MODULE 7

OSINT RECON FOR RED TEAMS AND DEFENDERS

@cybervalkyries

MODULE 7

An Overview

A quick map of what you will get:

1. A stepwise, safe OSINT workflow you can repeat.
2. A compact toolchain and when to use each tool.
3. Data handling and privacy rules you must follow.
4. Templates for recon runs, reporting, and a forensic timeline.
5. Three slow practice exercises with exact steps.

Why this module matters

Public data is fuel. It helps you map an environment, reduce noise, and prioritize follow ups. Do it ethically. Do it documented. Use what you learn to protect people and systems.

MODULE 7

Authorization

Authorization & Scope

Step 1. Before you run anything, get written permission. Put the scope in plain language. Who, what, where, and when. Save that file.

Step 2. Define the allowed sources. Public profiles, corporate domains, public archives. No private data. If a source requires login, stop and get explicit approval.

Step 3. Record who authorized this. Name, role, contact, and a signature or email timestamp. Keep that in your experiment folder.

Why This Matters

OSINT can accidentally cross legal boundaries. Permission reduces risk for you and your stakeholders.

MODULE 7

Minimal Toolchains

What To Know:

- Browser profile. Use a fresh, disposable browser profile or a controlled VM. Do not log into your personal accounts.

- Passive discovery feeds. Public search engines and archived pages. The Wayback Machine remains a primary archive to check historical content. Use it for historical snapshots only.

- Domain and infrastructure lookups. Tools that inspect certificates, exposed services, and public host metadata are useful for mapping assets. Use them to form hypotheses, not to attack.

- Mail and DNS validators. For email infrastructure understanding use validators that show SPF, DKIM, DMARC, and MX details. These help defenders fix email security.

- Metadata extraction tools. Use them for public documents only. They find server names, user names, and version strings in files that are explicitly public.

MODULE 7

Lab and Privacy Rules

Rules You MUST Follow:

- Never harvest data behind authentication without explicit permission.
- Never aggregate or publish identifying private data. If you collect sensitive material by accident, stop and notify the authorizing party.
- Keep raw data encrypted at rest. Work on copies. Keep checksums.
- Anonymize outputs you share outside the authorized team.

MODULE 7

Recon Workflow Overview

This is slow and repeatable

1) Intake and context.
2) Surface mapping.
3) Public profile analysis.
4) Infrastructure and metadata checks.
5) Synthesis and reporting.

Intake and Context

Step 1. Record scope and permission. Paste the signed scope into your experiment folder.

Step 2. Add a short goal. It should be one sentence.

- *For example:* map public domains and find external email policy gaps.

Step 3. List red lines.

- *For example:* no scraping of private groups, no login attempts.

MODULE 7

Surface Mapping

Step 1. Passive domain checks. Use passive DNS, certificate transparency logs, and public registries to list subdomains and related domains. Use community-reviewed tools only. Cyble is a great resource.

Step 2. Archive checks. Query web archives for historical pages and deleted content. Note dates and exact URLs. Use the archive as a historical source, not evidence of current content.

Step 3. Public repo and paste site sweep. Search public code repositories and paste sites for accidental secrets in public code. Do not interact with or download private content. When you find sensitive items, mark them and follow the disclosure process.

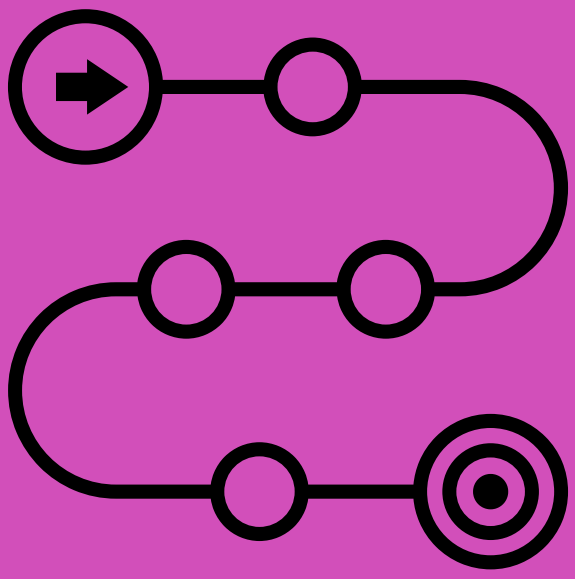
MODULE 7

Public Profile Analysis

A Step by Step Outline

Step 1. Map public profiles for named people on LinkedIn, GitHub, Twitter or similar public platforms. Document job titles, public projects, and contact channels. Keep only what is public and non-sensitive.

Step 2. Note patterns. Does an employee reuse an email handle? Does a username recur on other services?
Ask yourself these type of questions. This helps defenders reduce attack surface.



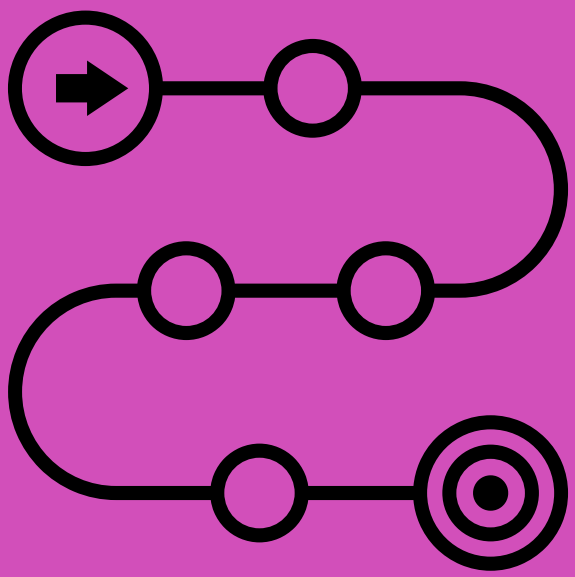
MODULE 7

Infrastructure & Email Checks

A Step by Step Outline:
Exact Actions You Can Run In Labs

Step 1. Look up MX, SPF, DKIM, DMARC publicly. Use a validator to read the records and record policy strength. These checks are read-only and safe.

Step 2. Gather TLS certificate history via public certificate transparency logs. Note IPs, hostnames, and issuers. This helps map legacy assets.



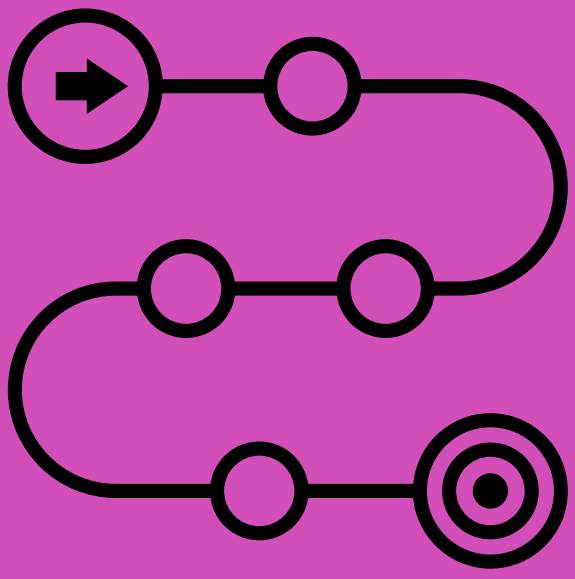
MODULE 7

Synthesis and Reporting

A Step by Step Outline:

Step 1. Build a short findings summary. One paragraph describing risk and recommended next steps.

Step 2. Create a prioritized list of items to remediate with estimated impact and ease. Keep the language non-technical for business stakeholders.

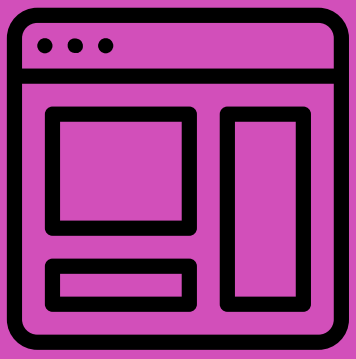


MODULE 7

Templates

Recon Run Header

Target:
Scope:
Authorized by:
Goal:
Start date:
End date:
Red lines:
Notes:



Data Capture Log

Filename, source, timestamp, short note, checksum
example: companysite-wayback-2025-07-01.html, Wayback Machine, 2025-07-01T12:03Z, archived homepage, sha256:...

Findings summary template

One line summary:
Evidence snapshots used:
Top risk 1: short description and recommended fix
Top risk 2: short description and recommended fix
Next steps: test after remediation, timeline, owner

MODULE 7

Practical Exercises

Exercise 1.
Passive domain mapping,
step-by-step

- Step 1. Create a new browser profile or use a recon VM.
- Step 2. In your recon folder, create the Recon run header and fill it.
- Step 3. Query passive DNS and certificate logs for the domain in scope. Save the returned JSON or textual output to your folder.
- Step 4. Use an archive checker to fetch historical front pages for the main domain and note any subdomains found in archived content. Save the snapshots.
- Step 5. Produce a one-paragraph summary that lists new or forgotten assets that need attention.

MODULE 7

Practical Exercises Continued

Exercise 2.
Public document metadata read, step-by-step

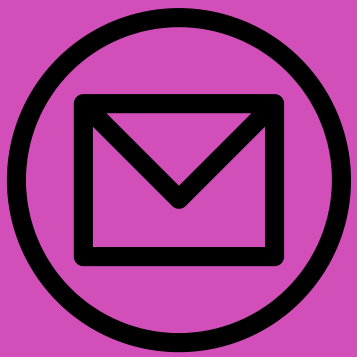
- Step 1. Pick a publicly posted PDF on the target domain or from a public press release. Confirm it is public.
- Step 2. Run a metadata extractor on a copy of the file. Save the metadata output to the experiment folder.
- Step 3. If the metadata contains internal hostnames or emails, redact those in your working copy and notify the authorized team. Do not publish the raw metadata.
- Step 4. Write a short note with recommended actions to sanitize future public documents.

MODULE 7

Practical Exercises Continued

Exercise 3.
Email configuration assessment, step-by-step

- Step 1. Use a public DMARC/SPF/DKIM validator on the target domain. Save the validator output.
- Step 2. Note whether DMARC is enforced or in monitor mode. Note SPF scope and DKIM presence.
- Step 3. Produce a one-page guidance note that explains how enforcing DMARC can reduce phishing. Keep it simple and actionable.



MODULE 7

Handling Sensitive Information

If you encounter private data you did not have permission to access, follow these steps immediately.

- Step 1. Stop collecting. Save a minimal note with date and time. Do not copy or download the data further.
- Step 2. Notify the authorizing contact with the evidence you are allowed to share. Use secure channels.
- Step 3. If legal counsel is available, involve them. Follow the reporting procedure you set at intake.

*OSINT best practice guidance and professional standards emphasize **transparency, privacy, and legal defensibility.** Follow recognized guidance for ethical collections. For a general overview of ethical concerns and professional practice, see recent discussions and guidance by industry and standards groups.*

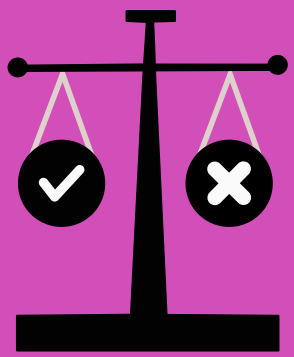
MODULE 7

More Information

Packaging outputs for defenders and stakeholders

- Keep raw outputs in an encrypted archive. Keep checksums.
- Deliver sanitized summaries to product teams and executives. Use plain language.
- Add a short remediation prioritization table. Make it two columns: impact and effort.

- **Common Mistakes & How to Avoid Them**
- Mistake: logging in with your main account.
  - Fix: use disposable browser profiles or VM.
- Mistake: saving raw scraped data unencrypted.
  - Fix: encrypt and checksum.
- Mistake: jumping from passive to active without permission.
  - Fix: stop and get approval.



MODULE 7

Sample Mini Run

From Start to Finish

Recon header

Target: examplecorp.com
Scope: public web pages and public code repos only
Authorized by: securitylead@examplecorp.com, email timestamp 2025-07-10T09:14Z
Goal: map public subdomains and email auth posture and produce prioritized fixes
Start date: 2025-07-10

Actions taken

Passive DNS query saved as passive-dns-examplecorp.json
Wayback snapshots saved for 2019 and 2023 homepages.
DMARC validator output saved as examplecorp-dmarc.txt.

Findings short sample

Found legacy subdomain legacy.examplecorp.com in an archive. Impact medium. Remediate by removing DNS entry and adding redirect.
DMARC is in monitor mode. Impact high for phishing risk. Recommend enforce policy and add monitoring.

MODULE 7

Further Reading

Further reading and living lists

Curated lists and periodic roundups help you stay sharp. Refer to curated community lists for tool updates and to industry posts for ethics guidance. These resources collect open source tools and explain common OSINT methods.