



Testowanie systemów IDS/IPS

Michał Melewski

carstein@man.poznan.pl

Zespół Bezpieczeństwa PCSS

Plan prezentacji

- 1) Błędy popełniane przy wykorzystywaniu systemów IDS/IPS.
- 2) Omówienie sposobów na ominięcie systemów IDS/IPS.
- 3) Co chcemy testować?
- 4) Oprogramowanie do testowania
- 5) Framework do testowanie systemów IDS/IPS

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Zrozumienie różnic pomiędzy systemem IDS a IPS
 - Świadomość celów; co chcemy osiągnąć
 - **Zgłosić podejrzaną działalność?**
 - **Zatrzymać atak?**
 - **Wykrywać nietypowe zdarzenia?**
 - **Jesteśmy paranoikami?**
 - A jeśli system się pomyli? Co wtedy?

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Jeden sensor vs. kilka sensorów
 - Oglądanie świata jednym okiem
 - **Postrzegając rzeczy jednowymiarowo, nie jesteśmy w stanie zauważyć wszystkiego**
 - Zasięg działania sensora
 - **A jeśli mamy segmenty?**
 - **A jeśli mamy VPN'a?**
 - **A jeśli mamy firewalla?**
- Korelacja zdarzeń

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Zarządzanie systemem i sygnaturami
 - Przeglądanie logów
 - System IDS/IPS też może mieć błędy
 - Reagowanie na zmiany w sieci
 - Reguły trzeba dostawać do systemów
 - Reguły trzeba uaktualniać

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Błędy systemów uczących się
 - Po co wogle system ma się uczyć?
 - Gdzie go uczyć?
 - Uczenie w trybie nadzoru?
 - Czy system można przeuczyć?

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Problemy systemów reaktywnych
 - Kontratak? Ale na kogo?
 - Jak reagować?
 - Czym reagować?
 - Czemu IPS na span-porcie jest bezsensem?
 - Inne problemy...

Sposoby ominięcia systemów IDS/IPS

- Ciągłość sesji
 - Zły adres MAC we fragmencie połączenia
 - Krótki TTL dla pakietu
 - Timeout sesji
 - Błędy reasemblacji

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Słabości porównywania łańcuchów
 - Directory traversal
 - URL encoding
 - UTF encoding

Błędy popełniane przy wykorzystywaniu systemów IDS/IPS

- Polimorficzny shellcode
 - Co to jest NOP?
 - Dlaczego NOP wskazuje na shellcode i czemu nie zawsze?
 - Mamy 55 zamienników NOPa.

Co możemy testować i jak?

- Wydajność systemu
- Reguły wykrywające ataki
- Preprocesory normalizujące ruch
- Jakość wdrożenia i zarządzania systemem IDS/IPS

Testowanie wydajności

- Co konkretnie testujemy:
- Po co to testujemy:
 - Żeby nie wprowadzać opóźnień do sieci
 - Żeby nie można było przeprowadzić ataku DoS/DDoS
- Narzędzia:
 - Stress tester: Ixia

Testowanie reguł

- **Możliwości**
 - **Przeglądanie i analiza reguł**
 - **Używanie exploitów**
 - **Dlaczego nie używać skanerów bezpieczeństwa**
 - **False Positive a False Negative**
- **Przydatne narzędzia**
 - **Metasploit,**
 - **Core Impact, CANVAS**
- **Jak wydobyć z tego informację?**

Testowanie preprocesorów

- Pierwsze pytania
 - **Czy samo testowanie reguł nie wystarczy?**
 - **Na jakim poziomie testować?**
 - **Czym testować?**
- Narzędzia
 - **Fragroute, stick, snot, nikto**
 - **IDS Informer**
- Jak interpretować wyniki testów?

Testowanie zarządzania

- Co tu wogle sprawdzać?
 - **Proces aktualizacji reguł**
 - **Proces aktualizacji oprogramowania**
 - **Sposób przechowywania i archiwizacji logów**
 - **Metody analizy logów**
 - **Politykę reakcji**
- Jak sprawdzać?
 - **Audyty wewnętrzny**
 - **Audyty zewnętrzny**

Podsumowanie - Idealny framework

- Założenia
 - **Chcemy testować pokrycie reguł i sprawność silnika**
 - **Potrzebujemy dobrej informacji zwrotnej**
 - **Chcemy móc przetestować dowolny produkt na rynku**
- Wymagania
 - **Duża baza gotowych ataków**
 - **Możliwość konstruowania własnych ataków**
 - **Możliwość swobodnej manipulacji pakietami**
 - **Możliwość emulacji/wirtualizacji celu**



Koniec

Pytania?