



Techniky vyhýbania sa sieťovej detekcii

Marián Novotný
novotny(at)eset.sk

O čom bude prezentácia

- Niečo o mne
- Sieťový IDS systém
- Principiálne zraniteľnosti IDS systému
- Príklad detekcie - zraniteľnosť [MS 08-67](#)
- Vyhýbania sa detekcii na
 - sieťovej (IP) úrovni
 - transportnej (TCP) úrovni
 - aplikačnej úrovni (SMB, DCE RPC)
- Prehľad nástrojov
- Záverečné zhrnutie - diskusia

Niečo o mne

- Momentálne
 - Dizajnér bezpečnostných sieťových algoritmov v ESET-e
 - Analýza, návrh a implementácia nových funkcionalít pre personálny firewall a systém detekcie útokov
 - Práca na produkte ESS/Endpoint pre Windows OS
 - Čiastočná spolupráca s FI MUNI
 - LABAK, záverečné práce
- V minulosti
 - Bezpečnostný konzultant
 - Výskum v oblasti bezpečnostných protokolov
 - PhD práca “Návrh a analýza bezpečnostných protokolov”

Sieťový IDS systém

- monitorovanej sieťovej komunikácie
 - Sieťová sonda
 - Koncová stanica
- vlastný model komunikácie
- Identifikácia zlých dát
- Účinnosť
 - Miera falošných poplachov
 - Miera detekcie útokov
- Open source nástroje
 - SNORT
 - Bro IDS

Principiálne zraniteľnosti IDS systému (2)

- Problémy
 - Komplexnosť špecifikácií sieťových protokolov
 - Redundancia návrhu sieťových protokolov
 - Nedodržiavanie špecifikácií výrobcami softvéru
 - rôznorodosť implementácií protokolov
 - Nedostatok informácií o koncovej stanici/aplikácii
 - hrozba DOS útoku
- Ak IDS systém **nedokáže interpretovať dáta**
 - Detekuje útok – zakáže
 - Falošný poplach
 - Nedetekuje útok - povolí
 - Bezpečnostná diera
- Ciel útočníka
 - **Vloženie** neexistujúcej komunikácie pre IDS
 - **Vyhnutie sa** inšpekcii komunikácii

Zraniteľnosť MS 08-67

- Známa **implementačná chyba** v MS WINDOWS
 - NetpwPathCanonicalize z knižnice netapi32.dll
 - Normalizuje cesty súborového systému
 - prístupná cez DCE/RPC rozhranie ServerService
 - NetprPathCanonicalize
 - NetprPathCompare
- Známa vďaka červovi **Conficker**
- Detekcia IDS
 - Hľadanie exploitu
 - POC exploit, metasploit,...
 - Hľadanie zlých vstupých dát, ktoré vyvolajú zraniteľnosť
 - potreba rozumieť stavu protokolu/zraniteľnej aplikácie
- Ukážka

Vyhýbania sa detekcii na sieťovej (IP) úrovni

- Ipv4 fragmentácia
 - Zlé vstupne dáta vo viacerých IP paketoch
 - Rôzne poradie
 - Prekrývajúce fragmenty
- Ipv6
 - IDS systém podporuje len IPv4, koncové stanice aj IPv6
 - Podpora pre komunikujúce stanice v rozšírenej hlavičke
- IDS
 - Zakázanie fragmentovaných paketov?
 - Vyskladanie paketu z fragmentov
- Ukážka

Vyhýbania sa detekcii na transportnej (TCP) úrovni

- Zlé dáta rozdelené a poslané vo viacerých TCP segmentoch
- Inšpekcia aplikačných dát
 - nutné vyskladanie streamu zo segmentov
- Prekrývajúce sa segmenty
 - Judy Novak a Steve Sturges. Target-Based TCP Stream Reassembly
 - Zakázať?
 - Potrebné info o OS
- Krátke segmenty

Vyhýbania sa detekcii na aplikačnej úrovni

- Aplikačné protokoly
 - Binárne
 - textové
- SMB protokol
 - zdielanie súborov, tlačiarňí
 - prístup pre IPC komunikáciu
 - IPC\$, *named pipes*
- DCE/RPC protokol
 - mechanizmus pre vzdialené volanie funkcií

Vyhýbania sa detekcii v SMB protokole

- Komplexný a redundantný protokol
 - Pripojenie na share pomocou 2 príkazov
 - Otvorenie súborov pomocou 7 príkazov
- Fragmentácia
 - Dáta pre RPC vo viacerých write commandov
- Kódovanie
 - Ascii, unicode stringy
- Špeciality
 - Normalizácia mena súboru
 - Andx príkazy
 - Špeciálne flagy

Vyhýbania sa detekcii v DCE/RPC protokole

- Otvorený protokol
- nezávislý na OS
- V MS WINDOWS prenášaný pomocou
 - UDP, TCP, SMB, HTTP
- Možná zmena interface
 - PDU alter context
- Fragmentácia
 - Vlastný mechanizmus fragmentácia dát
- Kódovanie
 - NDR
 - BE reťazce, EBCDIC

Zhrnutie techník

- Podporované v špecifikácii protokolov, používané
 - Fragmentácia, segmentácia
- Podporované v špecifikácii protokolov, nepoužívané
 - Špeciálne kódovania, zmeny kódovania
 - Divné flagy, padding
 - BE RPC, EBCDIC RPC
- Nepodporované v špecifikácii, implementované v OS, aplikácii
 - Fault tolerant implementácie
 - Prekrývanie TCP segmentov
 - Implementačné zvláštnosti
 - IDS chýbajú potrebné informácia

Nástroje

- Evader
 - Nástroj na testovanie IDS
 - RDP, HTTP, SMB
 - Viacero IP, TCP, SMB, MSRPC, HTTP techník
 - Kombinácia pomocou skriptu Mongbat
 - <http://evader.stonesoft.com/>
- Metasploit
 - Open source nástroj
 - http://www.offensive-security.com/metasploit-unleashed/Main_Page
 - Option, evasion, advanced
- Impacket
 - Vlastná implementácia SMB, RPC
 - Viacero pokročilých techník vyhýbania sa
- SCAPY

Nástroje - metasploit

- show evasion
 - DCERPC::fake_bind_multi
 - DCERPC::fake_bind_multi_append
 - DCERPC::fake_bind_multi_prepend
 - DCERPC::max_frag_size
 - DCERPC::smb_pipeio
 - SMB::obscure_trans_pipe_level
 - SMB::pad_data_level
 - SMB::pad_file_level
 - SMB::pipe_evasion
 - SMB::pipe_read_max_size
 - SMB::pipe_read_min_size
 - SMB::pipe_write_max_size
 - SMB::pipe_write_min_size
 - TCP::max_send_size
 - TCP::send_delay

Záver

- Prediskutovali sme principiálne zraniteľnosti IDS
- Príklad binárnych protokolov SMB, RPC a TCP/IP
- Analogické techniky pre
 - textové protokoly
 - iný typ detekcií
 - Klientské zraniteľnosti

Q&A

Ďakujem za pozornosť