BIS - Bezpečnost informačních systémů

Informace k projektu

Zadání projektu

The FITfather

Průvodce po Itálii. Na první pohled nijak zvláštní kniha. Přesto mě donutila zastavit můj jinak monotónní úklid dědova kabinetu. Ani tak název, jako její umístění vzbudilo moje podezření. Byla přímo uprostřed řady o šifrovacích algoritmech. Znal jsem svého dědu dobře a nikdy by nedopustil, aby byly knihy uloženy takto mimo jeho pečlivý systém. Na to byl přílišný pedant. Jak se tu tedy vzala?

Byl to již třetí den, co jsem vyklízel všechny dědovi věci. Odhadoval jsem, že na mě minimálně další dva ještě čekají, tolika věcmi to tu děda za ty roky zaskládal. Rozhodl jsem se, že je proto pravý čas na pauzu. Zaskočil jsem si koupit kafe do fakultní kavárny a vrátil jsem se zpět, abych se pohodlně usadil i s průvodcem na pohovce. Listoval jsem pomalu knihou, až jsem se dostal ke kapitole o Palermu. Vždy mě tam chtěl vzít. *Každý člověk by měl znát místo, odkud pocházeli jeho předkové*, jak rád říkával.

Náhle z knihy něco vypadlo. Byla to fotka, na které jsme s dědou stáli před branou Porta Nuova. Na zadní straně bylo napsáno 21/08/2017. Fotka vypadala úžasně, děda i já jsme se usmívali do objektivu, radostí bez sebe, že jsme v Palermu, kde se narodila jeho babička. Dokonalá vzpomínka na rodinný výlet. Byl tady ale jeden háček - nikdy jsem v Palermu nebyl.

Proč by měl děda fotku z okamžiku, který se nikdy nestal? Navíc, tak dobře upravenou, že i já bych na chvíli věřil, že si na to pamatuji. Něco tu nesedělo a já musel zjistit co.

Něco mě donutilo si přesednout k jeho počítači. Dosud jsem se zabýval pouze knihami a jeho notebook jsem nechal ležet tak, jak ho děda nechal. K mému překvapení byl pouze uspaný a na obrazovce se přede mnou objevil pokyn pro zadání hesla. Protože jsem vůbec netušil, jaké heslo děda používal, zkusmo jsem zadal 2182017.

Neprošlo.

21082017 také nic, tak jsem se obrátil na Google. Jaká jsou nejpoužívanější hesla? ….

Nakonec se podařilo.

Na ploše byla pouze ikona pro Putty, ale více mě zaujalo nastavené pozadí - zobrazovalo část mapy Itálie, přičemž některá z měst byla označená křížkem. Dohromady jich bylo deset. Palermo bylo navíc ještě zakroužkováno. Chtěl mi snad děda něco říct?

Nedalo mi to a začal jsem prohledávat lokální disk. Po chvilce hledání jsem našel soubor s názvem porta_nuova.txt. Byl to dopis, pro mě.

Milý xlogin00,

je toho tolik, kolik bych ti chtěl říct, ale nyní je již pozdě. Jestli čteš tyto řádky, selhal jsem a možná už nejsem mezi živými. Nemusíš být ale smutný. Pokud je to pravda, opět jsem se sešel s tvou babičkou, mou milovanou Ludmilou a to je vše, co jsem si přál.
Nyní ale čti pozorně, to co ti prozradím je velmi důležité a bohužel i nebezpečné.
Několik let jsem pracoval na této univerzitě v utajení, abych překazil plány mafii, která tu získala zázemí pro prodej zero day útoků na černém trhu.
Ve chvíli, kdy ti píšu tuto zprávu, se mi podařilo konečně nasbírat dost důkazů, které jim jednou pro vždy překazí všechny plány. Jestli vše půjde dobře, za týden bude mít vše v rukou policie a já s tebou konečně pojedu na slibovaný výlet do Itálie.
Pokud na mě přijdou, zabíjí mě, aby se dostali k důkazům. Zatím ale netuší, že jsem jim pravidelně útočil na síť a všechny důkazy v ní pečlivě ukryl. Vím, že po tobě chci víc, než mám právo žádat, ale prosím tě, najdi je a předej policii. Celé roky, aniž bys to věděl, jsem tě připravoval na tento moment
a věřím, že se ti podaří odhalit i mé nejzákeřnější skrýše. Zastav ty padouchy dřív, než se celá fakulta změní v hřiště jejich proradné organizace.
Buď však opatrný a nikomu nevěř. Fakulta je plná zlých lidí, kteří po tobě půjdou, jakmile se dozví, že chceš dokončit moji práci. A dávej si pozor na kmotra. Jsem si jist, že brzy pochopíš, kdo jím je.

Tvůj děda Alfons

V hlavě mi vířily miliony myšlenek. Měl jsem tolik otázek a tak málo odpovědí.

Ale jedno bylo jasné. Můj děda mi dal svůj poslední úkol a já udělám vše proto, abych ho splnil a dostal za mříže ty grázly, co se opovážili ublížit mé rodině.

Zelený kurzor líně blikal na černém pozadí terminálu a já v tu chvíli přesně věděl, co je potřeba udělat...

Verze pro suchary

Na mail vám přišel (nebo v několika hodinách přijde) privátní klíč, kterým se připojíte pomocí SSH na server BIS na uvedený port. Pokud by Váš ssh klient odmítal doručený klíč, tak použijte pro přístup server Merlin.

Ve vyhrazeném čase získejte co nejvíc tajemství (jsou to řetězce, které vždy obsahují slovo "tajemství") ukrytých na privátních serverech ve vnitřní síti. Získaná tajemství odevzdejte v textovém souboru secrets.txt. Vypracujte krátkou dokumentaci, která bude obsahovat

zmapování/schéma vnitřní sítě (servery, služby, zranitelnosti) s postupem získání jednotlivých tajemství (zmapování se týká pouze serverů, ne klientských stanic). Do WISu se odevzdává archiv xlogin00.tar.gz, který obsahuje dokumentaci ve formátu PDF doc.pdf a uvedený soubor secrets.txt.

Pravidla:

- Je zakázáno mazat jakékoliv soubory z kompromitovaných serverů (kromě těch, které na server sami nahrajete)
- **Uklízejte po sobě** - pokud na kompromitovaný server nahrajete jakékoliv skripty, exploity, nástroje, po dokončení práce je zase smažte
- Nesabotujte práci ostatním spolužákům
- Neprovádět útoky typu Denial of Service
- Nepoužívat nástroje Nessus a Metasploit
- Nenapovídejte spolužákům
- Snažte se nic nerozbít - víme, že to zvládnete, ale nám tím přidělláte práci a spolužákům třeba znemožníte získat body

---

Jakékoliv otázky směřujte na ijanus@fit.vutbr.cz, na stejnou adresu napište, pokud omylem něco rozbijete.

Datum odevzdání: 9.12.2020 22:59:59 ZULU (http://www.timezoneconverter.com)

POZOR! Projekt řešte samostatně, jakékoliv opisování povede k disciplinární komisi a k hodnocení 0b. I nekompletní řešení se hodnotí kladně.