Seznamte se - CrackMe

Vložil/a RubberDuck [1], 17 Prosinec, 2012 - 12:47

- Cracking [2]

Při snaze získat zkušenosti v oboru reverzního inženýrství nejednou člověk narazí na skutečnost, že bez svolení autora nemůže legálně zkoumat kód zvoleného programu. Prakticky na všechny aplikace a jejich jednotlivé části se totiž vztahuje copyright. Jinými slovy: Pokud se pomocí technik reverzního inženýrství pokusíme "rozebrat" prakticky jakýkoliv program nebo jeho část bez vědomí uživatele, stáváme se běžnými zločinci. I tento důvod byl jedním z těch, jenž dovedly crackery a reverzní inženýry k myšlence vytvořit si vlastní testovací aplikace s cílem poskytnout všem zájemcům možnost legálně testovat své znalosti a zkušenosti.

Pro tyto aplikace se vžil obecný název CrackMe a jedná se tedy o jakési "trenažery" od crackerů pro crackery, resp. reverzních inženýrů pro reverzní inženýry. Nevztahují se na ně omezení programovacích jazyků ani operačních systémů ani nic jiného. Poskytují mnoho úrovní náročnosti. Od kódů, kde stačí změnit jeden nebo dva bajty, až po komplexně zabezpečené aplikace s kontrolou integrity a aplikovaným packerem/kompresorem.

Protože na jednotlivé **CrackMe** se vztahují různé úkoly, můžeme se občas setkat s přesnějším rozdělením právě v závislosti na tom, jaký cíl dané CrackMe má. Zmíním zde tři nejčastější.

Asi nejznámější (i když ne podle jména) a nejoblíbenější mezi začátečníky je **PatchMe**. Program většinou obsahuje podmínku, kterou není možné obejít jinak, než fyzickou změnou kódu (tzv. patchováním). Tímto kódem může být i otravný Nag (v komerčních aplikacích známé okno s reklamou nebo informací o tom, že používáme neregistrovanou verzi programu atd.). Cílem je naučit nováčky, že je možné velmi jednoduše změnit chování celé aplikace změnou pár bajtů. Paradoxně ale PatchMe vytváří zkreslenou představu, že je každé CrackMe řešitelné touto cestou (obecně ano, ale pokud je aplikace velice rozvětvená a provádí se kontrola integrity na velkém množství míst, je realizace takového patche náročná, ne-li nemožná).

Další v řadě je **KeygenMe**. Jak název napovídá, cílem je vytvořit k dané aplikaci funkční keygen. Cílem je zdokonalit schopnosti číst a porozumět předloženému neznámému kódu, přesně se v něm orientovat a replikovat proces kontroly zadaných údajů (většinou kombinace login - password/SerialNumber). Úkol lze rovněž pojmout jako PatchMe (jak bylo zmíněno výše, ale nedoporučuje se). Pokud stačí pro aktivaci jen kombinace login - password/SN, jedná se v případě vytvoření generátoru o nejčistší řešení.

Posledním zmíněným je **UnpackMe**. Program je zašifrován/komprimován pomocí packeru/kompresoru a rychlá analýza tudíž není jen tak možná. Nejprve je nutné získat dešifrovanou/dekomprimovanou aplikaci v čisté formě a následně ji teprve začít zkoumat. Cílem je zvýšit schopnost čtení a orientace v cizím kódu a naučit uživatele možnosti dumpování dešifrované/dekomprimované aplikace z paměti. V reálném světě tuto techniku velmi často využívá malware pro znesnadnění analýzy a vyhnutí se detekci.

Takže pokud má někdo z čtenářů ambice věnovat se například zkoumání malware, CrackMe by měla být vaší první zastávkou na této dlouhé a náročné cestě. Pokud jste se ani teď nenechali odradit, doporučuji návštěvu portálu CrackMes.de [3]. Zde najdete rozsáhlou sbírku CrackMes všech náročností i použitých jazyků pro všechny možné platformy.

URL článku: https://security-portal.cz/clanky/seznamte-se-crackme

Odkazy:

[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/cracking
[3] http://www.crackmes.de