JAK SAMEMU ZDIAGNOZOWAĆ BEZPIECZEŃSTWO SWOJEGO SERWERA

Borys Łącki

20/21.11.2017

Od ponad 10 lat wykonując testy penetracyjne, ***testujemy bezpieczeństwo i zabezpieczamy*** *zasoby Klientów.*

LOGICALTRUST

aruba CLOUD

AGENDA

1) Incydenty komputerowe
2) Bezpieczeństwo serwerów – najważniejsze problemy
3) **Pomysły** i narzędzia
4) DEMO
5) Podsumowanie
6) Sesja pytań od uczestników

RANSOMWARE - APLIKACJA

Hackers now hit MySQL databases with ransomware

Hundreds of MySQL databases have been subject to ransomware attacks with hackers deleting data and replacing them with a ransom demand for 0.2 bitcoin.

According to a blog post by Ofri Ziv, who leads the Detecion team at Guardicore, the attacks look like an evolution of the MongoDB ransomware attacks first reported earlier this year by Victor Gevers.

He said that hundreds of databases were affected by the attacks, which began on February 12 and lasted 30 hours, and which were all traced back to one IP address, 109.236.88.20, an IP address hosted by worldstream.nl, a Netherlands-based web hosting company.

Hackers now hit MySQL databases with ransomware

The hosting company was notified and the attacks and Ziv said the suspected the attacker was “running from a compromised mail server which also serves as HTTP(s) and FTP server.”

DANE KLIENTÓW

GitLab.com melts down after wrong directory deleted, backups fail

Upstart said it had outgrown the cloud – now five out of five restore tools have failed

By Simon Sharwood, APAC Editor 1 Feb 2017 at 02:02 143 SHARE ▼

Source-code hub GitLab.com is in meltdown after experiencing data loss as a result of what it has suddenly discovered are ineffectual backups.

REPUTACJA / PRZESTĘPSTWO

Ponad tysiąc polskich stron WWW zarażało odwiedzających je internautów

Adam dodał 21 czerwca 2017 o 13:19 w kategorii Włamania z tagami: atak • exploit kit • Polska • wodopój

Czasem w świecie bezpieczeństwa zdarza się, że analiza przypadku jednej ofiary prowadzi do identyfikacji setek kolejnych. Poniżej znajdziecie opis takiego właśnie ciągu odkryć przeprowadzonych przez zespół firmy Exatel.

Ataki wodopoju, czyli takie, w których atakujący czeka cierpliwie aż ofiary same do niego przybędą, nie są nam obce. Patrząc tylko na nasze podwórko – niedawno wodopojem były chociażby witryny KNFu czy Urzędu Rejestracji Produktów Leczniczych. Rzadko jednak zdarza się odkryć sieć ponad tysiąca polskich witryn, kontrolowanych z jednego miejsca i regularnie infekujących odwiedzających je internautów.

STRATY FINANSOWE

11 million Euro loss in VoIP fraud .. and my VoIP logs

And the attackers made over 1 million in profits.

This just emerged from a raid (and hearing apparently) in Romania and other countries. The two main persons being fingered are Catalin Zlate and Cristian Ciuvat. It seems that they were scanning for PBX servers with phone extensions that have weak passwords. Then they abused these accounts to make phone calls for "free", except that free has the price of 11 million EUR for the victims!

UTRATA DANYCH, DOSTĘPNOŚCI

Hałas spowodowany wyrzutem gazu uszkodził dyski w serwerowni ING

Adam dodał 12 września 2016 o 15:17 w kategorii Info z tagami: awaria • dysk • hałaś • Inergen • ING

Do niecodziennego incydentu doszło w głównej serwerowni ING w Bukareszcie. W trakcie testów instalacji gaśniczej uszkodzeniu uległy liczne dyski twarde, powodując wielogodzinną awarię większości systemów banku.

Sobotnie popołudnie nie było łatwe dla klientów ING w Rumunii. Awaria, która rozpoczęła się ok. godziny 13, dotknęła większości systemów banku. Nie działały bankomaty ani płatności kartami, nie można było dostać się do strony WWW banku ani do systemu bankowości elektronicznej. Usługi udało się przywrócić dopiero ok. 23.

DANE OSOBOWE

Poważny wyciek informacji z firmy InPost – dane ponad 50 tysięcy osób, hasła

Adam dodał 23 sierpnia 2017 o 23:15 w kategorii Włamania, Wpadki z tagami: baza • Cebulka • dane • InPost • wyciek

W sieci pojawił się wczoraj zrzut bazy danych należącej do firmy InPost. Baza zawiera między innymi szczegółowe dane ponad 50 tysięcy pracowników i współpracowników oraz informacje o współpracy z organami ścigania.

Na najpopularniejszym polskojęzycznym forum w sieci Tor, zwany Cebulka, pojawił się wczoraj wpis nowego użytkownika, który twierdził, że włamał się do systemów firmy InPost. Na dowód swoich słów zamieścił linka do danych wykradzionych z serwerów firmy. Dane niestety wyglądają wiarygodnie. Tak wyglądał wpis użytkownika hackmachine:

Cebulka » Rekrutacja » inpost

Strony 1 — Napisz odpowiedź

Posty [1]

hackmachine
Obserwator
Zarejestrowany: Wczoraj
Posty: 4
Punkty: 0

Dzisiaj AM — 1

Temat: inpost

Pozostałości po włamie do sieci inpostu, w paczace takie rzeczy jak:
- baza danych portalu od administracji bezpieczeństwem informacji (o ironio):
  * spis pracowników w tym: imię, nazwisko, pesel, seria dokumentu, data rozpoczęcia i zakończenia pracy + numery telefonów i adresy skrzynek e-mail tych ważniejszych
  * spis budynków należących do firmy, w tym dokładny opis zabezpieczeń fizycznych
  * od zajebania innego gówna
- print z ustawieniami konsoli do zarządzania paczkomatami (miejsce gdzie przechowywane są dane do paczek)
- dane logowania do dwóch serwerów smtp

RANSOMWARE - KOREA

Sprzedał firmę hostingową by zapłacić milion dolarów okupu za ransomware

Adam dodał 19 czerwca 2017 o 23:36 w kategorii Włamania, Złośniki z tagami: hosting • Korea Południowa • milion dolarów • okup • ransomware

W dalekiej Korei Południowej rozgrywa się właśnie dramat właściciela firmy hostingowej Nayana, której wszystkie serwery zaszyfrował ransomware Erebus. Właściciel sprzedał firmę i oddał cały majątek by odzyskać dane klientów.

W ostatnią sobotę 10 czerwca ok. godziny 1:30 czasu lokalnego 3400 klientów południowokoreańskiej firmy hostingowej Nayana straciło dostęp do swoich danych. Firma poinformowała, że padła ofiarą ransowmare Erebus, które zaszyfrowało dyski 153 jej serwerów. Niestety wszelkie próby odzyskania danych zawiodły i właściciel firmy stanął przed trudnym wyborem.

“Chcę mieć Bezpieczny Serwer”

- Co jest dla mnie ważne i jak bardzo? (poufność vs. dostępność)
- Co mi grozi?

BEZPIECZEŃSTWO – CO ROBIĆ?

- Wiedzieć
- Podnosić koszty atakującym
- Szybko reagować
- Podnieść się po skutecznym incydencie jak najszybciej

ARUBA – TEMATY WEBINARÓW

- Hasła
- Aktualizacje
- Kopie zapasowe
- Bezpieczeństwo systemowe
- Bezpieczeństwo aplikacji

NAJCZĘSTSZE PROBLEMY

- Słabe hasła
- Brak aktualizacji
- Brak ograniczeń sieciowych
- Domyślna konfiguracja
- Zbędne zasoby
- Błędne uprawnienia
- Brak kopii zapasowych

HASŁA

pwgen -s

JaxXDYa7iCDB1yM5pUVn

- Zmiana portów (?!)
- Rekonfiguracja usług (klucze, wymuszanie polityki haseł, itp..)

Hashcat / John the Ripper

 # john ./shadow

Loaded 23 password hashes with 23 different salts

HASŁA - ONLINE

Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SuvV46] [service://server[:PORT][/OPT]]

Options:

-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE

-p PASS or -P FILE try password PASS, or load several passwords from FILE

Fail2ban

** Starting authentication failure monitor fail2ban [OK]*

AKTUALIZACJE - SYSTEMOWE

CRON-APT RUN [/etc/cron-apt/config]: Mon Nov 20 04:00:01 CET 2017

CRON-APT SLEEP: 2154, Mon Nov 20 04:35:55 CET 2017

CRON-APT ACTION: 3-download

CRON-APT LINE: /usr/bin/apt-get -o quiet=1 dist-upgrade -d -y -o APT::Get::Show-Upgraded=true

Reading package lists...

Building dependency tree...

Reading state information...

The following packages will be upgraded:

libssl-dev libssl-doc libssl1.0.0 lynx lynx-cur openssl procmail

7 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

aruba CLOUD

AKTUALIZACJE - APLIKACJE

An update to WordPress 4.7.7 (zwolnienie zabezpieczeń) is now available for the WordPress installations you are managing using Installatron.

The changes for this version are:

WordPress 4.7.7 is now available. This is a security release for all previous versions and we strongly encourage you to update your sites immediately.

Proces aktualizacji Moje Blog dostępnej z adresu x powiódł się.

Nowa zainstalowana wersja: 4.7.7

SUMY KONTROLNE

 # debsums | grep -vw OK

/bin/ps FAILED

1) find /var/www/ -exec sha512sum {} \; > sums

2) sha512sum -c sums

/var/www/html/index.html: DOBRZE

ZBĘDNE ZASOBY - UPRAWNIENIA

$ umask

0002

$ touch aaa

$ ls -l aaa

-rw-rw-r-- aaa

$ umask 0077

$ touch bbb

$ ls -l bbb

-rw------ bbb

ZBĘDNE ZASOBY

Test, Staging, Production

find /home/user/ -type f -mtime -5 -exec ls -ld {} \;

*find /tmp/ -iname "*sql*" -o -iname "*back*" -o -iname "*dump*"*

FIREWALL

- *netstat – lokalnie*
- *nmap - zdalnie*

CIS BENCHMARK

3.14 Verify that Docker server certificate key file permissions are set to 400 (Scored)

Profile Applicability:

- Level 1 - Docker

Description:

Verify that the Docker server certificate key file (the file that is passed alongwith '`--tlskey`' parameter) has permissions of '`400`'.

Rationale:

The Docker server certificate key file should be protected from any tampering or unneeded reads. It holds the private key for the Docker server certificate. Hence, it must have permissions of '`400`' to maintain the integrity of the Docker server certificate.

Audit:

Execute the below command to verify that the Docker server certificate key file has permissions of '`400`':

```
stat -c %a <path to Docker server certificate key file>
```

Remediation:

```
chmod 400 <path to Docker server certificate key file>
```

This would set the Docker server certificate key file permissions to '`400`'.

Impact:

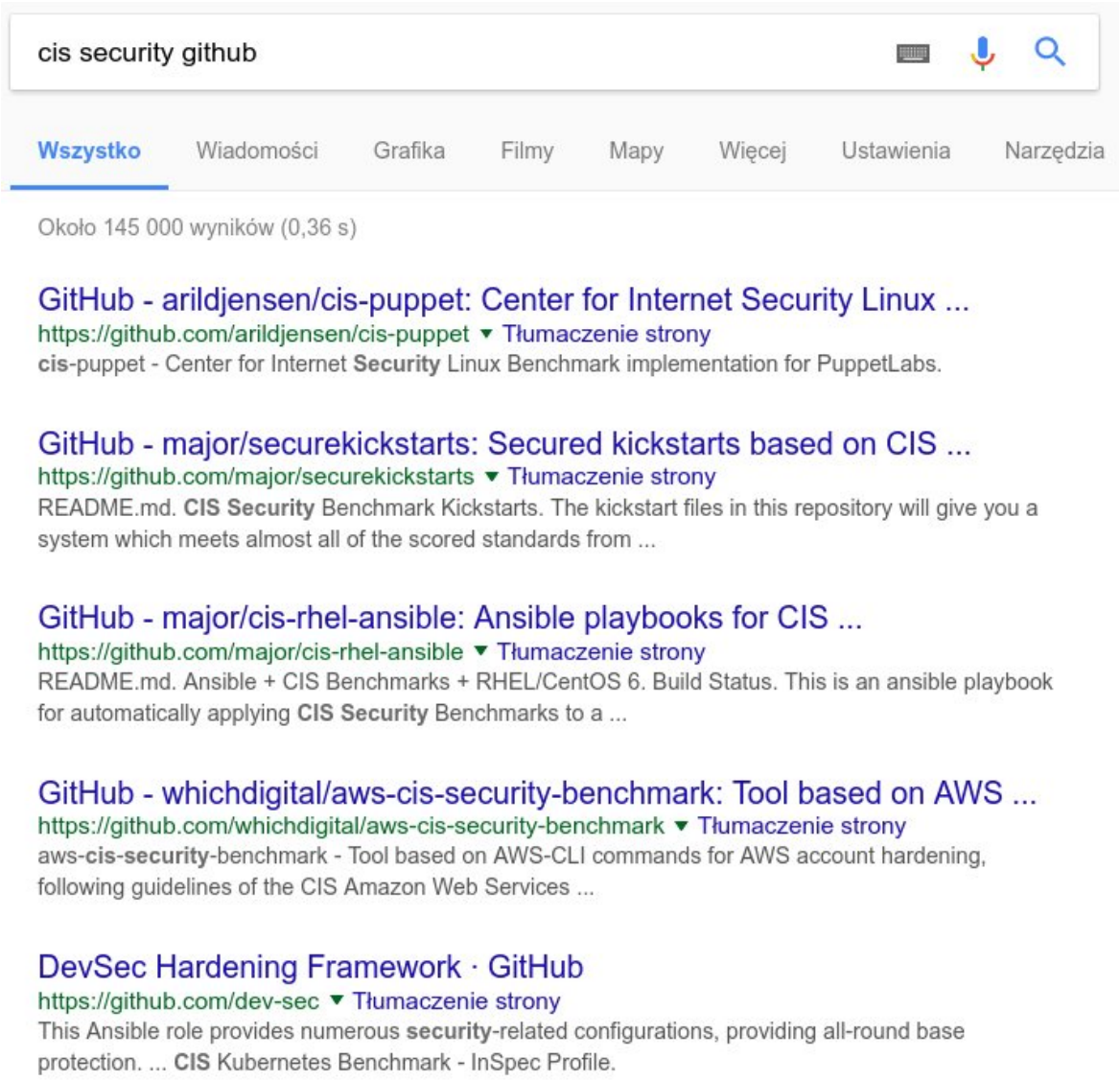
None.

Default Value:

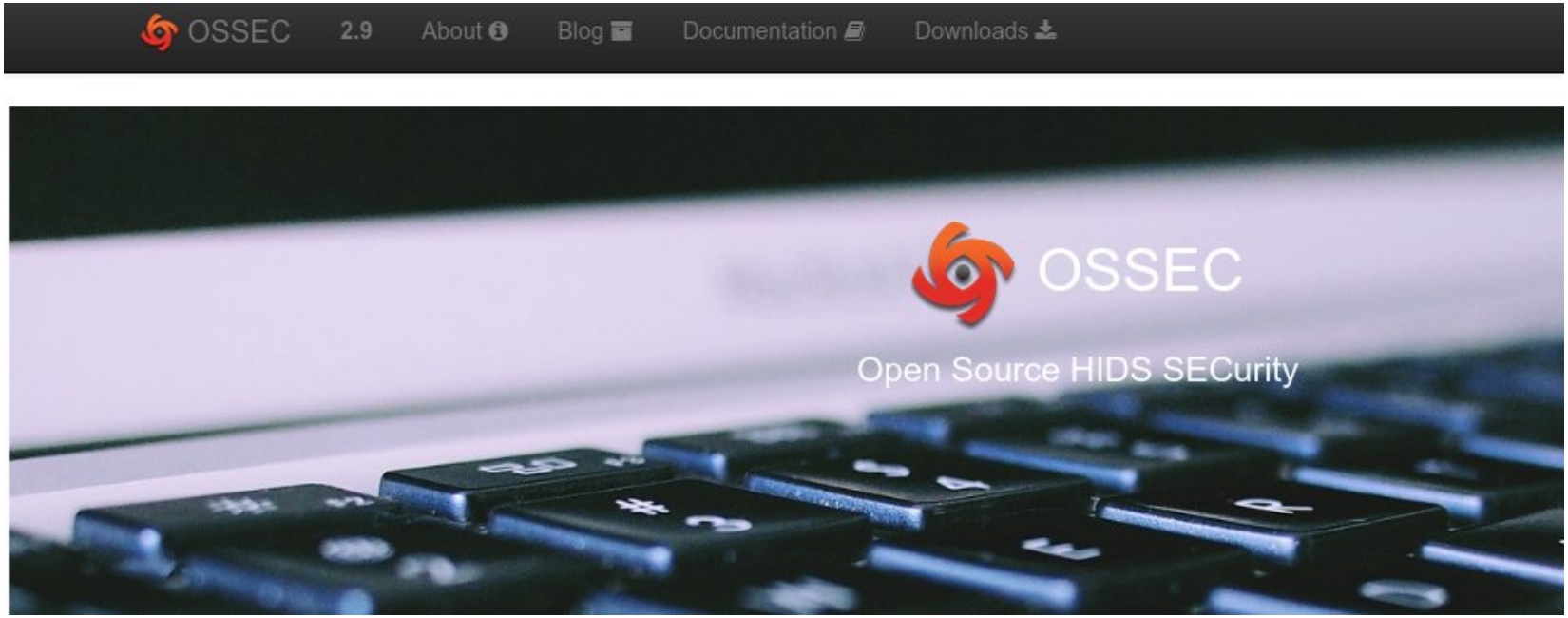
By default, the permissions for Docker server certificate key file might not be '`400`'. The default file permissions are governed by the system or user specific `umask` values.

aruba CLOUD

AUTOMATYCZNA WERYFIKACJA



NARZĘDZIA - OSSEC



NARZĘDZIA – UNIX-PRIVESC-CHECK

unix-privesc-check

Unix-privesc-checker is a script that runs on Unix systems (tested on Solaris 9, HPUX 11, Various Linuxes, FreeBSD 6.2). It tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases).

It is written as a single shell script so it can be easily uploaded and run (as opposed to un-tarred, compiled and installed). It can run either as a normal user or as root (obviously it does a better job when running as root because it can read more files).

windows-privesc-check

A long time ago, I started writing a tool to look for local privilege escalation vectors on Windows systems – e.g. weak permissions on files, directories, service registy keys. I never quite got round to finishing it, but the project could still be useful to pentesters and auditors in its current part-finished state.

I'd suggest giving it a try next time you do a security audit with local administrator rights, or next time you get a non-admin logon to a Windows system during a pentest. It was designed to be useful for both.

NARZĘDZIA - LYNIS

```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts...                [ OK ]
  - Checking UIDs...                                [ OK ]
  - Checking chkgrp tool...                         [ FOUND ]
  - Consistency check /etc/group file...            [ OK ]
  - Test group files (grpck)...                     [ OK ]
  - Checking login shells...                        [ WARNING ]
  - Checking non unique group ID's...               [ OK ]
  - Checking non unique group names...              [ OK ]
  - Checking LDAP authentication support            [ NOT ENABLED ]
  - Check /etc/sudoers file                         [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] Shells
------------------------------------
  - Checking console TTYs...                        [ WARNING ]
  - Checking shells from /etc/shells...
    Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] File systems
------------------------------------
  - [FreeBSD] Querying UFS mount points (fstab)...  [ OK ]
  - Query swap partitions (fstab)...                [ OK ]
  - Testing swap partitions...                      [ OK ]
  - Checking for old files in /tmp...               [ WARNING ]
  - Checking /tmp sticky bit...                     [ OK ]
```

DEMO

DOBRE PRAKTYKI

- Oddzielaj - dostęp do aplikacji
- Aktualizuj - oprogramowanie
- Weryfikuj - ustawienia
- Ograniczaj - uprawnienia
- Porządkuj - dane
- Monitoruj - zasoby
- Dokumentuj - procesy
- Automatyzuj

SZKOLENIA - RABAT

https://z3s.pl/szkolenia/

Atak i obrona:

- **Bezpieczeństwo aplikacji WWW**
- **Bezpieczeństwo aplikacji mobilnych**

-10%

Obowiązuje 10 dni
Hasło: 9oeAM

Dziękuję za uwagę

Borys Łącki

b.lacki@logicaltrust.net

www.arubacloud.pl