INFORMATION GATHERING AND RECONNAISSANCE WITH AI

Harnessing Artificial Intelligence for Penetration Testing

GATHERING INFORMATION

- Gather Information
  - Collecting Information about a Target's Digital Environment to Understand its Vulnerabilities
  - Network Topology
  - System Strengths and Weaknesses
  - Identifying Possible Entry Point
- Scanning
- Exploitation
- Maintaining Access
- Covering Tracks
- Reporting and Documentation

GATHERING INFORMATION

traditional methods

- Open Source Intelligence (OSINT)
- WHOIS Lookup
- Social Engineering
  - “psychological manipulation of a person to get useful and sensitive information from them” [1]

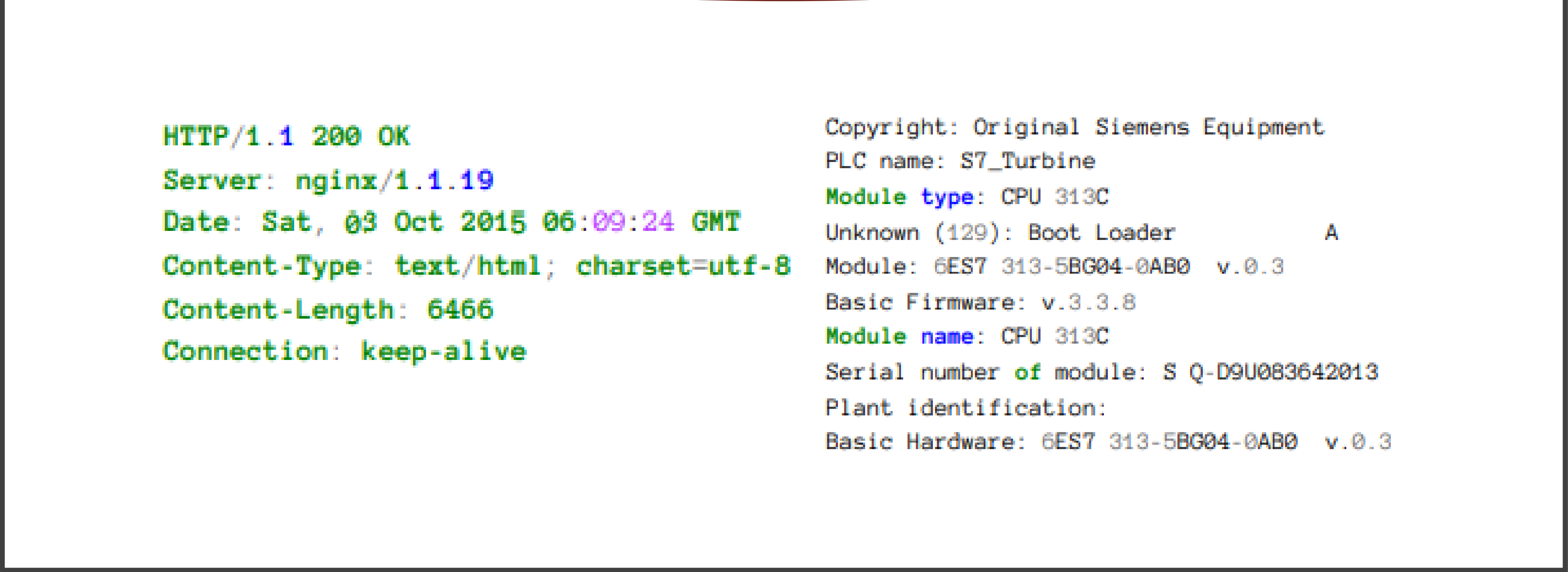
GATHERING INFORMATION

Importance of AI

- Automated Data Collection
- Data Processing
- Data Analysis and Interpretation
  - Natural Language Processing
- Predictive Analytics
- Machine Learning for Target Profiling

AI Tools for Gathering Information

Shodan



```
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader           A
Module: 6ES7 313-5BG04-0AB0  v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0  v.0.3
```

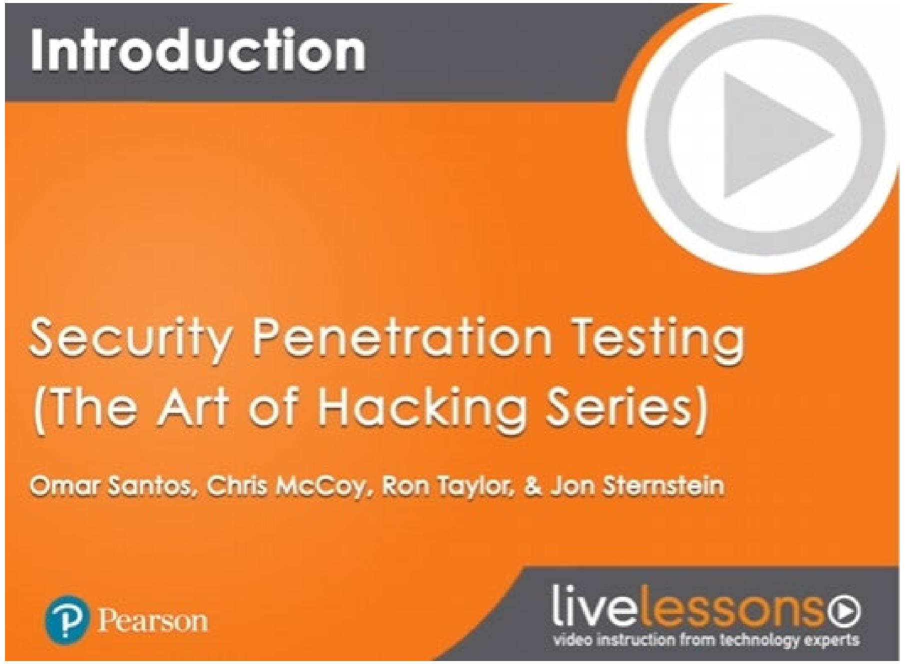
AI Tools for Gathering Information

nmap

- Nmap (with AI plugins)
- Nmap Scripting Engine (NSE)
  - 12 Useful NSE scripts: https://research.securitum.com/nmap-and-12-useful-nse-scripts/
  - Extensive script list: https://secwiki.org/w/Nmap/Script_Ideas

AI Tools for Gathering Information

o’reilly course



Introduction

Security Penetration Testing (The Art of Hacking Series)

Omar Santos, Chris McCoy, Ron Taylor, & Jon Sternstein

Pearson

livelessons

video instruction from technology experts

Lesson 4: Reconnaissance and Profiling Web Applications

4.3 Exploring Shodan, Maltego, Recon-NG, SpiderFoot, and TheHarvester

Pearson

livelessons

video instruction from technology experts

RESEARCH QUESTION

What are some creative challenges that real-world applications of these tools could help solve?

REFERENCES

1) C. Chebbi, Mastering Machine Learning for Penetration Testing, Packt Publishing, 2018.

2) J. Matherly, Complete Guide to Shodan, Leanpub, 2016.

3) N. Kühl, M. Schemmer, . M. Goutier and G. Sat, Artificial intelligence and machine learning, 2022, pp. 2235-2244.

4) S. Watts , Penetration Testing: Practical Introduction & Tutorials, 2022.

5) A. AlMajali, L. Al-Abed, R. Mutleq, Z. Samamah, A. A. Shhadeh, B. J. Mohd and K. M. Ahmad Yousef, "Vulnerability Exploitation Using Reinforcement Learning," in Jordan International Joint Conference on Electrical Engineering and Information Technology, Amman, 2023.

6) S. Morgan, 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics, Sausality, California, 2023.