Problematika bezpečnosti počítačových sítí

Joseph Soukup – P4

Fyzické zabezpečení

- Základem každého zabezpečení sítě je fyzické zajištění serveru
- Server by měl být v místnosti, kam se nemůže dostat nepovolaná osoba
- Základem jsou zamřížovaná okna, zamčené dveře, kamerový systém a popřípadě poplašné zařízení
- Velké serverové místnosti, popřípadě hlídá ochranka

Sociální inženýrství

- Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace
- Ve většině případů útočník nepřichází do osobního kontaktu s obětí

Pretexting

- Utváření a využívání vymyšleného scénáře s cílem přesvědčit oběť k učinění potřebné akce nebo získání potřebné informace
- Cílem je přesvědčit oběť o legitimnosti akce, která je po ni požadována – rodné číslo, …
- Množstvím firem stále ověřuje totožnost klienta podle rodného čísla, rodného jména matky či jiných relevantně snadno dostupných informací

Phishing

- Podvodná technika používaná na internetu k získávání citlivých údajů (hesla, …)
- Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku -> vypadá stejně jako oficiální
- Stránka: https, certifikát

Adware

- Produkty znepříjemňující práce nějakou reklamní aplikací
- Od běžných bannerů až po neustále vyskakující pop-up okna
- Nejsou bezpečné -> jedná se o reklamy

Spyware

- Internetové stránky k odesílání dat z počítače bez vědomí jeho uživatele
- Do počítače se dostane stažením s programem – jako Adware
- Často se to týká například klientských programů pro peer to peer sítě
- Patří mezi malware
- Znaky – neznámá domovská stránka, pomalý start PC

Malware

- Určený ke vniknutí nebo poškození počítačového systému
- Zahrnují počítačové viry, trojské koně, spyware a adware
- Programy navržené tak, aby poškozovaly nebo zcela mazaly data
- Programátor nebo správce systému, který byl propuštěn za zaměstnání, může v systému zanechat zadní vrátka

Exploit

- Speciální program, data nebo sekvence příkazů, které využívají programátorskou chybu, která způsobí původně nezamýšlenou činnost software a umožňuje tak získat nějaký prospěch
- Většina exploitů slouží k získání přímo administrátorských zpráv
- Typ zranitelného místa
- Nutnost mít přímý přístup k napadanému systému (local), nebo postačuje použití jiného počítače (remote)
- Výsledek útoku (EoP, DoS, Spoofing atd.)

Vzdálený exploit

- Využívá počítačová síť, takže není potřeba přímý přístup k cílovému systému

Místní exploit

- Je nutný přímý přístup k systému a většinou je jeho účelem získat oprávnění, která jsou vyšší, než byla uživateli přidělena správcem počítače

Virus

- Vkládá do jiných spustitelných souborů či dokumentů
- Některé viry mohou být cíleně ničivé
- Jiných virů je relativně neškodných, popřípadě pouze obtěžujících
- Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“)
- Virus se mezi dvěma počítači může přenést jedině tím, že někdo přenese celého hostitele

Rezidentní a nerezidentní viry

- Buď se ve chvíli spuštění hostitele rozšíří do nalezených nenakažených souborů, nebo se pouze uloží do operační paměti počítače, ve které zůstane až do doby vypnutí počítače, a mezitím infikuje soubory

Stealth viry

- Se snaží zamaskovat svou přítomnost v souborů tím, že se zachytí na přerušení, kudy prochází veškeré požadavky na čtení dat ze souboru
- Vir si pak kontroluje, zda se požadavek týká i infikovaného souboru, v tomto případě pak vrátí aplikace data původního neinfikovaného souboru
- Antivirus si buď kontroluje, zda není adresa přerušení přepsána, případně na čtení používá přímo služby diskového řadiče

Makro viry

- Jedná se o makra, která jsou schopna se kopírovat z dokumentu do dokumentu
- Případně i ovládat systém
- Šíří se v dokumentech kancelářských balíků

Červ

- Je schopen automatického rozesílání kopií sebe sama na jiné počítače

- Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření
- Vykonává obvykle tento program v počítači nějakou sekundární činnost, které je červem nesena jako „náklad“
- Např. šifrování souborů nebo činnost jako vir

DoS (DDoS – distributed…)

- Denial of Service – odmítnutí služby
- Technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele
- Vnucení opakovaného resetu cílového počítače
- Narušení komunikace mezi serverem a obětí tak, aby jejich komunikace byla buď zcela nemožná, nebo alespoň velmi pomalá
- Jeho cílem je v jednom čase útok na jednu konkrétní službu

Botnet

- Označuje síť počítačů infikovaných speciálním softwarem, který je centrálně řízen z jednoho centra
- Botnet pak provádí nažádoucí činnost, jako je rozesílání spamu, DDoS útoky a podobně
- Pro tvorbu botnetu je uznání a finanční zisk
- Označuje množinu kompromitovaných počítačů (zvaných zombies) na kterých běží software

Topologie

- Multi server
- Stromová topologie
- Náhodná
- Hvězdicová topologie
    - Operátor botnetu rozesílá viry a červy, které infikují počítač oběti zákeřnou aplikací ve které je bot
    - Bot na infikovaném počítači se přihlásí ke svému C&C serveru (Tím je nejčastěji IRC server)
    - Spammer využije služeb botnetu za příslušnou finanční částku
    - Spammer poskytne správci zprávy (spamové emaily), které chce poslat do světa
    - Správce pak vydá botům instrukce co mají vykonat přes IRC server a boti je splní a rozesílaní tak spam

Man in the middle

- Snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem (lze přesměrovat komunikaci)
- Nemusí být v případě spoléhání na digitální certifikát nutné, aby útočník filtroval celou komunikaci
- Stačí otrávit DNS nebo ARP cache uživatele, a tím ho nevědomky přesměrovat na jiné webové servery

- Pokud z nich uživatel do svého prohlížeče bez ověření nainstaluje falešný kořenový certifikát certifikační autority, může pak důvěřovat falešnému elektronickému podpisu nebo phishingové webové stránce

Flooding

- Útok hackerů s hodně vysokým počtem dotazů, což vede k odmítnutí služby
- Odesílat data na všechny porty VLAN sítě – MAC flooding
- Zaplavování přepínačů rámci (pakety) s náhodně generovanými zdrojovými MAC adresami

Snooping

- Ochrana proti Spoofing a starvation
- Umožňuje nakonfigurovat porty jako trusted a untrusted
    - Trusted mohou posílat DHCP request
    - Untrusted mohou pouze propouštět request
- Umožňuje přepínači sestavit tabulku, která mapuje MAC adresy, IP adresy, VLAN a číslo portu

DHCP Starvation

- Zařízení vyčerpá adresní prostor serveru na určitou dobu nebo se sám stane DHCP serverem v man-in-the-middle

Port security

- Vypnout nepoužívané porty
- Určit MAC adresu která bude mít přístup na port
- Snooping

Zabezpečení bezdrátových sítí

WEP

- Zastaralé
- Šifruje přenášené rámce

WPA

- Používá 128bitový šifrovací klíč a 48bitový inicializační vektor
- WPA zahrnuje počítadlo rámců, které chrání před útoky snažícími se zopakovat předchozí odposlouchanou komunikaci
- Algoritmus CRC-32

WPA2

- Algoritmus CCMP založený na AES
- Povinná pro všechna nová zařízení, jež chtějí být certifikována jako Wi-Fi

PSK

- Každý uživatel musí před vstupem do sítě zadat heslo
- Heslo musí být uloženo na všech přístupových bodech Wi-Fi sítě

AES

- Jedná se o symetrickou blokovou šifru šifrující i dešifrující stejným klíčem data rozdělená do bloků pevně dané délky
- AES pracuje s maticí bytů 4x4 označována jako stav