Slicing for Dummies

Slicing znamená přístup a manipulace systému bez autorizace. Může to být jak zneužití chyby v systému s účelem přimět ho vykonat neplánované instrukce, tak neoprávněné získání přihlašovacích údajů. V následujícím textu je obecně popsán, jak funguje kybertechnika a slicing.

Kybertechnika

Kyber systém se skládá z uzlů a linek. Uzly jsou zdroji výpočetní síly. Každý z nich má přesně danou funkci kterou v systému vykonává. Každý uzel je identifikován sériovým číslem, který přesně udává jeho výrobce, typ a verzi.

K systému lze přistupovat buď autorizovaně pomocí přístupových údaj nebo neautorizovaně pomocí slicingu. Přihlašovací údaje jsou dvojího typu: heslo a biometrické údaje. Heslo je známo jen uživateli, který svou znalostí prokazuje systému svou identitu. Biometrické údaje jsou většinou používány buď pro zvýšenou bezpečnost nebo pro snadnější přístup. Většinou se používá otisk prstu nebo sken sítnice.

Principy slicingu

Každý slicing probíhá v principu následovně: začíná v místě přístupu, kterým je většinou terminál. Uzel, který je místem přístupu se většinou označuje jako *vstupní uzel.* V každém okamžiku slicer může vykonat příkaz na libovolném uzlu v síti, který má pod kontrolou. Každý uzel je nejdříve potřeba *objevit* z nějakého jeho sousedního uzlu. Objevené uzly lze *ovládnout*. Uzel, na který je útok veden budeme označovat jako *cílený uzel*.

Typy uzlů, vhodné útoky

Každý útok funguje proti konkrétním verzi uzlu konkrétního výrobce. Použití nevhodného útoku může vést k detekci a následnému obnovení systému, které efektivně zabraňuje pokračování útoku.

Časové okno, detekce, obrana

Na každý slicing je jen omezený čas - *časové okno*. Každý útok může být detekován. Důsledkem detekce je zvýšená schopnost systému účinně se bránit, čímž dojde k snížení celkového časového okna. Detekováno může být i použití nevhodného útoku, jelikož způsobí neočekávané chování cíleného uzlu, které může být zachyceno systémem. Je tedy třeba postupovat obezřetně, používat vhodné útoky a dobře plánovat další akce.

Útoky a akce

Útoky lze obecně rozdělit do tří kategorií: prohledávání (scan), získávání informací (fingerprinting) a získání přístupu (exploit)

Prohledání okolí

Tento útok zjistí informace, které uzly sousedí s aktivním uzlem. Součástí výstupu jsou sériová čísla objevených uzlů.

Ovládnutí

Tento útok umožňuje převzít kontrolu nad cílovým uzlem.

Stažení dat

Příkaz stáhne všechny data, která jsou pod správou daného uzlu.

Informace o uzlu

Akce vypíše informace o uzlu, zejména pokud uzel podporuje nějaké nestandardní akce, jsou tyto akce vypsány.

Vyvolání akce uzlu

Pokud uzel umožňuje provádět nějaké akce, například otevřít dveře, zaměřit a odpálit raketu, lze je pomocí tohoto útoku provést.

Zobrazení mapy

Akce zobrazí všechny objevené uzly.

Uzly

Každý uzel má pevně danou funkčnost. V této sekci se budeme zabývat nejčastějšími typy uzlů a jejich funkcemi.

Databáze

Databáze slouží primárně pro ukládání dat.

Podporované příkazy pro databázi jsou stažení dat, prohledání okolí a ovládnutí.

Ovladač

Tento uzel umožňuje ovládání fyzických zařízení. Ať už se jedná o elektronický zámek u dveří, bezpečnostní kameru či zbraňový systém, ovládací uzel je zodpovědný za správu a manipulaci s těmito zařízeními.
Podporované příkazy pro ovladač jsou informace o uzlu, vyvolání akce uzlu, prohledání okolí a ovládnutí.

Honeypot

Honeypot je uzel, který nemá žádnou funkci, vyjma bezpečnostní. Není využíván žádným jiným uzlem, a proto je každý přístup označen za neautorizovaný, vedoucí k detekci útočníka.
Honeypot podporuje všechny typy příkazů, nicméně každý příkaz urychluje detekci útoku a obnovení systému.

Běžný uzel

Většína uzlů v síti má technický charakter bez žádné speciální funkce.
Podporované příkazy pro běžný uzel jsou prohledání okolí a ovládnutí.

Terminál

Terminál je pro uživatele vstupní uzel k systému. Je zodpovědný za příjem vstupů od uživatele a přesměrování těchto vstupů k cílovému uzlu.
Jediný podporovaný příkaz pro terminál je prohledání okolí.

Výrobci

V této sekci jsou představeni nejznámější společnosti, které se pohybují na trhu s kybernetickými komponentami.

Adas Corporation - Adasca BioMechanical Corporation

Adasca BioMechanical Corporation společnosti Arkania - obvykle zkrácená na Adascorp - má dlouhou a místy neurčitou historii. Společnost byla po staletí nepřetržitě vlastněna a provozována členy královské rodiny Adasca a je nejznámější pro pokrok v oblasti bioinženýrství a lékařského výzkumu. Nicméně, společnost je přítomna na rozmanitých trzích a její portfolio obsahuje například harware pro vojenské droidy a finanční služby. Před třista lety se tehdejší prezident společnosti lord Arkoh Adasca pokoušel využít galaktickou energii pomocí gargantuanských exogortů - běžněji známých jako vesmírní slimáci. Tento šílený plán byl

naštěstí ukončen jeho smrtí a zničením ústřednou společnosti Adascorp. Po mnoha desetiletích soudních sporů a nespočetně vyplacených odškodnění společnost začala opět operovat.

AraTech Industries

Společnost Aratech je společnost zabývající se výrobou automobilů a je jednou z předních společností v konglomerátu Antarian Rangers (TAR). Aratech má unikátní produktové portfolio: je jediným výrobcem modelu 008 Heavy Landspeeder, který je bezpochyb jedním z nejvýkonnějších vozidel v galaxii. Kromě toho jeho výrobní linky produkují také Corvette třídy Aratech Hunter, která je největší a nejsilnější podvodním dopravním prostředkem v galaxii, který je volně dostupný. Aratech je v kybertechnologiích zastoupen jen okrajově, jeho hlavní doménou jsou přepravní prostředky.

CEC - Correlian Engineering Corporation

Corellian Engineering Corporation o sobě tvrdí, že je to nejdéle existující podnikatelský subjekt v galaktické historii. Ačkoli lze toto tvrzení zpochybnit, nikdo nezpochybňuje kvalitu výrobků CEC. Nejchytřejší a nejpopulárnější vědci a inženýři Republiky se této společnosti shromažďují a vytvářejí pokročilé nové lodě, droidy a další technologie. Před invazí Impéria agenti Imperiální Výzvědné Služby tiše infiltrovali mohutnou sít kancelářských a výrobních budov CEC. Plánem bylo převzít kontrolu nad obrovskou obranou společnosti těsně před příchodem Impéria v případě , že by korporace kladla odpor při obsazování Correlie. Něco se však pokazilo a všichni agenti beze stopy zmizeli. V současnoti je CEC největší hrozbu pro imperiální plány na Correlii.

Czerka

Původně založená jako Czerka Mining and Industrial, tato století-stará korporace se diverzifikovala do podniků produkujícím širokou škálu výrobků, od spotřebitelských potravinových produktů po vojenské zbraně. Jedná se o jeden z nejbohatších a nejúspěšnějších ekonomických podniků, který obchoduje prakticky na každé civilizované planetě, je vlastníkem několika hvězdných systémů a zaměstnavatelem několika miliard lidí - má dokonce své zastoupení v senátu republiky. Czerka je jedinečná v tom, že je schopna vyjednávat obchodní dohody i s Hutt kartelem a jinými nezávislými světy, ignorujíce politické hranice a vytvářejíce ohromující zisky. Navzdory tomu, že společnost je známa svým nedostatkem loajality, nikdo si nemůže dovolit přestat obchodovat s Czerkou. Kdykoli, kdekoliv ... jsme tam je slogan společnosti - motto, které bezohlední oportunisty dychtivě podporují.

GSI - Galactic Solutions Industries

Galactic Solutions Industries je rychle se rozvíjející společnost v oblasti osobních zbraní na Nar Shaddaa. Společnost byla založena geniálním vynálezcem a magnátem Addalarem Hylandem krátce po obnovením konfliktu mezi Republikou a Impériem. První výrobní verze pistole GSI-B4 společnosti GSI byla známá pro svou impozantní palebnou sílu na poměry lehce ukrytelné

zbraně. Podle zpráv Republiky i Impéria, Galactic Solutions Industries je ochotna obchodovat s oběma frakcemi. Motto společnosti vskutku propaguje tuto skutečnost: Zůstáváme neutrální, abyste Vy neutrální být nemuseli! GSI je známo tím, že kontaktuje bojovníky na obou stranách války, aby si od nich vyžádala pomoc s výzkumem a získávala od nich zpětnou vazbu.

Příkazy

V této části probereme jednotlivé komponenty a implementace útoků, které lze použít proti konkrétním uzlům. Každý uzel je identifikován sériovým číslem, který udává výrobce a typ uzlu. V první části probereme, jak z sériového čísla určit typ uzlu a výrobce. V druhé části vypíšeme seznam konkrétních příkazů, kterými lze provádět útoky a na které cíle je lze aplikovat.

Sériová čísla

V následující tabulky jsou uvedeny pravidla, kterými sériové číslo kóduje typ uzlu.

databáze	první velké písmeno sériového čísla je symetrické podle svislé osy
ovladač	druhé písmeno sériového čísla je samohláska
honeypot	stejné podmínky jako databáze, ale po vypuštění písmen je sériové číslo dělitelné 13
běžný uzel	poslední písmeno sériového čísla je obojetná souhláska
terminál	první písmeno sériového čísla je S

Následující tabulka shrnuje způsoby, jak sériové číslo kóduje výrobce uzlu.

Adascorp	poslední trojčíslí sériového čísla je seřazeno vzestupně
Aratech	druhá číslice v sériovém čísle je 2, poslední číslice je 7
CEC	třetí znak sériového čísla je 2, pátý znak je 8
Czerka	po vypuštění písmen je sériové číslo dělitelné 3
GSI	první trojice čísel v sériovém čísle je seřazena sestupně

Seznam příkazů

V této sekci probereme jednotlivé příkazy a uvedeme, na které typy uzlů kterých výrobců je lze použít.

`alist`	výpis informaci o uzlu výrobce AraTech Industries
`clear`	vyvolání akce na uzlu výrobce AraTech Industries
`cmd`	vyvolání akce na uzlu výrobce Galactic Solutions Industries
`CPREM`	stažení dat z uzlu výrobce Czerka Corporation
`dir`	výpis informaci o uzlu výrobce Correlian Engineering Corporation
`dir-a`	výpis informaci o uzlu výrobce Galactic Solutions Industries
`exploitator`	ovládnutí uzlu výrobce AraTech Industries
`get-rm`	stažení dat z uzlu výrobce Galactic Solutions Industries
`hydra`	ovládnutí uzlu výrobce Galactic Solutions Industries
`ll`	výpis informaci o uzlu výrobce Czerka Corporation
`ls-l`	výpis informaci o uzlu výrobce AdasCorp
`map`	prohledání okolí z uzlu výrobce AraTech Industries
`mapAll`	prohledání okolí z uzlu výrobce Galactic Solutions Industries
`msf`	ovládnutí uzlu výrobce AdasCorp

`mv-sec`	stažení dat z uzlu výrobce Correlian Engineering Corporation
`nmap`	prohledání okolí z uzlu výrobce AdasCorp
`od`	vyvolání akce na uzlu výrobce Correlian Engineering Corporation
`open`	vyvolání akce na uzlu výrobce AdasCorp
`powaEx`	ovládnutí uzlu výrobce Czerka Corporation
`pwn-or`	ovládnutí uzlu výrobce Correlian Engineering Corporation
`s-entry`	vyvolání akce na uzlu výrobce Czerka Corporation
`scan`	prohledání okolí z uzlu výrobce Czerka Corporation
`scp`	stažení dat z uzlu výrobce AraTech Industries
`sec-scan`	prohledání okolí z uzlu výrobce Correlian Engineering Corporation
`all show-map`	zobrazení všech objevených uzlů
`wget`	stažení dat z uzlu výrobce AdasCorp

Příkaz se vždy skládá následovně:

`<sériové číslo uzlu><mezera><příkaz>,`

kde <mezera> znamená jedno stisknutí spacebar klávesy (prostě mezera). Jedinou vyjímkou je příkaz na zobrazení všech objevených uzlů, který se zadává jen jako příkaz a kterým je vždy vhodné slicing započít. Všechny příkazy rozlišují malá a velká písmena.