EUROPEAN CYBERSECURITY CHALLENGE 2018

SKILLSET OVERVIEW

(draft)

INTRODUCTION

The following document provides an overview of the skills needed to perform the technical and non-technical tasks associated with the ECSC2018 final. In particular, this document offers a good indication of the type of technical tasks participants are expected to solve during the event.

The list is not intended to be exhaustive and should be used is conjunction with the more general **ECSC Curricula**. The ECSC Curricula offers a complete list of resources, such as articles and books, which can be used by coaches and teams during their preparation for the London final.

TEHNICAL SKILL SETS

1. Participants are expected to be familiar with concepts related to the fundamentals of penetration testing, such as enumeration of targets and services, exploitation and post-exploitation techniques;
2. Participants are expected to be capable of writing simple scripts to assist them during the penetration testing process;
3. Participants are expected to be capable to perform a variety of remote client and server side attacks;
4. Participants are expected to be familiar with the details of OWASP Top 10 Most Critical Web Application Security Risks and ways in which these risks can be identified and assessed, in particular, be familiar with recent exploits and vulnerabilities that affect well known content management systems (CMS);
5. Participants are expected to be familiar with the usage of specialised tools, such as network scanners, web application scanning and fuzzing tools, exploitation frameworks, etc.
6. Participants should be familiar with writing basic custom exploits (*stack buffer overflow*);
7. Participants should be familiar with common attack patterns, such as drive by downloads, watering hole attacks, etc.
8. Participants should be familiar with the usage of common debuggers, such as *gdb* or *windbg;*
9. Participants should have a good understanding of basic concepts related to reverse engineering of binary executables (*ELF* and/or *PE* files);
10. Participants should be familiar with common anti-debugging techniques;
11. Participants should be familiar with common Linux commands and tools (for e.g. *grep, cut, sed*);
12. Participants should have knowledge of some online blockchain explorer;
13. Participants should be familiar with classic ciphers (*ROT*, *Bacon*, *Transposition*, *Substitution,* etc.);
14. Participants should be familiar with basic attacks against modern cryptographic primitives and protocols;
15. Participants should be familiar with common encoding and decoding schemes;
16. Participants are expected to have a good understanding of common Operating System misconfigurations;
17. Participants should be familiar with basic deobfuscation techniques and tools (for e.g. *php* and *javascript* deobfuscation);
18. Participants should be familiar with common forensics techniques and tools (file carving, Windows Registry forensics, memory forensics, file recovery techniques etc.);
19. Participants should be familiar with log analysis (for e.g. *syslog,* Windows *Event Log,* webserver log formats);
20. Participants should be familiar with common network analysis tools and techniques (for e.g. be familiar with *tcpdump* and/or *Wireshark*);
21. Participants should be familiar with basic tools and decompiling techniques used for analysing Android applications;
22. Participants should be familiar with basic steganography tools and techniques (e.g. *Steghide*, *stegcracker*);

SOFT SKILLS

1. Participants are expected to have excellent drafting and documenting skills;
2. Participants are expected to be able to explain complex information security risks to technical and non-technical audiences;
3. Participants are expected to have excellent presentation skills;
4. Participants are expected to have excellent time management and decision making skills;
5. Participants are expected to have good negotiations skills;
6. Participants are expected to have excellent task and team management skills;

READING RESOURCES (INDICATIVE)

1. OWASP Top 10 Most Critical Web Application Security Risks
2. The Art of Memory Forensics
3. Rtfm: Red Team Field Manual
4. Metasploit: The Penetration Tester's Guide
5. Penetration Testing: A Hands-On Introduction to Hacking
6. Violent Python
7. Serious Cryptography
8. Nmap 6 Cookbook
9. Kali Linux Revealed

TRAINING RESOURCES (INDICATIVE)

ENISA's free training resources, such as:

- ENISA's Artefact analysis fundamentals
- ENISA's Advanced artefact handling
- ENISA's Forensic analysis: Network Incident Response
- ENISA's Forensic analysis: Webserver Analysis
- ENISA's Introduction to advanced artefact analysis
- ENISA's Dynamic analysis of artefacts
- ENISA's Static analysis of artefacts
- ENISA's Network forensics
- ENISA's Mobile threats incident handling