DOSSIER

ABOUT ME

Hello everyone, I am Deeptansh Nagar. I am from Kota, Rajasthan and a dedicated cybersecurity enthusiast with a focus on proactive learning and real world problem solving. Throughout my internship, I have gained hands on experience in OSINT, malware analysis, threat intelligence, and privacy technologies, while collaborating on team driven research and content creation. My strengths lie in breaking down complex technical topics into accessible, practical resources, whether through guides, case studies, or curated news digests.

I value precision, adaptability, and integrity in my work, and thrive in environments that encourage continuous learning and innovation. My goal is to contribute to advancing digital security, leveraging strong analytical skills and effective communication to make a genuine impact. Always open to new challenges, I am committed to personal and professional growth within the dynamic world of cybersecurity.

WEEKLY TASK SUMMARIES

WEEK 1 : OSINT TOOL GUIDE & DEMONSTRATION (MASTO)

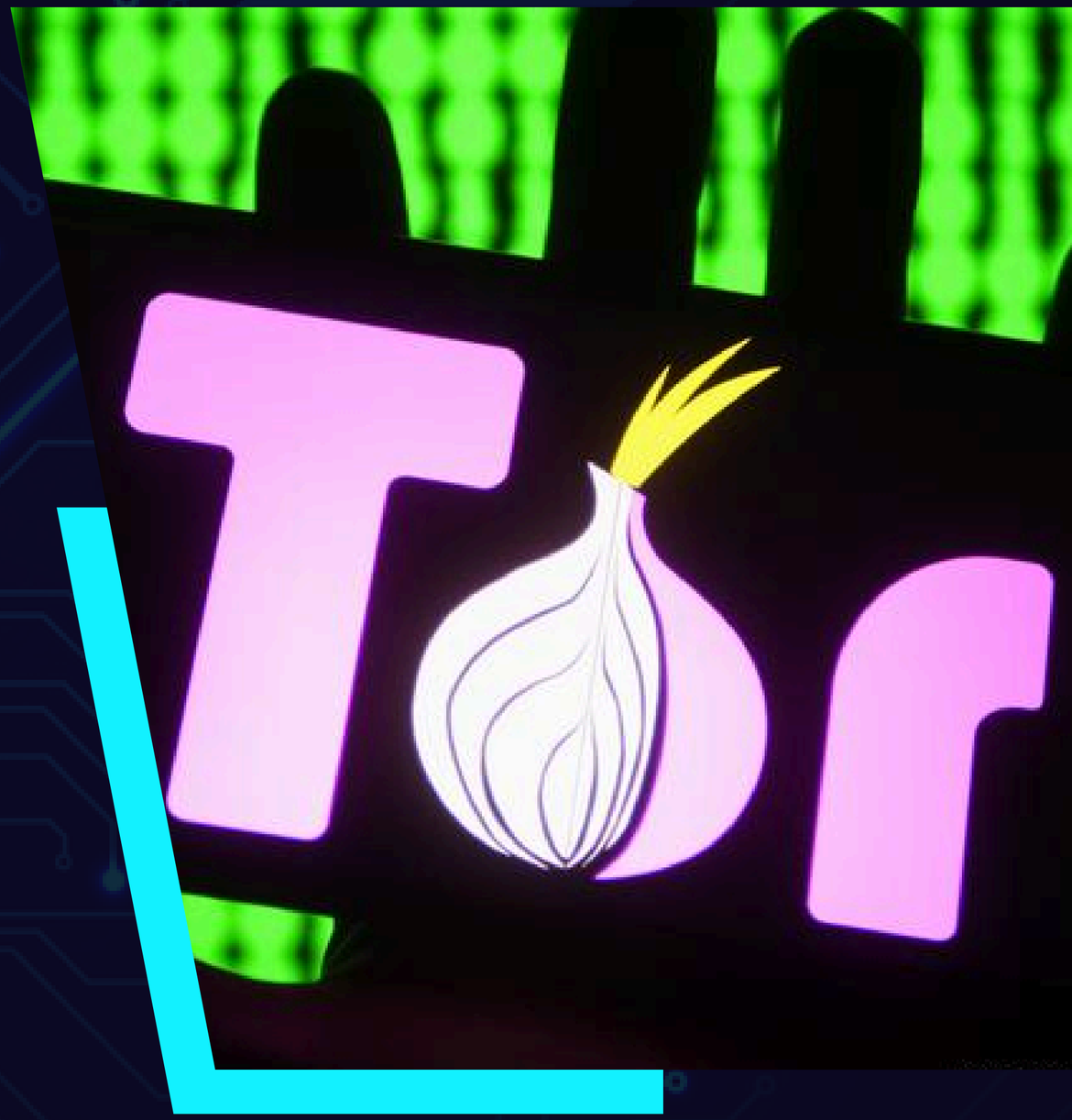
- Explored the Masto OSINT tool, focusing on its ability to gather intelligence from Mastodon and other fediverse instances without account login requirements.
- Demonstrated features such as instance information extraction, bypassing restricted profiles, and retrieving admin/user details.
- Highlighted Masto’s resolution of 401 API errors and discussed reliability improvements in version 2.0.
- My primary contribution: Leading the demonstration, scenario testing, and documenting key API constraints & outcomes.

WEEK 2: RESEARCH PAPER - DETECTION OF DOMAIN GENERATION ALGORITHMS

- Investigated the mechanics of DGAs, their challenges for defenders, and discussed static/dynamic malware analysis.
- Evaluated real world cases like the Kraken botnet and discussed advanced detection techniques (e.g., ML, real time DNS monitoring).
- Provided comparative tables of DGA types and discussed evasion strategies and organizational countermeasures.
- My key role : Analyzed machine learning applications and contributed to real-world case study summarization.

WEEK 3 : HOW TO GUIDE - USING TOR FOR ANONYMITY

- Produced a detailed guide on Tor, its installation, configuration, and safe practices for maintaining privacy and anonymity.
- Covered platform specific steps, security levels, and risks associated with misusing Tor.
- Documented practical tips and troubleshooting for diverse user scenarios.
- My individual task : Drafted Linux and macOS installation guides and best-practice recommendations.

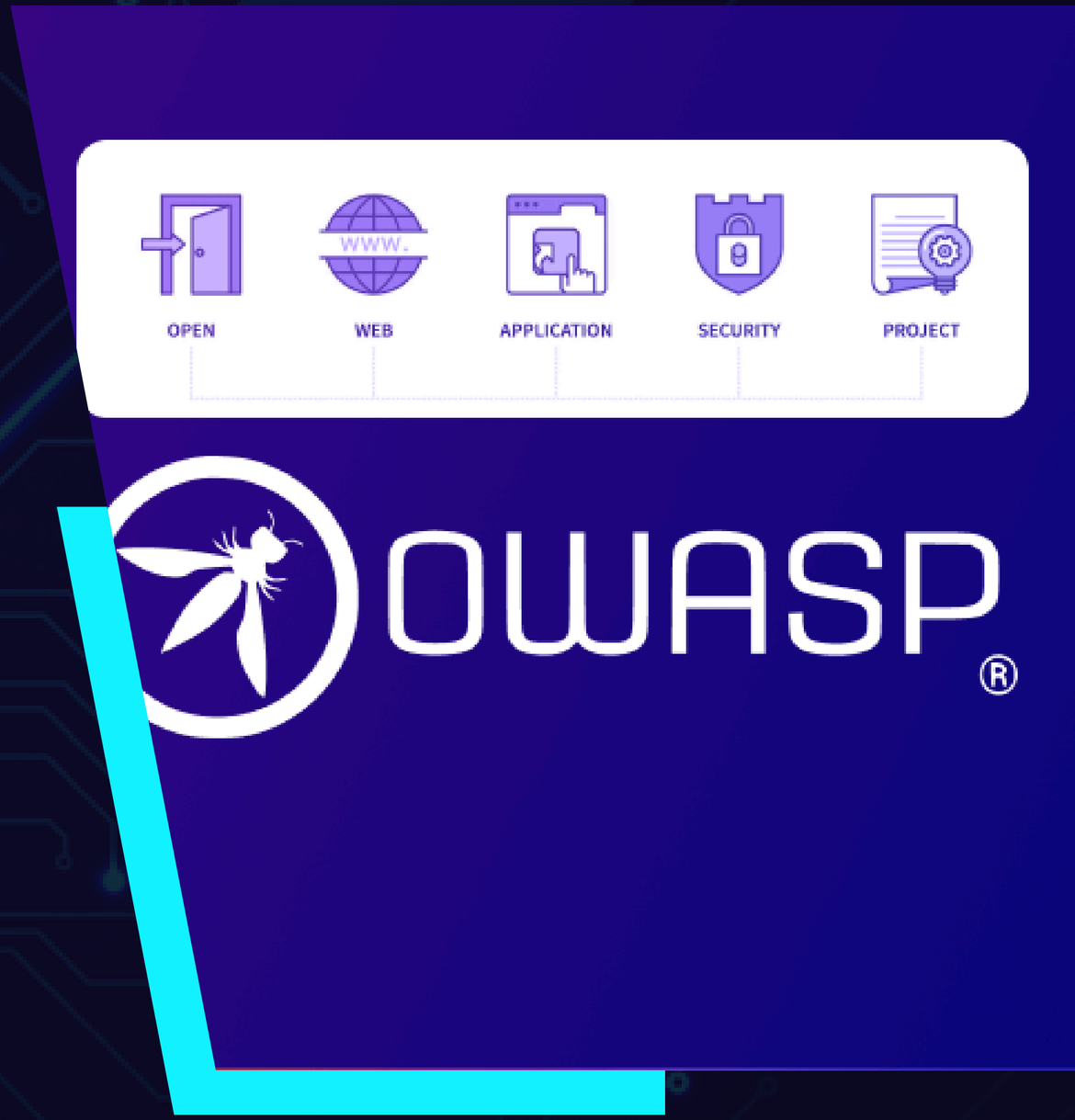


WEEK 4 : NEWS CURATION - CYBERSECURITY WEEKLY DIGEST

- Curated and summarized major global cybersecurity stories : Apple zero day WebKit exploit, LabHost phishing platform takedown, Cloudflare HTTP/2 DDoS attacks, and high profile healthcare breaches.
- Provided actionable insights on protocol vulnerabilities, AI driven email spam, and emerging trends.
- Organized weekly digest with additional reading and practical advice for organizations.
- Contribution : Researching primary stories and writing summaries, especially on AI powered threats.

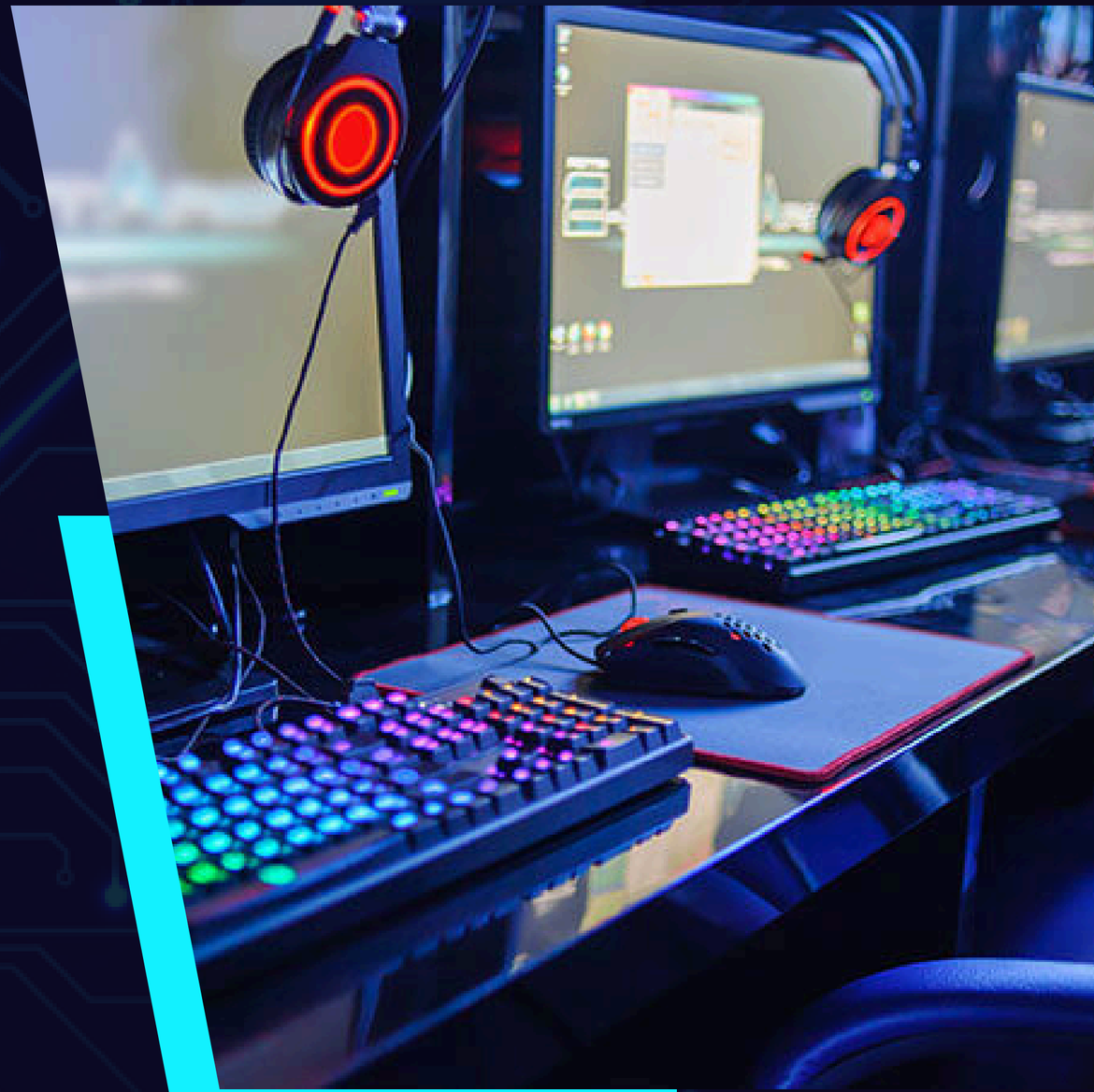
WEEK 5 : CASE STUDY - NOTORIOUS OWASP TOP 10 BREACHES

- Selected and detailed 10 of the most significant hacks mapped to OWASP Top 10 categories (e.g., Equifax, NotPetya, SolarWinds, Facebook Cambridge Analytica).
- Analyzed technical flaws, attack vectors, and mitigation lessons for each case.
- My focus : Research and writing for the Equifax and Colonial Pipeline cases, summary charts, and cross-case insights.



WEEK 6 : BLOG - OPTIMIZING SPEED & SECURITY FOR ONLINE GAMING

- Researched the impact of latency, DDoS attacks, VPN/proxy solutions, and account security in online gaming.
- Compared different cybersecurity tools and practices to enhance both gaming speed and digital protection.
- Summarized best practices for gamers and content creators.
- My input : Lead writing on proxy/VPN comparisons and actionable security recommendations.



WEEK 7 : CAROUSEL / PRESENTATION - CYBER WEAPONS NATIONS DON'T TALK ABOUT

- Developed a multi slide presentation on the covert use of cyber weapons by major nation states (e.g., US, China, Russia, Iran).
- Examined real world incidents (Stuxnet, NotPetya) and discussed future cyberwarfare trends and regulatory gaps.
- Contributed graphics, researched case examples, and led the final editing.
- Teamwork : Joint research and split of content writing, I handled the Russia/US/Israel analysis slides.

LEARNINGS & INSIGHTS

- **KEY CONCEPTS & SKILLS -**
  - OSINT and social network intelligence gathering tools.
  - Malware analysis, DNS based botnet detection, and machine learning for threat identification.
  - Installation/configuration of anonymization tools like Tor.
  - Vulnerability analysis using OWASP Top 10 as a framework.
  - Techniques for curating cybersecurity news and translating complex threats into actionable insights.
  - Communication and educational content creation (how to guides, blogs, carousels).
- **TOOLS / PLATFORMS EXPLORED -**
  - Masto (for Mastodon OSINT), PyPI package management.
  - Tor Browser on multi-OS environments.
  - Machine Learning libraries for DGA research.
  - VPN and proxy selection/comparison tools.
- **EVOLUTION OF CYBERSECURITY UNDERSTANDING -**

  My understanding shifted from purely technical perspectives to a holistic appreciation of cyber threats including global attack trends, state level offensive capabilities, and the importance of communication for both technical and non technical audiences.

SELF - EVALUATION

Area	Start of Internship	End of Internship	Comment on Improvement
TECHNICAL UNDERSTANDING	6 OUT OF 10	9 OUT OF 10	Deepened with OSINT, malware, and tool exploration.
WRITING AND COMMUNICATION	7 OUT OF 10	9 OUT OF 10	Regular content creation (guides, news digests, blogs) enhanced clarity & engagement.
RESEARCH AND ANALYSIS	6 OUT OF 10	8 OUT OF 10	Real-world case reviews and DGA research sharpened analytical skills.
COLLABORATION AND TEAMWORK	8 OUT OF 10	9 OUT OF 10	Consistent co-authoring, feedback sessions, and split presentation work.

TOP 3 TAKEAWAYS

- **COMMUNICATION IS KEY -**

  Translating complex concepts into user-friendly guides/blogs is essential for clear communication enables impact beyond technical circles.

- **CONTINUOUS LEARNING MATTERS -**

  The field is dynamic : exploring new tools, attack trends (AI powered threats, state cyber weaponary) and hands on research is vital to remain effective.

- **COLLABORATION BRINGS PERSPECTIVE -**

  Working with peers on case studies, curation, and shared deliverables led to richer insights and more robust, polished outputs.

LINKS OF MY WORK -

WEEK 1	[TOOL GUIDE]
WEEK 2	[RESEARCH PAPER]
WEEK 3	[HOW-TO GUIDE]
WEEK 4	[NEWS CURATION]
WEEK 5	[CASE STUDY]
WEEK 6	[BLOG]
WEEK 7	[CAROUSEL]

THANK YOU