AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

System IPS oparty o iptables

Marcin Fabrykowski

5 lutego 2013

System IPS

Cel pracy

Celem pracy było wykonanie systemu IPS

IPS

Intrusion Prevention System

System IPS

Cel pracy

Celem pracy było wykonanie systemu IPS

IPS

Intrusion Prevention System

System IPS

Schemat działania

1. Analiza ruchu sieciowego
2. Wykrycie podejrzanych zachować
3. Reakcja na wykryte zagrożenia
4. Zapisanie danych o ataku
5. Poinformowanie o próbie ataku
6. Udostępnienie historii ataków i podjętych działań

Analiza danych

Analizowane dane

Pakiety TCP/IP

Używane narzędzie

Netfilter/iptables

Analiza danych

Analizowane dane

Pakiety TCP/IP

Używane narzędzie

Netfilter/iptables

Rozpoznawane ataki

- SSH BruteForce
- SYN Flood
- ICMP Flood
- ICMP Timestamp Request
- Skanowanie pakietami SYN
- Skanowanie funkcjami systemowymi
- Skanowanie pakietami ACK
- Spoofing z zewnątrz
- Spoofing z wewnątrz
- Złośliwe oprogramowanie

Raportowanie

Schemat raportowania

1. zapis pakietów do pliku
2. zapis pakietów do bazy danych
3. prezentacja pakietów administratorowi

Wykorzystane technologie

- iptables
- python/Django
- python/Scapy

AGH

Dziękuję za uwagę