CTF Report Structure

A Comprehensive Guide to Writing CTF Reports

Naveen Bassi

2024-October

Contents

Preamble

This is a blueprint I followed for the CTF-style lab work we had at MITT during my time as a Network Security student at PACE UoW. This guide is organized into several sections, which serve as guidance on how and where to store certain data and to assist in managing time, as well as being efficient and organized during actual engagements. This document provides a procedure to follow as well as a skeleton folder structure to aid your work.

You are free to follow the headers as is. Their descriptions should provide explanations of what is expected in them. It is up to your requirement whether to omit or add content.

> Please add a star on **GitHub/nav33nb/ctf-report** if you find this helpful.

```
 1  ## Root Directory
 2  ReadMe.md        # Main document outlining the process
 3  scans/           # Contains results from various scans
 4      nmap/
 5      feroxbuster/
 6      nikto/
 7  exploit/         #  Exploit information for each service
 8      service1/
 9      service2/
10      service3/
11  loot/            # Gathered information from target hosts
12      192.168.X.X_file1
13      192.168.X.X_file2
14      192.168.X.X_file3
15  pdf/             # Holds generated PDF reports
16      ReadMe_default.pdf
17      ReadMe_eisvogel.pdf
18  img/             # Holds screenshots and imgs
19      img1.png
20      img2.png
```

Usage & Report Generation

Report can be generated to a PDF via Pandoc. See Pandoc - https://pandoc.org/. Pandoc uses LaTeX templates to convert Markdown to PDF. Markdown provides the content and its structure, while LaTeX provides the style. As long as you have a template, the same Markdown source can be formatted in multiple ways. See some examples under `pdf`/.

```
 1  # Step 1: Clone the repository
 2  git clone https://github.com/nav33nb/ctf-report.git
 3
 4  # Step 2: Update the ReadMe file with your findings
```

```
 5  code ReadMe.md # or any editor of your choice
 6
 7  # Step 3: Install the build requirements
 8  sudo apt-get install \
 9      pandoc \
10      texlive-latex-base \
11      texlive-fonts-recommended \
12      texlive-extra-utils \
13      texlive-latex-extra
14
15  # Step 4: Run Pandoc to convert Markdown to PDF (or other formats)
16  pandoc \
17      --from markdown ReadMe.md \
18      -o ReadMe_default.pdf
19
20  # Step 5: (Optional) Use a custom template, such as Eisvogel
21  # See: https://github.com/Wandmalfarbe/pandoc-latex-template
22  # To use the custom template, run the command like this:
23  # Note that custom templates come with their own dependencies
24  pandoc \
25      --from markdown ReadMe.md \
26      -o ReadMe_eisvogel.pdf \
27      --template eisvogel \
28      --listings
```

1. Introduction

Introduce yourself, your team, the context, and the setting of the engagement. Discuss the duration, environment, and context of the report.

2. Lab Setup / Briefing

- Explain the high-level lab setup, describe your network, and your perspective on the target.
- Explain the target scope, their network, and known information (if any).
- Explain your choice of VM, tools, and any other decisions made before engaging.
- Code Blocks are an effective way to establish facts, show results and present exact information

Figure 1: Add figures and their description like this, pandoc will auto assign a number. Place screenshots under `img`/

```
1  // Network Information
2  // CAN ALSO SHOW THIS VIA CLI SCREENSHOT
3  SELF   - <NETWORK-CIDR-HERE>
4  TARGET - <NETWORK-CIDR-HERE>
```

3. Assumptions and Scope Considerations

In this section share assumptions and scope that you've agreed to before the engagement. Some possibilities to discuss here are:

- What is the target network, target domain, and in-scope items?
- Is there a target hint or service shared by the instructor as a starting point?
- Are you supposed to search for a FLAG or KEY? How will it be identified?
- What is the objective: compromising the machine or exploring multiple attack vectors?

4. Initial Enumeration and Host Discovery

In this section start discusing actual engagement process with the target. Some possibilities to discuss here are:

- Example, if you run a ping sweep to discover active hosts and discuss the findings. Save the results to `-oN scans/nmap/init-hosts.nmap`.
- Run an initial scan and save the results to `-oN scans/nmap/init-scan.nmap`.
- *If feasible at this stage, run more advanced scans. Each result should be saved under `-oN scans/nmap/SCANTYPE.nmap`.*

```
1  // PRESENT YOUR FINDINGS, SHOW ACTIVE HOSTS
2  192.168.X.X      192.168.X.X
3  192.168.X.X      192.168.X.X
4  192.168.X.X      192.168.X.X
5  192.168.X.X      192.168.X.X
6  192.168.X.X      192.168.X.X
7  ... and so on
```

5. Scope Reduction / Discussion

In this section discuss your results from previous section. When dealing with a NETWORK CIDR RANGE, there are expected to be multiple positives. Showcase your findings in reducing your scope to one or two high-value targets.

- Provide details if there are multiple hosts that were found active and responding.
- Reduce the scope, discuss and filter out targets not aligning with the assumptions; provide reasons.
- Reduce the scope, perform manual enumeration, and discuss any techniques or tools used.
- Reduce the scope by performing some preliminary discovery using tools. Show your work and provide screenshots. Prefer keeping results organized. For example,

    - `scans/TOOL/HOST.txt`

BY THIS POINT, YOU'VE LIKELY DISCOVERED THE TARGET.

6. Targeting the Host

In this section, once the target is discovered, discuss and switch to specific host targeted approaches. Some possibilities are:

- Performing service enumeration like Nmap script scans

    - save the output to `-oN scans/nmap/192.168.X.X.nmap`.

- Perform variations like aggressive scan, if feasible

- save it accordingly to `-oN scans/nmap/192.168.X.X_aggressive.nmap`.

- Discuss your findings and the open services, and provide screenshots.
- You can also Perform manual enumeration and discuss the services:

  - If it's a web service, what kind is it? What port (HTTP/HTTPS)? What type of service (store, blog), etc.?
  - If it's FTP, does it require a password? Are there any open shares, etc.?
  - … and so on.

- Perform service enumeration. Any results and information gathered should be accordingly stored under specific folders, like so:

  - `scans/gobuster/192.168.X.X.txt`
  - `scans/feroxbuster/192.168.X.X_extrainfo.txt`
  - `scans/nikto/192.168.X.X.txt`
  - … and so on.

```
1  // PROVIDE NMAP RESULT HERE IN THE REPORT
2  Nmap scan report for 192.168.X.X
3  Host is up (0.00064s latency).
4  Not shown: XYZ closed TCP ports (conn-refused)
5  PORT   STATE SERVICE VERSION
6  service1
7  service2
8  service3
9  ... and so on
```

7. Exploitation

7.1. Service 1

In this section discuss a specific service in detail. Discussion should attempt to poke at issues with the service. Some possibilities to discuss are:

- What is this service? What does it do?
- What port is this service running on? Is it the usual port? Do you gain any information from this?
- Can you perform some manual enumeration here? Provide some screenshots.
- Do you know the service version?

  - Is it the latest version or is it outdated?
  - Is it vulnerable? Are any exploits available?

- Discuss vulnerabilities and exploits for this service. Provide screenshots and store exploit artifacts under `exploit`/`service1`/:

    - What is the exploit?
    - What versions are affected by it?
    - What should the exploit allow us to do?
    - How is the exploit available? For example, through `exploit-db`, through `metasploit`, etc.
    - Show any configuration needed to run this and execution, and provide screenshots.

- What kind of access do you gain through this exploit?

    - If it is a user shell, what more information can you gain from this? Discuss approaches for discovery.
    - Discuss how gathered information from a restrictive shell may be used; provide screenshots.
    - Can you find ways to elevate privileges to a root shell and compromise the machine?

- Rediscuss assumptions and look for FLAGS.

7.2. Service 2

Perform similar analysis for Service 2. Depending on the context of engagement, you may have to exploit each service individually to showcase multiple attack vectors or gather intelligence from multiple services to compromise the host.

7.2.1. Sub-technique

- Use subheadings like this to discuss sub-techniques used for specific services.
- Sometimes, some techniques have exploits that require changes due to deprecation or code changes. Research and provide explanations, and use code blocks to highlight any changes made.
- Discuss findings and provide screenshots.

```
1  // USE CODE BLOCKS TO HIGHLIGHT
2  // CHANGES MADE TO SCRIPTS OR CODE
3
4  fmt.print("Hello World")
5  // changed to
6  fmt.print("Hello Friend")
```

7.3. Service 3

Follow the same logic.

7.3.1. Sub-technique

- Any findings you make must be stored under `loot`/. This can be credentials, db dumps, users and passwd files, shadow files, credentials, or any other sensitive information.

    - `loot`/192.168.`X.X_file1`
    - `loot`/192.168.`X.X_file2`
    - ... and so on

7.3.2. ... and so on

8. Conclusion

In this section you will bring together the main points of report. Note below:

- The conclusion should add nothing new; only reiterate the main points from the above report.
- What did you do? What were the assumptions?
- How did you target each service, and what were the main findings?
- Any extra actions performed, such as processing loot, password cracking, privilege escalation, enumeration, and tools used?
- Wrap up and highlight the main issues.

8.1. Tools & Techniques Showcased

In this section discuss the various tools you used during the engagement and in what capacity they were used.

- nmap - Host discovery, service enumeration
- *TOOL 2 - HOW YOU USED IT*
- *TOOL 3 - HOW YOU USED IT*
- ... and so on

8.2. Results

In this section concisely discuss Line-by-line issues with their potential exposure and risks.

- *ISSUE 1 PRESENT, EXPLOITED USING [TECHNIQUE], RESULTED IN [EXPOSURE AND OUTCOME]*
- *ISSUE 2 PRESENT, EXPLOITED USING [TECHNIQUE], RESULTED IN [EXPOSURE AND OUTCOME]*

    - *SUBISSUE 2 CAUSES [FURTHER EXPOSURE]*

9. Recommendations

In this section discuss how you understand each issue, and what recommendation do you offer for fixing each issue?

- *IT IS RECOMMENDED FOR ISSUE 1 THAT [FIX TO BE DONE]*
- *IT IS RECOMMENDED FOR ISSUE 2 THAT [FIX TO BE DONE]*

    - *IF NOT FIX REDUCE EXPOSURE BY [FIX TO BE DONE]*
    - *SOME SUB ISSUE DISCUSSED*

- … and so on

10. References

1. Kali Linux Documentation
2. Network Mapper Reference Guide
3. … and so on