Zarządzanie bezpieczeństwem w sieciach

mgr inż. Rafał Jachowicz, Instytut Informatyki Stosowanej PŁ

**RAPORT**

**Laboratorium nr 3**

Monitorowanie sieci za pomocą IDS

Autor raportu:

……………………………………

1. Konfigurowanie sieci.

|  |  |
| --- | --- |
| Pytania | Odpowiedź |
| Czy wszystkie komputery widzą się w sieci? |  |
| Czy z komputera sieci wewnętrznej jest dostęp do Internetu? |  |
| Czy komputer IDS ma dostęp do Internetu? |  |
| Czy komputer włamywacz ma dostęp za pomocą polecenia *ping* do komputerów sieci wewnętrznej? |  |

1. Firewall.

|  |  |
| --- | --- |
| Pytania | Odpowiedź |
| Proszę wymienić, które porty i usługi są w tym momencie przepuszczane/udostępniane na firewallu opartym o IPTables |  |

1. Raport z zadania 2 (pkt. 3 instrukcji).

|  |  |
| --- | --- |
| Pytania | Odpowiedź (proszę tutaj opisać w kilku zdaniach) |
| Co pokazało narzędzie Arpwatch? |  |
| Co pokazało narzędzie Ntop? |  |
| Ntop - Jaki był udział pakietów Unicast, Broadcast i Multicast? |  |
| Ntop - Jakie były długości pakietów? Jaka długość dominowała? |  |
| Ntop - Jaki był *TTL* pakietów? Jaka wartość dominuje, a jaka jest średnia? |  |
| Ntop - Co jeszcze można odczytać za pomocą tego narzędzia o ruchu sieciowym? |  |
| Jakie informacje udostępnia narzędzie ICMP Watch? |  |
| Co pokazało narzędzie Snort? |  |
| Co pokazało narzędzie Nmap na IDS’ie? |  |

**Oprócz odpowiedzi proszę dołączyć screeny pokazujące rezultaty powyższych narzędzi.**

1. Raport z zadania 3. Atak diagnostyczny na sieć – skanowanie portów z sieci **wewnętrznej (z komputera Klienta)**.

|  |  |
| --- | --- |
| Pytania | Odpowiedź (proszę tutaj opisać w kilku zdaniach) |
| Jaki był rezultat skanowania portów? |  |
| Co zarejestrował IDS? |  |

**Oprócz odpowiedzi proszę dołączyć screeny pokazujące rezultaty powyższych narzędzi.**

1. Raport z zadania 3. Atak diagnostyczny na sieć – skanowanie portów z sieci **zewnętrznej (z komputera włamywacza)**.

|  |  |
| --- | --- |
| Pytania | Odpowiedź (proszę tutaj opisać w kilku zdaniach) |
| Jaki był rezultat skanowania portów? |  |
| Co zarejestrował IDS? |  |

**Oprócz odpowiedzi proszę dołączyć screeny pokazujące rezultaty powyższych narzędzi.**

1. Raport z zadania 5. Testowanie programu Darkstat.

|  |  |
| --- | --- |
| Pytania | Odpowiedź (proszę tutaj opisać w kilku zdaniach) |
| Jaki był rezultat skanowania portów? |  |
| Co można było zobaczyć w programie Darkstat? |  |

**Oprócz odpowiedzi proszę dołączyć screeny pokazujące rezultaty powyższych narzędzi.**

1. Raport z zadania 5. Testowanie programu Wireshark (Windows).

|  |  |
| --- | --- |
| Pytania | Odpowiedź (proszę tutaj opisać w kilku zdaniach) |
| Jaki był rezultat skanowania portów? |  |
| Co można było zobaczyć w programie Wireshark? |  |

**Oprócz odpowiedzi proszę dołączyć screeny pokazujące rezultaty powyższych narzędzi.**