Penetrační testy – OSSTMM

Jaromír Vaněk
e-mail: vanekj5@fel.cvut.cz
ICQ: 342-453-214
Jabber: kredits@jabber.cz

Bezpečnostní audit vs. penetrační testy

- Bezpečnostní audit
  - zhodnocení současného stavu vůči nějaké normě
- Penetrační testy
  - testování bezpečnosti pokusem o průnik
  - blízký reálnému útoku
  - poskytne obrázek o tom, co všechno by mohl dokázat utočník při současné úrovni zabezpečení

Co je OSSTMM?

- Open Source Security Testing Methodology Manual
- veřejně dostupná otevřená metodika pro testování bezpečnosti
- autor: Pete Herzog, vznik: 2001
- organizace ISECOM (http://www.isecom.org/)
- v současné době verze 2.2 (na verzi 3.0 se pracuje)

Proč používat OSSTMM?

- bez nějakého standardu jsou penetrační testy závislé na konkrétním testerovi a jeho zkušenostech
- OSSTMM má jasně dané kroky, které se musí provést
- výsledky testů jsou mezi sebou porovnatelné
- OSSTMM zavadí tzv. RAVs (Risk Assessment Values)

ISECOM - RISK ASSESSMENT VALUES

OPSEC	
Visibility	1
Access	0
Trust	0

Class A	CONTROLS	Missing
Authentication	0	0
Indemnification	0	0
Resistance	0	0
Subjugation	0	0
Continuity	0	0
Class B		
Non-Repudiation	0	0
Confidentiality	0	0
Privacy	0	0
Integrity	0	0
Alarm	0	0

	LIMITATIONS	Total
Vulnerabilities	0	0,00000
Weaknesses	0	0,00000
Concerns	0	0,00000
Exposures	0	0,00000
Anomalies	0	0,00000

CALCULATION WORKSHEET	
Porosity	0
Total Controls	0
Class A Controls	0
Class B Controls	0
Whole Coverage	#DIV/0!
True Coverage	#DIV/0!
True Coverage A	#DIV/0!
True Coverage B	#DIV/0!
Missing Controls	0
Missing Controls A	0
Missing Controls B	0
Coverage Missing	#DIV/0!
Total # Limitations	0
Limitations Value	0

Vulnerability	0,00000000
Weakness	0,00000000
Concern	0,00000000
Exposure	0,30103000
Anomaly	0,00000000

	RAV TOTALS
OPSEC	4,01730417
CONTROLS	0,00000000
LIMITATIONS	0,00000000
Δ	-4,01730417

RAV	95,98269583

Struktrura OSSTMM [1]

- Testování je rozděleno na 5 sekcí (channels):
  - **Information security testing** (*jak organizace funguje, kolik dat musí spravovat, profily zaměstnanců*)
  - **Process security testing** (*co všechno o sobě organizace navenek prozrazuje, sociální inženýrství*)
  - **Internet technology security testing** (*skenování sítě, hledání bezpečnostních slabin, pokusy o průnik a získání citlivých dat*)
  - **Communications security testing** (*telefony, hlasové schránky, faxy*)
  - **Wireless security testing** (*elekromagnetické vyzařování, Wi-fi, Bluetooth, bezdrátové periferie*)
  - **Physical security testing** (*zabezpečení prostor, dveře, ploty, monitorovací zařízení, alarmy*)

Struktrura OSSTMM [2]

- Každý channel se dělí na moduly:
  - Network surveying (*struktura sítě, doménová jména, IP adresy serverů*)
  - Port scanning (*které porty jsou otevřené, nastavení firewallu*)
  - Service identification (*identifikace běžících služeb*)
  - System Identification (*identifikace operačního systému*)
  - Vulnerability research (*nalezení potenciálních zranitelností podle běžících služeb a OS*)
  - Internet application testing (*nalezení chyb v aplikacích vytvořených danou organizací*)
  - Router testing (*jaké pakety propouští router do/z vnitřní sítě, co je zakázáno/povoleno*)
  - Trusted system testing (*nalezení systémů, které jsou závislé na dalších systémech*)
  - Firewall testing (*otestování ACL, podobné jako sekce Router testing*)
  - Intrusion Detection System Testing (*druhy paketů, které nejsou pomocí IDS testovány*)
  - Containment Measures Testing (*bezpečnost před viry a trojskými koni*)
  - Password Cracking (*ověření síly hesel pomocí automatických nástrojů*)
  - Denial of Service Testing (*systémy, které jsou zranitelné DoS*)
  - Security Policy Review (*ověření bezpečnostní politiky vůči aktuálnímu stavu*)

Struktrura OSSTMM [2]

- Každý channel se dělí na moduly:
  - Network surveying (*struktura sítě, doménová jména, IP adresy serverů*)
  - Port scanning (*které porty jsou otevřené, nastavení firewallu*)

Enumerate Systems

- Collect broadcast responses from the network
- Probe past the firewall with strategically set packet TTLs (Firewalking) for all IP addresses.
- Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
- Use a TCP source port 80 and ACK on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.
- Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use DNS connect attempts on all hosts in the network.
- Use FTP and Proxies to bounce scans to the inside of the DMZ for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

Penetrační testy – OSSTMM

Děkuji za pozornost