Společnost Trusted Newtork Solutions, a.s., při příležitosti Dne s průmyslovými partnery FI 2022 vyhlašuje:

Soutěž nové generace pentesterů*ek o nejpřesvědčivější phishing

V případě red-team assessmentu organizace jsou jedním z testovaných vektorů útoku uživatelé. Vašim úkolem bude sestavit věrohodný phishing, kterým vmanipulujete uživatele k vykonání vámi zamýšlené akce, která bude simulovat průnik do interní sítě organizace.

Stejně jako v případě reálného testu je k dispozici pouze omezené množství informací, konkrétně:

- Předmětem testu je organizace vyrábějící firewally Kernun (viz kernun.cz) a její uživatelé, kteří využívají pro svou práci stanice s OS Windows a běžnou sadu kancelářských nástrojů, mezi které patří MS Office 2019 a Adobe Acrobat Reader. Zároveň tyto uživatelé používají pouze výchozí prvky kybernetické ochrany, tj. Windows Defender, mají k dispozici příkazový řádkek či Powershell a mohou spouštět a instalovat další programy bez omezení. Pro ostatní je možné předpokládat výchozí nastavení Windows 10.
- Dále je možné předpokládat, že organizace nemá správně nakonfigurovaný spam filter a žádnou další ochranu koncových stanic.

O co se soutěží:

- 1x Hak5 Bash Bunny + možnost stáže přímo v TNS
- 1x Hak5 USB Rubber Ducky
- 1x poor man's rubber ducky – vývojová deska založená Atmega32u4

Pravidla a průběh:

- Do soutěže se registrujete zasláním e-mailové správy na spp_soutez@tns.cz, kde do správy uvedete e-mailovu adresu, ze které bude phishing zaslán. E-mail odešlete ze svého MUNI e-mailu, abychom vás byli schopni identifikovat a v případě výhry kontaktovat. Případné dotazy směřujte také na tento e-mail.
- Soutěžní e-maily s phishingem zasílejte do půlnoci 16.5.2022 na adresu uzivatel42@tns.cz,
- Vyhlášení proběhne v rámci dne s SPP. Analýza, diskuse a postřehy z praxe proběhnou samostatně na workshopu také v rámci dne s SPP.

Zadání soutěžního úkolu:

- Na základě výše uvedených informací připravte věrohodnou e-mailovou kampaň – phishing, který běžného uživatele přijměje k vykonání akce/akcií tak, aby bylo možné demonstrovat spuštění vlastního kódu, volitelně také na straně vlastního c&c serveru spuštění detekovat.
- Kampaň musí být sestavena z věrohodné zprávy a škodlivé přílohy dle vlastního uvážení (může se jednat jak o aplikaci, tak o soubor využívající jiné aplikace z výše zmíněných nebo obsažených standardně ve Windows). Škodlivý soubor bude zaslán jako příloha e-mailu.
- Samotná zpráva může být adresovaná skupině nebo jednotlivci, ovšem nesmí se jednat o spear phishing. Pro zvýšení věrohodnosti můžete využít technik OSINT pro zjištění používaných technologií, stylu vyjadřování a podobně. Doporučuje se využití i dalších technik pro zvýšení úspěchu kampaně[1].
- Škodlivá příloha musí být soubor libovolného formátu, kterým budete schopni docílit spuštění vlastního kódu. Nemusí se jednat pouze o spustitelný soubor, existují různé varianty, jak docílit spuštění kódu i ze souborů s nespustitelnou přílohou. V případě nutnosti uživatele prostřednictvím zprávy instruujte, co za akce má vykonat pro úspěšné spuštění vašeho kódu.
- E-mail bude zaslán do půlnoci 16.5.2022 na adresu uzivatel42@tns.cz, jako soutěžní se bude počítat poslední phishing ze zaregistrované adresy.
- Soutěž je určena primárně studentům bakalářských a magisterských programů se zájmem o kybernetickou bezpečnost.

Vyhodnocení:

- Vyhlašovatel provede odhad úspěšnosti této kampaně na základě poznatků ze své praxe.
- Hodnocení bude probíhat ve dvou oblastech:
  - Věrohodnost zprávy – bude hodnocena míra přesvědčivosti pro vykonání zamýšlené akce, např. použité záminky. Toto hodnocení tvoří 50 % celkové váhy.
  - Technické provedení přílohy – bude se hodnotit úsilí které bylo vloženo do zamaskovaní spustitelného souboru, prostředky, které byly využity pro obejití detekce Windows Defenderem a podobě. To tvoří také 50 % celkové váhy.
  - Volitelné – extra body budou uděleny za schopnost detekce spuštění přílohy na straně domnělého útočníka, a to dalších 30 % hodnocení (celkem je možno získat 130 %).

[1] https://en.wikipedia.org/wiki/Social_engineering_(security)