

# Hypervisor rootkity

vid

<http://www.vid-site.sk>

# Hardwarova virtualizacia

- Rozne na Intel (VMX / VT-x) a AMD (Pacifica)
- Vyradne jednoduchsia na implementaciu nez softwarova
- Pri neuplnej virtualizacii minimalne naroky na pamat

# Moznosti HW virtualizacie

- Virtualizacia pamate
- Odchytenie niektorych eventov (prepnutie procesu, exceptiony, casovac, I/O pristup)
- Virtualizacia externeho HW

# Ako to funguje

- Hypervisor zapne na procesore virtualizacny mod (na Inteloch moznost zakazat)
- Hypervisor vyplni strukturu popisujucu stav VM
- Hypervisor spusti VM
- VM bezi az dokym sa nestane udalost ktoru chce hypervisor odchytit
- Vtedy sa beh VM prerusi, stav VM sa zapise do struktury, riadenie sa odovzda hypervisoru

# Ako to funguje #2

- Hypervizor zisti o aky event sa jedna, moze emulovat specialnu instrukciu, odovzdat exception na spracovanie naspet do VM, moze zmenit hodnoty registrov alebo pamate, atd...\
- Ked je spracovanie eventu hotove, odovzda riadenie naspet do VM
- A toto cele dokola

# Vyuzitie na rootkit

- Rootkit “zavrie” beziaci system do VM:
- Struktura popisajuca stav VM sa naplni hodnotami z CPU
- Beh systemu pokrakuje vo uz VM, kde rootkit je hypervizor a ma nad systemom kontrolu

# Vyhody virtualizacie pre rootkit

- Ma kontrolu nad systemom vramci moznosti HW virtualizacie
- Moze zabranit pristupu k pamati kde je kod rootkitu, alebo namiesto nej podstrcit inu pamat
- Moze filtrovat pristup k I/O zariadeniam, ale potrebuje HW-specificky kod
- Kod rootkitu bezi z pohladu “neviditelne”, nepotrebuje nic hookovat ani menit pamat systemu

# Nevyhody virtualizacie pre rootkit

- Virtualizacia musi byt v BIOSe povolená (defaultne je zakázaná), ale system nesmie pocas inicializacie este bezat vo VM
- Zapnutie virtualizacie uz vyzaduje root prava (musi bezat v ringu 0)
- Mnoho udalosti sa neda priamociaro zachytit, napr. volanie konkretnej systemovej funkcie
- HW Intel virtulizacia nebude fungovat

# Detekcia virtualizacnych rootkitov

- Spôsob zavedenia rootkitu zanecha stopy (driver, MBR pristup), ktore sa relativne tazko zahladzuju (treba HW-specific emulaciu alebo zasahy do kernelu)
- Spracovanie eventov hypervizorom zanecha stopy (TSC, timer), z ktorých nie vsetky idu zahladit (cache)

# Doterajsia diskusia v IT komunitie

- Joanna Rutkowska (do 2003 transsexual Jan Krysztof Rutkowski) predstavil/a prvokrat tuto myslienku na BlackHat-e ako “100% nedetekovatelny rootkit”
- Nasledovali priklady ako sa virtualizacia da detekovat, na ktore nasledovali ukazky ako detekcii zabranit, atd. stale dokola
- Eventualne Rutkowska ustupil/a od pozicie schovavania faktu ze system bezi vo VM

# Diskusia #2

- Teraz stavia argument na tom ze detekcia virtualizacie neprezradi ci sa jedna o normalny hypervizor (VMWare, Xen), alebo rootkit, a je treba zasah uzivatela
- Tvrdi ze v buducnosti bude virtualizacia tak rozsirena ze bude pouzivana takmer vsade, takže detekcia samotnej virtualizacie bude zbytocna.

# Diskusia #3

- Tu je vsak problem ze na spustenie hypervizor rootkitu v systeme ktory uz bezi vo VM je treba prebit sa “von” z VM, cize potrebuje poznat “exploit” na hypervizore – toto demonstrovala na poslednom BlackHate so systemom beziacim v Xene.

# Otazky

Uliat prednasajuemu  
!!!