FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ | ústav telekomunikací

Informační bezpečnost

Zadání projektu předmětu

Bezpečnost ICT 1 (BPC-IC1)

v akademickém roce 2019/2020

Cílem projektu je najít, popsat a prakticky demonstrovat ve virtualizačním prostředí útok na zvolený operační systém (Windows, Linux, macOS, Android, iOS apod.) využívající veřejně známou bezpečnostní slabinu/zranitelnost.

1. Požadavky na realizaci útoku:

1. **Bezpečnostní slabina/zranitelnost** může být způsobena implementační chybou či vlastností softwaru spuštěného na OS či samotným OS.
2. Bezpečnostní slabina/zranitelnost musí být **realizovatelná na systému starším ne více než 5 let**.
3. Verze OS či distribuce systému, stejně jako nainstalovaná oficiální uživatelská aplikace (Skype, MS Office apod.) či služba (SSH, Samba, doménový řadič, apod.) je volitelná. Instalace aplikace útočníka není povolena.
4. **Jedná se o lokálně či síťově vedený útok**, a to bez aktivní spolupráce oběti s útočníkem.
5. Virtualizované bude celé testovací prostředí, tj. strana oběti, útočníka atd. Jako virtualizační nástroj bude využit **Oracle VM VirtualBox**.
6. Je možné využívat cizí knihovny a zdrojové kódy (*např. exploity*). Je však zakázáno využívat knihovny implementující a automatizující celý útok (*např. Metasploit*).

2. Výstupy semestrálního projektu:

1. **Vytvoření laboratorní úlohy** demonstrující útok na operační systém využívající veřejně známou bezpečnostní slabinu/zranitelnost (*např. formou **Capture the Flag**, **Red Team Versus Blue Team***) v prostředí VirtualBox.
2. **Vytvoření návodu** k laboratorní úloze včetně zadání a postupu: max. **5 stran formátu A4**.
3. Prezentace postupu řešení a dosažených cílů:

   a. PREZENTACE 1: 7. týden: **Popis postupu řešení:**
   Popis cílů laboratorní úlohy.
   Popis bezpečnostní slabiny a samotného útoku nejlépe dle formátu CVE.
   Současný stav řešení (*např. vytvořená infrastruktura, naprogramované aplikace, aktuální fáze vypracování laboratorní úlohy apod.*)

   b. PREZENTACE 2: 13. týden: **Dosažené výsledky a zhodnocení:**
   Demonstrace útoku ve virtualizovaném prostředí (*videoukázka*).

3. Hodnocená budou tato kritéria:

1. Funkčnost úlohy ve virtuálním prostředí.
2. Kvalita zpracování laboratorní úlohy a návodu k laboratorní úloze.
   (*např. srozumitelnost, funkčnost a názornost demonstrované slabiny/zranitelnosti a samotného útoku*).
3. Aktuálnost a dopad útoku
   (např. aktuální čistá instalace Windows 10 > než Windows 7 bez nainstalovaných aktualizací a spuštěnou zranitelnou oficiální aplikací, získání administrátorského oprávnění > než odepření služby).
4. Kvalita prezentace výsledků a jejich vyhodnocení.

Projekty jsou hodnoceny za **tým o 3 studentech**. Tým a vybraný útok musí být znám **do 3. týdne semestru**. Tým, vybraný útok (*název a stručný popis cíle laboratorní úlohy 2-3 věty*) a reference na zdroje je nutné vyplnit do online tabulky https://bit.ly/3af05JA (*nutné přihlášení pod VUT účtem*). **Vybrané téma projektu musí být schváleno vyučujícím**.

Během průběžné kontroly **v 7. týdnu lze získat max. 5 bodů**, během závěrečného hodnocení **v 13. týdnu semestru lze získat max. 10 bodů**. Celkem lze získat maximálně 15 bodů. **Pro zápočet je nutné získat alespoň 7,5 bodů.**

4. Odevzdání projektu:

Odevzdání projektu *(návod k laboratorní úloze, videoukázka, zdrojové kódy*) bude provedeno prostřednictvím e-learningu v archivovaném souboru zip s číslem skupiny. Odevzdání projektu provede **pouze jeden člen** řešitelského týmu, a to nejpozději **do 11. týdne semestru (tj. do 13. 04. 2020)**.

5. Struktura dokumentu “Návod k laboratorní úloze”:

Odevzdaný dokument musí splňovat veškeré náležitosti technického dokumentu (**psát spisovně a v trpném rodě**). Rozsah dokumentu je stanoven na max. 5 stran formátu A4 (titulní strana se do vymezeného rozsahu nepočítá). Struktura dokumentu je uvedena níže.

1. Titulní strana
2. Cíle laboratorní úlohy
3. Zadání
4. Teoretický úvod
5. Praktická část
6. Samostatné úkoly / otázky ke cvičení
7. Literatura

Seznam použitých zdrojů včetně použitých externích kódů a knihoven bude v práci řádně citován. V opačném případě bude práce hodnocena jako plagiát, a celý projekt bude ohodnocen celkovým počtem 0 bodů. **Bibliografické citace budou zapsány ve tvaru odpovídající normě ČSN ISO 690.**

6. Bodové hodnocení a hodnotící kritéria:

Průběžná kontrola (5 b):

1. Popis cílů laboratorní úlohy.
2. Popis bezpečnostní slabiny/zranitelnosti a samotného útoku.
3. Současný stav řešení (*např. vytvořená infrastruktura, naprogramované aplikace, aktuální fáze vypracování laboratorní úlohy apod.*).

Závěrečné hodnocení (10 b):

1. Funkčnost a kvalita zpracování laboratorní úlohy. (6 b)
2. Kvalita a formální zpracování návodu k laboratorní úloze. (2 b)
3. Kvalita prezentace výsledků a jejich vyhodnocení. (2 b)

7. Doporučené zdroje:

- Všeobecné a typografické pokyny a zásady pro psaní studentských prací, viz https://www.vutbr.cz/www_base/vutdisk.php?i=200408a223
- Jak psát prezentaci, viz https://www.vutbr.cz/www_base/vutdisk.php?i=200403aa7f
- Prezentace SP studenti, viz https://www.vutbr.cz/www_base/vutdisk.php?i=200407a994

- Databáze CVE všeobecně známých zranitelností v oblasti informační bezpečnosti, viz https://cve.mitre.org/
- Databáze exploitů, viz https://www.exploit-db.com/

- Hackování bez Metasploitu https://medium.com/@hakluke/haklukes-guide-to-hacking-without-metasploit-1bbbe3d14f90
- Příklad náplně laboratorní úlohy (**LAMPSecurity Training, CTF4**), viz https://www.vutbr.cz/www_base/vutdisk.php?i=200388a332
- Příklad náplně laboratorní úlohy (**LAMPSecurity Training, CTF7**), viz https://www.vutbr.cz/www_base/vutdisk.php?i=200405ad47
- Příklad náplně laboratorní úlohy (**SANS Technology Institute**), viz https://www.vutbr.cz/www_base/vutdisk.php?i=200389a14a

Ing. Petr Dzurenda, Ph.D.
dzurenda@feec.vutbr.cz
3. 2. 2020