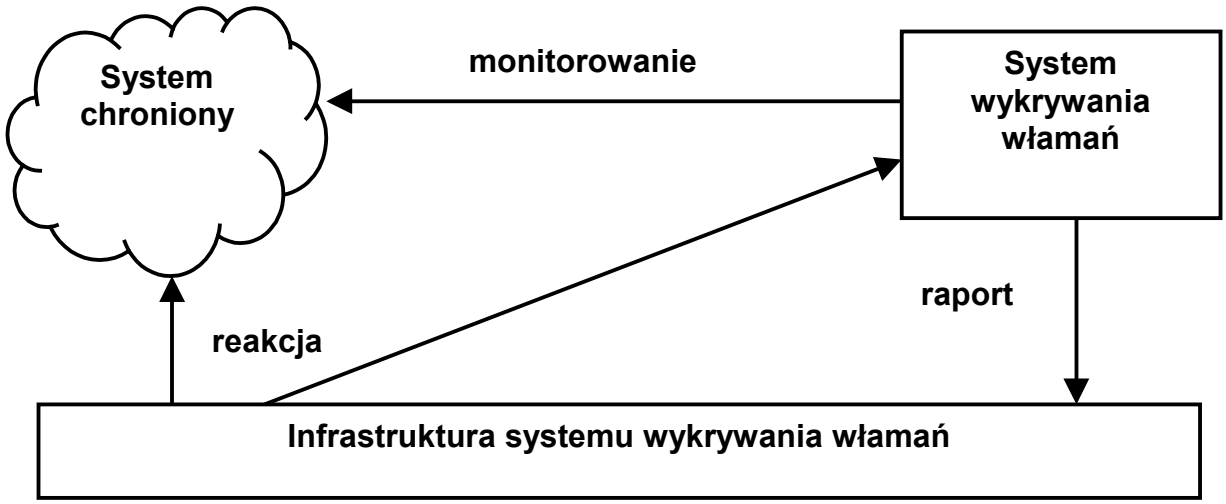
Niektóre metody ataków sieciowych:

- **Skanowanie adresów sieciowych**
- **Skanowanie adresów sieciowych,**
- **Skanowanie portów sieciowych,**
- **Analiza usług sieciowych,**
- **Wybór celu ataku sieciowego,**
- **Sondowanie luk w systemie bezpieczeństwa,**
- **Automatyczne ataki ukierunkowane na odgadnięcie haseł,**
- **Metody zaawansowane**

Koncepcja systemu wykrywania włamań

Wymagania:

- **Ciągła czujność**
- **Niewidoczność**
- **Infrastruktura**
- **Zmylenie przeciwnika**



Rysunek zaczerpnięto z:
E. Amoroso. *Intrusion Detection: Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Responce.* AT&T Inc., 1999.

Metody wykrywania włamań

Dobry system wykrywania włamań powinien stosować kilka różnych technik.

- **Przetwarzanie raportu audytu**
  - Przegląd wzorców w dostępie i użytkowaniu.
  - Odkrycie powtarzających się prób ominięcia zabezpieczeń.
  - Odkrycie zastosowania nietypowych przywilejów.
  - Odstraszanie.
  - Dodatkowa forma ochrony użytkownika.

- **Przetwarzanie na bieżąco**

- **Profile normalnego zachowania**

- **Sygnatury nienormalnego zachowania**

- **Zgodność parametrów z wzorcem**

Metody wykrywania włamań

NETWORK IDS SIGNATURE RESULTS

Attack	CVE	No. of packets	Cisco Secure IDS 2.5	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security NFR Network Intrusion Detection	Snort 1.7	Symantec NetProwler 3.5
AMD	CVE-1999-0704	11	Y	Y	N	Y	Y	N	Y	N
RDS	CVE-1999-1011	22	Y	Y	N	Y	Y	Y	Y	Y
WU-FTP	CVE-1999-0368	44	N	Y	N	N	Y	Y	Y	N
SNMP write	CAN-1999-0517	2	N	Y	N	N	Y	Y	N	N
Guest SMB login	CAN-1999-0519	19	N	Y	N	Y	Y	N	Y	N
IMAPD	CVE-1999-0005	8	Y	Y	Y	N	Y	Y	Y	N
PHF	CVE-1999-0067	10	Y	Y	Y	Y	Y	Y	Y	Y
Unicode	CVE-2000-0884	10	Y	Y	N	Y	Y	Y	Y	N
IIS 5 ISAPI	CAN-2001-0241	11	Y	Y	N	N	N	Y	Y	N
Total (out of 9)			6	9	2	5	8	7	8	2
Detect attacks fragmented (Frag-T9)			Y	Y	Y	Y	Y	Y	Y	N

Y = YES N = NO

Porównanie wykrywalności ataków przez systemy IDS,
źródło: www.networkcomputing.com, 20.08.2001

Metody wykrywania włamań

Typologia włamań.

NP1 - zewnętrzne nadużycie.
NP2 - nadużycie sprzętu.
NP3 - maskarada.
NP4 - późniejsze nadużycie.
NP5 - obejście kontroli.
NP6 - aktywne nadużycie zasobu.
NP7 - pasywne nadużycie zasobu.
NP8 - nadużycie przez zaniechanie.
NP9 - pośrednie wspomaganie.

Symptomy

- **Powtarzanie się podejrzanego działania.**
- **Omyłkowe polecenia lub odpowiedzi pojawiające się podczas wykonywania sekwencji automatycznych.**
- **Wykorzystanie znanych słabych punktów.**
- **Niespójności kierunkowe w pakietach przychodzących lub wychodzących.**
- **Niespodziewane atrybuty pewnego żądania usługi lub pakietu.**
- **Niewyjaśnione problemy z pewnym żądaniem usługi, z systemem lub środowiskiem.**
- **Zewnętrzna wiedza o włamaniu.**
- **Pojawianie się podejrzanych objawów w ruchu pakietów w sieci.**
- **Logowanie się użytkowników o dziwnych porach,**
- **Nieudane próby zalogowania się,**
- **Niewyjaśnione ponowne uruchamianie systemu lub zmiany zegara systemowego,**
- **Nieautoryzowane użycie polecenia *su*,**
- **Logowanie się użytkowników z nietypowych miejsc w sieci,**
- **Ruch sieciowy związany ze skanowaniem ICMP, portów lub połączenia z nielegalnymi portami,**
- **Niektóre operacje tworzenia lub modyfikacji plików systemowych, modyfikacji kont i praw dostępu.**

Pułapki internetowe

Internetowa pułapka jest zbiorem elementów funkcjonalnych, które posługują się legalnym i uprawnionym oszustwem w celu odwrócenia uwagi potencjalnego intruza od rzeczywistych, wartościowych zasobów poprzez użycie zasobów fikcyjnych i skierowanie intruza do systemu gromadzenia informacji wiążących się z włamaniami oraz reagowania.

Zagadnienia techniczne:

- **Wykrywanie działań, które są włamaniami**.
- **Wykrywanie działań wyzwalających**.
- **Odwołanie kwalifikacji zdarzeń jako włamania**.
- **Pozostawanie w ukryciu**.

Przygotowanie pułapki

- **Korespondencję od administratora**
- **Sfabrykowana pocztę**
- **Sfabrykowane punkty skanowania**
- **Fikcyjny plik haseł**
- **Komunikaty systemowe.**

Pułapki WWW

http://*adres_pułapki*/http://*adres_pierwotny*

Problemy:

- **Wiersz stanu przeglądarki**
- **Wiersz adresu**
- **Adresy URL wpisywane przez użytkownika**
- **Podgląd źródła dokumentu**

Pułapki internetowe

Cel stosowania pułapek:

1. **Poznanie sposobu działania intruza oraz uzyskanie informacji o technikach z jakich korzysta. Zdobytą wiedzę można użyć do lepszego zabezpieczenia sieci produkcyjnej.**
2. **Zdobycie niepodważalnych dowodów włamania, które można wykorzystać do zlokalizowania włamywacza oraz w postępowaniu prawnym.**

Umiejscowienie pułapek:

- **Tarcza (*shield*) - emulowanie niewykorzystywanych serwisów sieciowych na serwerach produkcyjnych.**
- **Pole minowe (*minefield*) - umieszczenie komputerów pułapek bezpośrednio między serwerami produkcyjnymi jako kolejnych maszyn.**
- **ZOO - całe wirtualne podsieci, które kuszą napastnika słabymi zabezpieczeniami**.

Przesłanki decyzji o zastosowaniu pułapki

- **Czy firma ma dostatecznie zasoby by pozwolić na dodatkowe maszyny pełniące role wabików?**
- **Czy jest ktoś, kto będzie czuwał nad logami i alarmami generowanymi przez system?**
- **Czy firma zamierza tropić i ścigać prawnie włamywaczy?**
- **Czy są dostępne odpowiednie środki by odpowiadać na atak?**

Specter Intrusion Detection System 5.5

Emulowane systemy operacyjne:

- Windows NT
- Windows 98
- SunOS / Solaris
- NeXTStep
- Tru64 (dawniej Digital Unix)
- Linux
- Windows2000
- MacOS
- Digital Unix
- Irix
- Unisys Unix

- Konfigurowalny stopień zabezpieczeń emulowanych systemów (pięć poziomów)
- Emulacja plików z hasłami
- Konfigurowalny stopień trudności haseł (siedem poziomów)

Emulowane serwisy:

- SMTP
- Finger
- FTP
- NetBios
- Telnet
- HTTP

Pułapki:

- POP3
- SUN-RPC
- Generic
- IMAP4
- BO2K
- DNS
- SUB-7

Verizon NetFacade 1.3

Emulowane systemy operacyjne:

- **Cisco IOS**
- **Redhat Linux**
- **SunOS 4.1.4 dla Sun Sparc**
- **IRIX**
- **Solaris**
- **Microsoft Windows NT 4.0**

Atrapy serwisów:

- FTP
- SMTP
- Echo (UDP i TCP)
- Rlogin
- Rusers (UDP)
- Telnet
- HTTP (Apache, Microsoft IIS, Netscape Enterprise)
- Daytime (UDP i TCP)
- Portmap/tcpbind (UDP i TCP)
- SSH
- IMAP
- Finger
- Mountd (UDP i TCP)

Reagowanie na incydenty

Reagowanie na incydenty składa się z decyzji i działań podejmowanych przez menedżerów zasobów w czasie rzeczywistym. Działania te mają na celu minimalizację wpływu incydentu *na zasoby* i zmniejszenie ryzyka ponownego naruszenia bezpieczeństwa. Podstawą podejmowanych decyzji i działań są dostępne świadectwa incydentu.

Reakcja zależy od zaobserwowanych czynników:

- **Jakie zasoby zostały uszkodzone? Czy mają one kluczowe znaczenie? Czy nastąpiło pogorszenie wydajności zasobu?**
- **Czy incydent wystąpił po raz pierwszy?**
- **Czy został wywołany przez źródło szkodliwe czy nieszkodliwe?**
- **Czy źródło informacji o incydencie jest wiarygodne?**
- **Jaki będzie skutek modyfikacji funkcji chronionego systemu? Czy ma to być wyłączenie wszystkich operacji? Czy ma to być odcięcie usług wewnętrznych czy zewnętrznych? Czy ma to być odcięcie usług dla zadanej lokalizacji (adresu)?**
- **Jakie będą skutki zaniechania działań? Ze względu na niepewność lub niemożność podjęcia decyzji często nie reaguje się na incydenty.**
- **Czy proponowana reakcja jest legalna i mieści się w ramach polityki bezpieczeństwa?**

Ataki wykrywane przez *IDS* w pakiecie *PGPnet*

Back Orifice	**Jolt2**	**Port Scanning**
Bonk	**Land**	**Smurf**
Fraggle	**Nestea**	**SYN Flood**
IP Spoofing	**Ping Flood**	**Teardrop**
Jolt	**Ping of Death**	**UDP Flood**

Literatura:

1. S.Garfinkel, G.Spafford. *Practical Unix and Internet Security.* O'Reilly & Associates 1996 (*tłum*. RM 1997).
2. E.Amoroso, *Intrusion Detection: Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response.* AT&T Corp, 1999, (*tłum*. RM 1999).
3. D.Atkins. *Internet Security: Professional Reference.* New Riders Publishing 1997 (*tłum*. LT&P 1997)
4. M.Strebe, C. Perkins, *Firewalls. SYBEX 2000,* (*tłum.* MIKOM 2000).