FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ ústav telekomunikací

Informační bezpečnost

Zadání semestrálního projektu předmětu

Bezpečnost ICT 1 (BPC-IC1)

v akademickém roce 2021/2022

1. Cíle projektu:

Semestrální projekt je zaměřen na osvojení si základů softwarových zranitelností a jejich exploitace. Cílem semestrálního projektu je **nastudovat a prakticky demonstrovat vybrané bezpečnostní zranitelnosti**.

Projekt je řešen ve skupině o třech studentech. Každá skupina implementuje vlastní zranitelnou aplikaci obsahující alespoň tři softwarové zranitelnosti. Student může kombinovat nízkoúrovňové (Low level) i vysokoúrovňové (Hight level) zranitelnosti, viz např. výčet níže:

- Low level:
  - Integer overflow
  - Stack overflow
  - String format
  - Heap overflow (pokročilé)
  - ROP (Return-Oriented Programming) (pokročilé)

- High level:
  - Path hijacking
  - SUID/GUID oprávnění
  - SUDO miskonfigurace (find, cat, more, ENV, apod.)
  - Python library hijacking (https://medium.com/analytics-vidhya/python-library-hijacking-on-linux-with-examples-a31e6a9860c8)
  - Linux capabilities (getcap) (https://hackmag.com/security/linux-privileges-escalation/)
  - Cron + weak permissions (https://hackmag.com/security/linux-privileges-escalation/)
  - Password extracting / Password cracking

Výstupem projektu bude vlastní aplikace (*psaná v C*) kombinující některé vybrané bezpečnostní zranitelnosti (*např. buffer overflow, integer overflow, format string apod.*). Aplikace bude obsahovat minimálně tři vybrané zranitelnosti z toho alespoň jednu z kategorie Low level. Avšak, čím více bude zranitelností implementováno, tím lépe. Exploit bude psán v jazyce Python.

Doporučená literatura, materiály:

- Laboratorní cvičení a přednášky kurzu Bezpečnost ICT 1
- Online dokumenty zabývající se exploitací, viz např. zdroje:
  - https://exploit.education/ (řešení https://blog.lamarranet.com/)
  - https://ironhackers.es/en/tutoriales/introduccion-al-exploiting-parte-1-stack-0-2-protostar/
  - https://es.slideshare.net/saumilshah/how-functions-work-7776073
  - https://ctf101.org/

2. Registrace zadání:

Registrace projektů je otevřena od **08.03.2022**. Každá skupina si registruje své téma online na odkazu níže (přístup přes VUT login):
https://docs.google.com/spreadsheets/d/1rgbfOShKcIG_CQXTB0ZXbcIgsEoWF5yW2IncsT7Nny0/edit#gid=0.

3. Výstupy semestrálního projektu:

1.) **Prezentace k projektu:** o délce 7-10 minut. Studenti představí svůj projekt (prezentace PowerPoint, PDF) a prakticky demonstrující funkčnost a exploitaci své aplikace pomocí vytvořené videoukázky, kterou okomentují.
2.) **Videoukázka:** demonstrující funkčnost aplikace a její exploitaci. Videoukázka je součástí prezentace.
3.) **Technická dokumentace:** popisující účel a funkcionalitu vytvořené aplikace, potřebný SW/HW, instalační a uživatelský manuál (*rozsah 2-3 normostrany*).

4. Odevzdání projektu:

Odevzdání projektu (*technická dokumentace, videoukázka, zdrojové kódy*) bude provedeno online na odkazu https://drive.google.com/drive/folders/1VxcQ-f6SZuM4Ta49lyTbZ_K-j2_es4ln?usp=sharing a to do adresářem s číslem skupiny a názvem projektu, např. **LL00-HackExGame**. **Odevzdání projektu provede pouze jeden člen týmu, a to nejpozději do 12. týdnu semestru (do 26. 04. 2022)**.

5. Prezentace projektu:

Prezentace projektů proběhne ve 12. a 13. týdnu v rámci laboratorních cvičení, tj. 27. – 28. 04. 2022 a 04. – 05. 05.2022.

6. Hodnocení projektu:

Projekt je hodnocen jako celek maximálně 15-ti body. Hodnocena bude:

1.) kvalita zpracovaní semestrálního projektu, tj. aplikace a exploitu,
2.) kvalita ústní prezentace výsledků a jejich demonstrace,
3.) formální zpracování prezentace a technické dokumentace.

7. Struktura dokumentace a prezentace:

Odevzdaná technická dokumentace musí splňovat náležitosti technického dokumentu (**psát spisovně a v trpném rodě**). Rozsah dokumentu je stanoven na 2-3 normostrany. Šablona (MS Word) technické dokumentace je umístěna v Elearningu. Seznam použitých zdrojů, včetně použitých externích kódů a knihoven musí být v práci citován.

Petr Dzurenda

Digitally signed by Petr Dzurenda
Date: 2022.03.08 11:16:13 +01'00'

Ing. Petr Dzurenda, Ph.D.
dzurenda@vut.cz
08. 03. 2022