
- Credential harvesting
- VPN gateway exploitation
- Backdoor establishment

Phase 3: Actions / Impact (Weeks 5-6)

- Data exfiltration (15,000+ documents)
- DDoS attack (200k+ IoT devices)
- Website defacement
- Data dump release
- Social media amplification

🛡️ Defender Countermeasures

The website includes a comprehensive "Security Team Playbook" featuring five critical defenses:

1. **DDoS Protection -** Cloud-based mitigation and rate limiting
2. **Log Monitoring & SIEM -** 24/7 SOC with real-time alerting
3. **Security Awareness Training -** Phishing simulations and education
4. **Access Controls & MFA -** Zero-trust architecture
5. **Patch Management -** Aggressive update schedules

🎬 Presentation Guide

Speaking Points for Narration:

1. **Introduction (0:00-0:20)**
   - Introduce Echo Strike and Operation Digital Justice
   - Establish the hacktivist context and motivation

2. **Attack Phases (0:20-1:00)**
    - Walk through the three-phase timeline
    - Highlight reconnaissance, delivery, and impact stages
3. **Impact & Countermeasures (1:00-1:30)**
    - Emphasize the real-world damage
    - Connect to defender strategies
4. **Conclusion (1:30-1:45)**
    - Reinforce the importance of proactive security
    - Reiterate attacker type declaration

📸 Screenshots

Hero Section

> Large title "OPERATION DIGITAL JUSTICE" with glitch effect, subheading about corporate accountability, and prominent CTA button.

Attacker Profile

> Four-card grid showing MOTIVE, TACTICS, TARGET, and IMPACT in neon-accented cards with icons.

Artifacts Section

> Three realistic mock artifacts: manifesto excerpt, leaked email, and social media brag post.

Timeline

> Three-phase vertical timeline with numbered markers, detailed bullet points, and expandable details.

Countermeasures

> Five-item grid showing defensive strategies with icons and descriptions.

✅ Assignment Checklist

- [x] Single-page website created
- [x] Pure HTML, CSS, JavaScript (no frameworks)
- [x] Gen Z cyber aesthetic implemented
- [x] Dark mode with neon accents
- [x] Attacker profile (motive, tactics, target, impact)
- [x] Three realistic artifacts included

- [x] Three-phase timeline (recon → delivery → impact)
- [x] Defender countermeasures section
- [x] 150-200 word narration script
- [x] Interactive elements (smooth scroll, click events)
- [x] Responsive design (mobile & desktop)
- [x] Clean, commented code
- [x] Footer with attacker type declaration
- [x] Educational disclaimer included

🚀 How to Run

1. **Download all files:**

```
index.html
styles.css
script.js
```

2. **Ensure all files are in the same folder**
3. **Open `index.html` in a web browser:**
   - Double-click the file, or
   - Right-click → Open with → [Your Browser]
4. **Interact with the site:**
   - Click "View the Operation Timeline" button
   - Click timeline items to expand details
   - Hover over cards to see effects
   - Press 'T' key for quick timeline navigation

📚 Educational Context

Disclaimer: All data on this website is **fictional** and created solely for **educational purposes**. No real organizations, individuals, or events are depicted. This project demonstrates understanding of:

- Hacktivist motivations and tactics
- Cyber attack lifecycle (kill chain)

- Social engineering techniques
- DDoS attack mechanics
- Data exfiltration methods
- Appropriate defensive countermeasures

👨‍💻 Author Information

Student Name: [Your Name]
Course: Cyber Security Fundamentals
Assignment: Portray the Attacker - Story + Website
Submission Date: [Your Date]
Instructor: [Instructor Name]

🎓 Learning Outcomes Demonstrated

1. ✅ Understanding of different attacker types (Hacktivists)
2. ✅ Knowledge of attack lifecycle and methodologies
3. ✅ Ability to analyze attacker motivations and tactics
4. ✅ Understanding of appropriate defensive countermeasures
5. ✅ Technical skills in web development (HTML/CSS/JS)
6. ✅ Storytelling and presentation skills
7. ✅ Ethical awareness in cyber security education

📞 Contact & Support

For questions about this project:

- **Email:** [your.email@university.edu]
- **GitHub:** [github.com/yourusername]
- **LinkedIn:** [linkedin.com/in/yourprofile]

🙏 Acknowledgments

- Anthropic Claude for development assistance
- Course materials on cyber threat actors
- MITRE ATT&CK Framework for attack pattern reference
- OWASP for security best practices

📄 License

This project is created for educational purposes as part of a university assignment. All content is fictional and should not be used for any malicious purposes.

🔗 Quick Links

- Assignment Brief
- Course Homepage
- Cyber Security Resources

Last Updated: November 18, 2025

Status: ✅ Complete and Ready for Submission

🎯 FINAL SUBMISSION SUMMARY

1. URL of the Site

File Path: `index.html` (open in browser)

2. Attacker Story Script (197 words)

See "Narration for Presentation" section above

3. Attacker Type Declaration

Our attacker type is: Hacktivists

End of README