Przykłady działania systemów IDS/IPS:

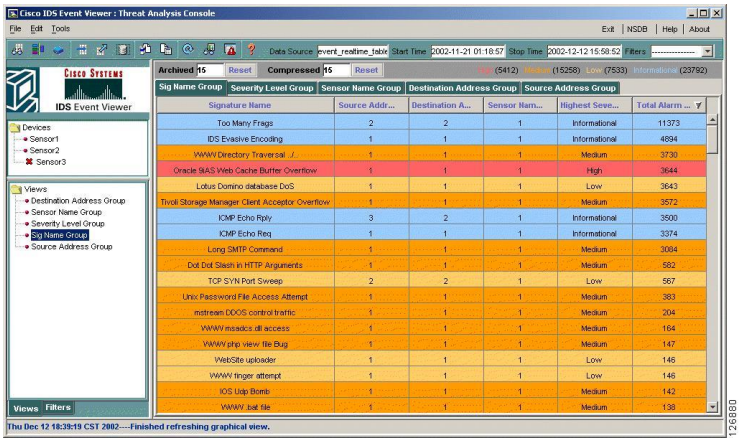
```
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2014-10-03 12:51:44

Summary:
  Total number of files:        34013
  Added files:                  3921
  Removed files:                11
  Changed files:                199


---------------------------------------------------
Added files:
---------------------------------------------------

added: /etc/aide.conf.rpmsave
added: /etc/cron.daily/mlocate
added: /etc/fake
added: /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
added: /etc/profile.d/vim.csh
```

Rys. 1. Alert systemu IDS AIDE pokazujący zmiany, które nastąpiły w wyniku przeprowadzonego ataku na sieć komputerową. Za pomocą tego ataku w systemie zostały utworzone katalogi, które nie istnieją w normalnym systemie operacyjnym.



Rys. 2. Statystyki programu CISCO IDS obrazujące ustalone poziomy ochrony według ważności danych zawartych w poszczególnych grupach. Obok wymienionych grup pokazano liczby adresów źródłowych i docelowych do nich przypisanych. W ostatniej kolumnie widoczna jest liczba alarmów jakie zostały odnotowane podczas działania sieci w określonym czasie.

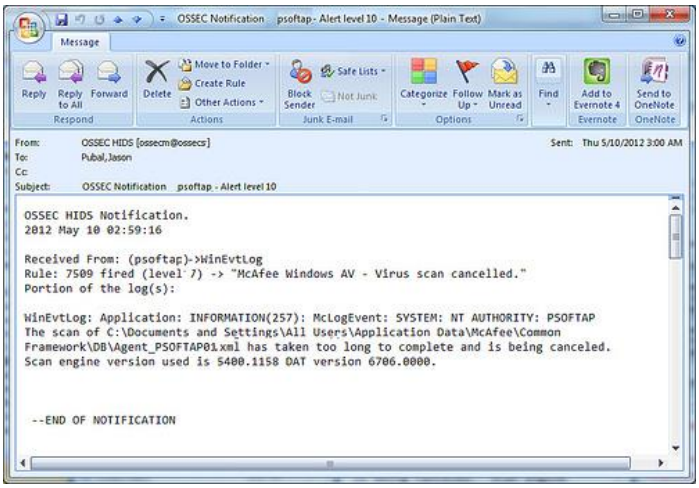
OSSEC HIDS Notification.
2011 Mar 28 03:32:35

Received From: m00->/var/log/auth.log
Rule: 5551 fired (level 10) -> "Multiple failed logins in a small period of time."
Portion of the log(s):

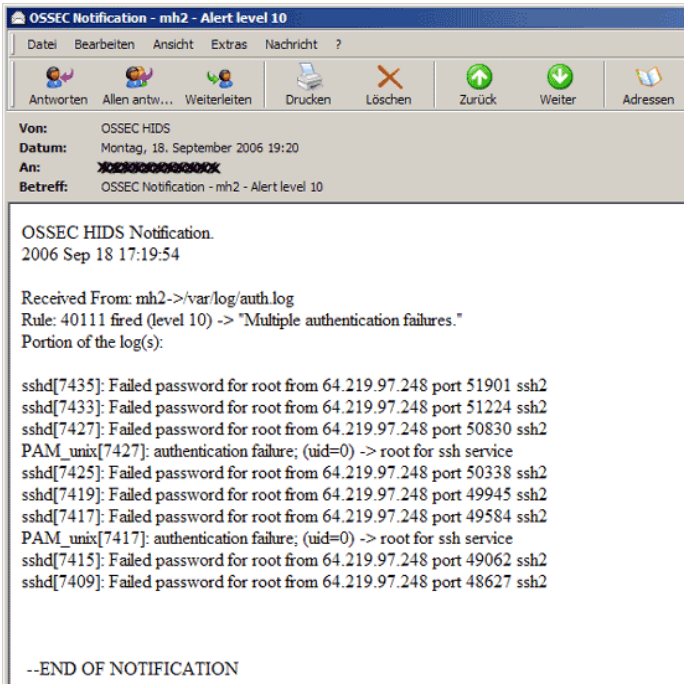
Mar 28 03:32:33 m00 sshd[13396]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root
Mar 28 03:32:31 m00 sshd[13394]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root
Mar 28 03:32:29 m00 sshd[13392]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root
Mar 28 03:32:26 m00 sshd[13390]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root
Mar 28 03:32:23 m00 sshd[13387]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root
Mar 28 03:32:21 m00 sshd[13385]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root
Mar 28 03:32:18 m00 sshd[13383]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=srv4.cclassiphosting.com user=root

--END OF NOTIFICATION

Rys. 3. Powiadomienia od oprogramowania OSSEC HIDS o wielokrotnych próbach nieudanego logowania w krótkich odstępach czasowych. Są to próby logowania do konta *root* ponawiane co 2-3 sekund w zależności od odpowiedzi. Autentykacja nie powiodła się. Jest to bardzo popularny atak, w związku z czym należy ustawiać blokowanie kont po kilkukrotnej próbie nieudanego logowania, aby nie zezwolić na udane logowanie niepowołanej osoby.

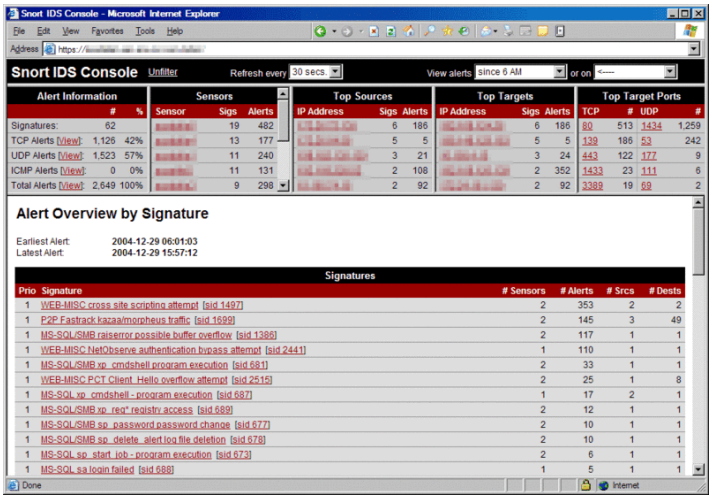


Rys. 4 OSSEC. Powiadomienie OSSEC HIDS ilustrujące akcję, gdzie system zarejestrował przerwanie skanowania dysku za pomocą oprogramowania antywirusowego McAfee Windows AV. Dołączona została również ścieżka, w którym momencie przerwany został proces skanowania oraz dodatkowe dane dotyczące antywirusa.

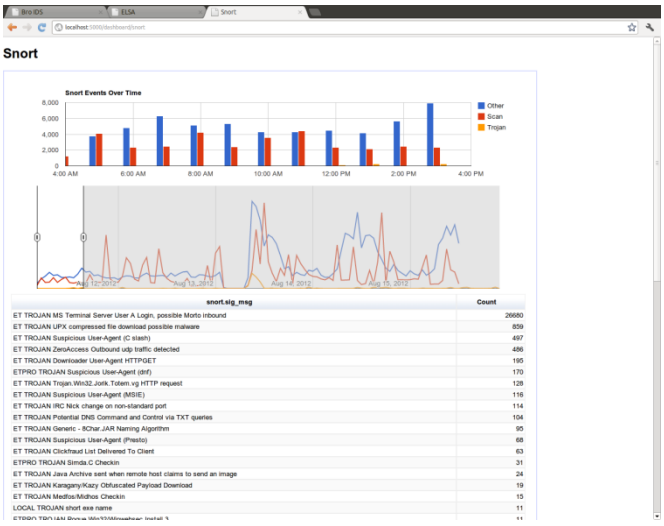


Rys. 5. Powiadomienie o niepoprawnym haśle do konta. Przesyłany jest również adres źródłowy hosta, z którego odbywała się próba logowania oraz porty przez, które uzyskiwany był dostęp.

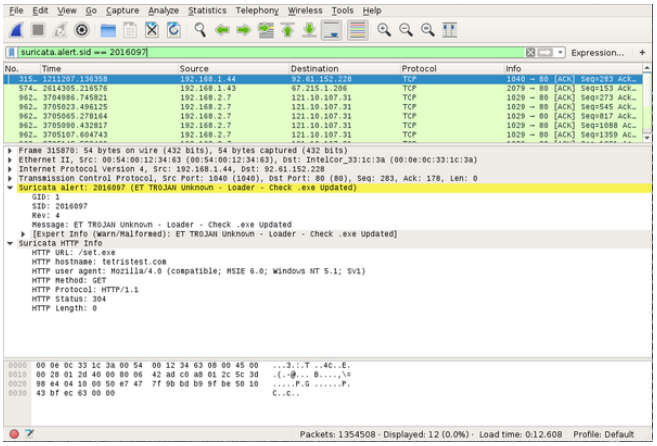
Rys. 6. Statystyki programowe SNORT IDS ilustrujące liczbę zdarzeń skanowania hostów, skanowania sieci, hostów sieciowych oraz serwerów sieciowych. Można zaobserwować również podział i liczbę zaobserwowanych anomalii w obserwowanej sieci. Poniżej widoczne są również statystyki liczbowe dla poszczególnych użytkowników.



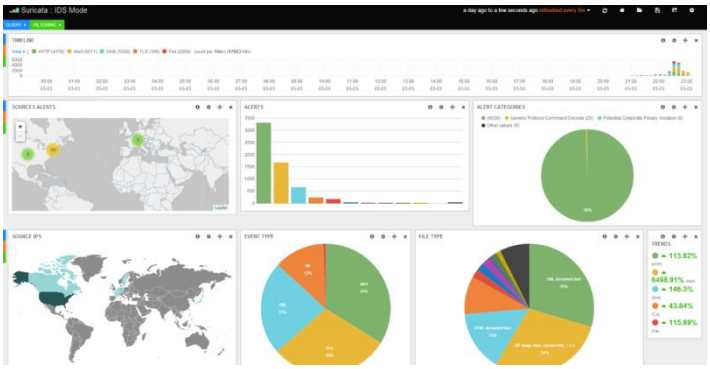
Rys. 7. Statystyki Snort IDS pokazujące jakie protokoły w sieci są najczęściej atakowane. Jest to procentowy udział odnotowanych zagrożeń. Powyższe dane są określane na podstawie wyłącznie bazy sygnatur. Przedstawione są sygnatury np. nadzorujące ruch w sieciach p2p, obserwujące próby logowania do kont lub baz danych, uruchamiania skryptów lub programów, dostępu do rejestru, zmian haseł, usuwania plików lub logów. Sygnatury posiadają odpowiednio dobraną liczbę sensorów. Dane posortowano według odnotowanych alertów przez system Snort IDS.



Rys. 8. Raport systemu IDS SNORT obrazujące godziny, w których zabezpieczony system był skanowany. Odnotowano użycie Trojanów oraz innych niewyszczególnianych anomalii. Snort sig msg przedstawia liczbę zdarzeń zarejestrowanych.



Rys. 9. Obraz systemu SURICATA przedstawiający moment wykrycia Trojana w sieci. Program pozwala określić adres docelowy, gdzie przesłany został zainfekowany plik, adres źródłowy skąd pochodzi atak oraz protokół po jakim jest przesyłany (w tym przypadku jest to protokół TCP).



Rys. 10. Statystki systemu SURICATA IDS. Wykres zawiera odnotowane niepożądane zdarzenia wyłącznie w godzinach 21.00-23.15. Przedstawione mapy pozwalają określić lokalizację zarejestrowanych zdarzeń na poziomie kraju. Poniżej zaobserwować można dane, wyróżniające procentowe podziały typów zdarzeń oraz podział plików fizycznych, które są najbardziej narażone na np. przechwycenie w obserwowanym przez nas systemie.

W celu zapewnienia właściwego poziomu bezpieczeństwa infrastrukturze teleinformatycznej należy jednocześnie ją monitorować i kontrolować. Zapewnia to połączenie technologii IDS z technologią IPS. Wdrożony system NIDS/NIPS wymaga ciągłego dostosowywania go do zmieniających się zagrożeń jak i charakteru ruchu sieciowego. W procesie tym bardzo ważnym aspektem jest dokumentowanie wprowadzanych sygnatur i poleceń w celu zachowania przejrzystości, czytelności i odtwarzalności – na wypadek ewentualnej przebudowy systemu.

Przykłady systemów IDS.

KFSensor

KFSensor jest komercyjnym programem opartym o technologię IDS - honeypot dedykowanym dla systemu Windows. Działa poprzez symulację wrażliwych usług systemowych oraz koni trojańskich. Dzięki swoim funkcjom zapewnia wyższy poziom informacji niż te oferowane przez zapory sieciowe. Jest zarządzany za pomocą graficznego interfejsu, działa na najwyższym poziomie modelu OSI – warstwie aplikacji. Wyposażony jest w demon usług internetowych, który obsługuje wiele portów i adresów IP oraz rejestruje w dzienniku każdy bajt ataku. Wydarzeniom mogą być przypisane różne stopnie zagrożenia opisane kolorami, dzięki czemu łatwo jest dostrzec coś niezwykłego lub poważnego. Można zdefiniować raporty niestandardowe i filtrację dziennika, aby wyświetlić tylko te z portów, protokołów lub źródłowego adresu IP, na których wystąpiło zdarzenie. Istnieją dwa główne komponenty systemu KFSensor: KFSensor Server oraz KFSensor Monitor. KFSensor Server

zapewnia podstawową funkcjonalność systemu, słucha zarówno portów TCP jak i UDP na komputerze, współdziała z odwiedzającymi oraz generuje wydarzenia. Nie posiada interfejsu użytkownika i działa w tle. KFSensor Monitor zawiera interfejs użytkownika systemu KFSensor, służy do konfiguracji serwera KFSensor oraz monitorowania zdarzeń generowanych przez KFSensor Server.

STerm

STerm jest klientem Telnet, cechującym się unikatową funkcjonalnością. Tworzy dwukierunkową sesję usługi Telnet z hostem docelowym podszywając się pod zaufanego hosta. Używa technik ARP Poisoning, MAC Spoofing oraz IP Spoofing, aby ominąć listy dostępowe ACL, zasady zapory i protokołu IP na serwerach i urządzeniach sieciowych.

IRS

IRS jest programem którego głównym celem jest skanowanie adresów IP, pod względem ograniczeń określonych w listach kontroli dostępu, filtracji adresów IP, reguł zapory dla danej usługi na hoście. Łączy w sobie techniki "ARP Poisoning" i "Half-Scan", które próbują połączyć się z wybranym portem celu wykorzystując podszycie się pod połączenia TCP. IRS nie jest skanerem portów ale skanerem „ważnych źródłowych adresów IP" dla danej usługi.

Źródła:

* http://sekurak.pl/wprowadzenie-do-systemow-ids/
* http://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html
* http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BSW1-0109-0014
* http://edu.pjwstk.edu.pl/wyklady/bsi/scb/index82.html
* http://security.psnc.pl/files/szkolenia/KDM_070517.pdf
* http://1.bp.blogspot.com/-LGaxEuLwTtI/Uxc37RLW8AI/AAAAAAAAAb8/7z6QKA9PJjc/s1600/suricata.PNG
* http://xmodulo.com/host-intrusion-detection-system-centos.html
* https://www.howtoforge.com/intrusion_detection_with_ossec_hids
* http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.html
* https://commons.wikimedia.org/wiki/File:Snort_ids_console.gif
* https://danielparraz.wordpress.com/2011/03/28/ossec-hids-how-cool-is-it/
* https://www.softether.org/1-features/3._Security_and_Reliability

https://www.tenable.com/blog/securitycenter-42-and-community-dashboard-site-released