



UNDERSTANDING CYBER KILL CHAIN'S FIRST STEP: INFORMATION RECONNAISSANCE

Challenge description

11/09/2019
European Cyber Security Challenge 2019
Bucharest, Romania

1. Initial Write-Up

As a security researcher, you received a hint that sensitive data, like administrator pass, is being exposed over the internet from a restaurant's website. Sadly, the message has been damaged, only a picture could be recovered. Use OSINT tools and tactics to find which website it was and see if you can truly find the possible administrator password and notify the owner of the website.

Warning! This is a drill with live, operational environment. Only passive reconnaissance is allowed, no active scanning or brute forcing shall be applied. All legal consequences of breaking this rule is the responsibility of those conducting it

2. Challenge specifications

- Category: OSINT tools and skills/ analyst mindset
- Difficulty : Easy
- Expected time to solve: <2h

3. Technical specifications

- Distribute the attached GIF to the participants

4. Questions and answers

1. CTF Specific questions:
 - a. Question 1: What is the originating website (**www.rosrestaurant.com**)
 - b. Question 2: What is the possible administrator password (**WK7JNgYcDkzac**)
 - c. How is it possible to obtain information from OSINT methods? (**Due to crawled data indexed by search robots, most of the required information to conduct successful attack**)

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance
Bucharest, Romania **11/09/2019**

against weak services is available from open source intelligence. Some data says 80% of the sensitive, and critical data to breach a system is available in open databases.)

- d. What are the google dorks to be used to uncover relevant information? ('Site', 'Index Of', 'intext' 'intitle')
 - e. Can you use the obtained password to further investigate the problem? (**Actually, without permission this is a solid nope**)
 - f. Where is the administrator password located? (**In the _vti_private folder, service.pwd file**)
 - g. What functionality allows the attacker to simply uncover the administrator password? (**'Index of' functionality, to provide the catalogue of webserver**)
 - h. How could you possibly remediate this issue? (**Turn off index of functionality, if business need are not requesting such catalogue to be publicated**)
2. Non-Flag specific:
- a. Question 1: Are you allowed to exploit this vulnerability?
 - i. yes
 - ii. no
 - iii. **yes, if I have permission from the owner**
 - iv. yes, if I'm not going to change or manipulate the data stored in the system
 - b. Question 2: What is the recommended action if you gain attention to such a vulnerability?
 - i. exploit the vulnerability, and create a complete test report on possible effect
 - ii. **conduct an assesment of possible threats, and send notification to the site owner without exploiting the vulnerability**
 - iii. leave it alone
 - iv. store it for later exploiting
3. Open Questions:
- a. OSINT techniques provide the first step in cyber kill chain, why is it necessary to conduct OSINT before attack?
 - i. **OSINT techniques reveal information from public data, and therefore they're visible for all internet users, also for malicious attackers**
 - ii. **It is confirmed, that 80% of data leading to a compromising attack is available in public sources.**
 - iii. Search engines are trained to provide vulnerability information with specific commands
 - iv. OSINT provides minimal data, therefore additional steps should be taken to compromise a system
 - b. How google dorks can help conducting OSINT tasks
 - i. **Google dorks are designed to narrow the search results by filtering specific background data collected by the survey robots**
 - ii. Google dorks are designed for hackers
 - iii. **Google dorks are using built-in functionality of google search engine, and can find specific data, which can not be find through key-word or free search**

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance
Bucharest, Romania **11/09/2019**

- iv. Google dorks are designed by malicious users, and the usage of them is prohibited by law
- c. INDEX OF is a normal functionality on web servers, what is your suggestion to avoid information leaking through this vulnerable 'service'?
 - i. Switch 'index of' completely off on webservers
 - ii. Assign permission to each user
 - iii. Create white list
 - iv. **Disable the service unless business needs requires to enable it**

5. Attack Scenario

As a security researcher you received a hint that sensitive data, like administrator pass, is being exposed over the internet from a restaurant's website. Sadly the message has been damaged, only a picture could be recovered. Use OSINT tools and tactics to find which website it was and see if you can truly find the possible administrator password and notify the owner of the website. It is possible, that the attack hasn't occurred yet, but due to the high risk factor the participants might help to prevent a successful attack. Due to the high activities of botnets, it is likely, that another botnet perk will be assimilated, if the owner neglects necessary countermeasures.

6. Installation instructions

The scenario is based on existing public data, therefore no setup required

7. Tools needed

Description:

The challenge is supposed to teach OSINT techniques therefore no specific tools needed

8. Artefacts Provided

GIF file from the damaged message ZIP-ed

Name	Format	Comment	Checksum (SHA256)
------	--------	---------	-------------------

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance
Bucharest, Romania

11/09/2019

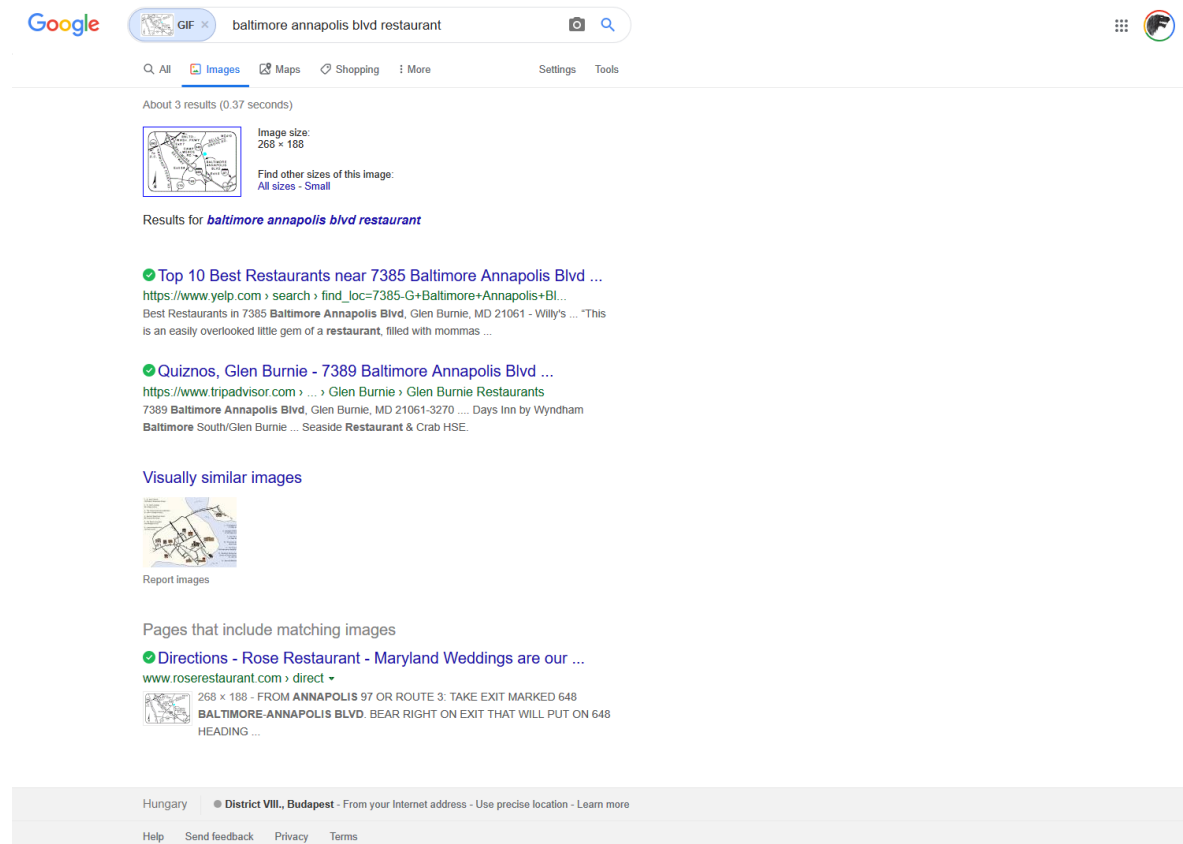
Artifact GIF	GIF	Password:	138392a1c2272b309f05b9c32ee2b99eb2328d5d3a12a7a64ba2ae37a4584b02
-------------------------------	------------	------------------	---

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance

Bucharest, Romania 11/09/2019

9. Walkthrough (writeup)

1., Analyze the picture. Reverse search will not help, but googling for the address and restaurant keyword will.



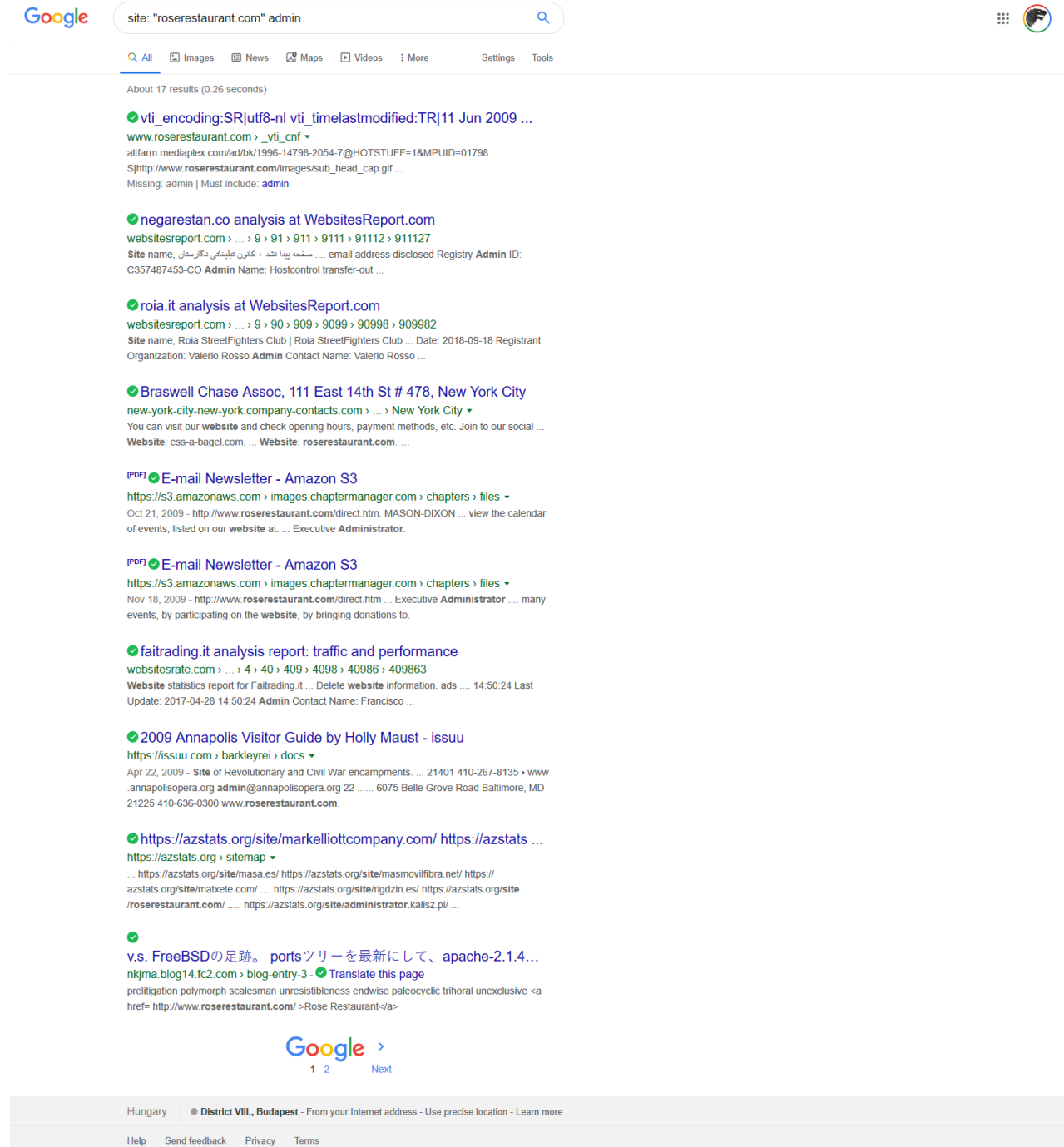
The screenshot shows a Google search interface. The search bar contains the text "baltimore annapolis blvd restaurant". Below the search bar, there are tabs for "All", "Images", "Maps", "Shopping", and "More". The "Images" tab is selected. Below the tabs, it says "About 3 results (0.37 seconds)". There is a small map thumbnail showing a location in Baltimore, Maryland. Below the map, there is a link to "Results for baltimore annapolis blvd restaurant". The search results list several restaurants near 7385 Baltimore Annapolis Blvd, including "Top 10 Best Restaurants near 7385 Baltimore Annapolis Blvd ..." and "Quiznos, Glen Burnie - 7389 Baltimore Annapolis Blvd ...". There is also a section for "Visually similar images" and "Pages that include matching images", which includes a link to "Directions - Rose Restaurant - Maryland Weddings are our ...". At the bottom of the page, there is a location bar showing "Hungary" and "District VIII., Budapest".

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance

Bucharest, Romania

11/09/2019

2., Use google dorks to further explore the site (only passive tools are allowed, no dirbuster, etc)



Google search results for "roserrestaurant.com" admin. The search returned 17 results in 0.26 seconds.

- vti_encoding:SR|utf8-nl vti_timelastmodified:TR|11 Jun 2009 ...**
www.roserrestaurant.com > _vti_cnf ▾
altfarm.mediaplex.com/ad/bk/1996-14798-2054-7@HOTSTUFF=1&MPUID=01798
S|http://www.roserrestaurant.com/images/sub_head_cap.gif ...
Missing: admin | Must include: admin
- negarestan.co analysis at WebsitesReport.com**
websitesreport.com > ... > 9 > 91 > 911 > 9111 > 9112 > 911127
Site name, Roia StreetFighters Club | Roia StreetFighters Club ... Date: 2018-09-18 Registrant Organization: Valerio Rosso Admin Contact Name: Valerio Rosso ...
- roia.it analysis at WebsitesReport.com**
websitesreport.com > ... > 9 > 90 > 909 > 9099 > 90998 > 909982
Site name, Roia StreetFighters Club | Roia StreetFighters Club ... Date: 2018-09-18 Registrant Organization: Valerio Rosso Admin Contact Name: Valerio Rosso ...
- Braswell Chase Assoc, 111 East 14th St # 478, New York City**
new-york-city-new-york.company-contacts.com > ... > New York City ▾
You can visit our website and check opening hours, payment methods, etc. Join to our social ...
Website: ess-a-bagel.com. ... Website: roserrestaurant.com. ...
- E-mail Newsletter - Amazon S3**
https://s3.amazonaws.com > images.chaptermanager.com > chapters > files ▾
Oct 21, 2009 - http://www.roserrestaurant.com/direct.htm: MASON-DIXON ... view the calendar of events, listed on our website at: ... Executive Administrator.
- E-mail Newsletter - Amazon S3**
https://s3.amazonaws.com > images.chaptermanager.com > chapters > files ▾
Nov 18, 2009 - http://www.roserrestaurant.com/direct.htm ... Executive Administrator ... many events, by participating on the website, by bringing donations to.
- faitrading.it analysis report: traffic and performance**
websitesrate.com > ... > 4 > 40 > 409 > 4098 > 40986 > 409863
Website statistics report for Faitrading.it ... Delete website information, ads ... 14:50:24 Last Update: 2017-04-28 14:50:24 Admin Contact Name: Francisco ...
- 2009 Annapolis Visitor Guide by Holly Maust - issuu**
https://issuu.com > barkleyrei > docs ▾
Apr 22, 2009 - Site of Revolutionary and Civil War encampments. ... 21401 410-267-8135 • www .annapolisopera.org admin@annapolisopera.org 22 6075 Belle Grove Road Baltimore, MD 21225 410-636-0300 www.roserrestaurant.com.
- https://azstats.org/site/markelliottcompany.com/ https://azstats ...**
https://azstats.org > sitemap ▾
... https://azstats.org/site/masa.es/ https://azstats.org/site/masmovilibra.net/ https://azstats.org/site/matxete.com/ ... https://azstats.org/site/rigdzn.es/ https://azstats.org/site/roserrestaurant.com/ https://azstats.org/site/administrator.kalisz.pl/ ...
- v.s. FreeBSDの足跡。 portsツリーを最新にして、 apache-2.1.4...**
nkjma blog14.fc2.com > blog-entry-3 - Translate this page
prelligation polymorph scalesman unresistiblenss endwise paleocyclic trihoral unexclusive Rose Restaurant


Google >
1 2 Next

Hungary ● District VIII., Budapest - From your Internet address - Use precise location - Learn more


Help Send feedback Privacy Terms

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance

Bucharest, Romania 11/09/2019



🔍



🔍 All
🖼 Images
📺 Videos
📍 Maps
📰 News
⋮ More
⚙ Settings
🛠 Tools

About 23 results (0.30 seconds)

Index of /_vti_bin/_vti_adm - Rose Restaurant
www.rosrestaurant.com/_vti_bin/_vti_adm
 Index of /_vti_bin/_vti_adm. Name - Last modified - Size - Description - Parent Directory, -. Apache Server at www.rosrestaurant.com Port 80.





Index of /_vti_pvt - Rose Restaurant
www.rosrestaurant.com/_vti_pvt
 Index of /_vti_pvt. Name - Last modified - Size - Description ... writeto.cnf, 2012-11-05 10:38, 24. Apache Server at www.rosrestaurant.com Port 80.

Index of /_vti_log - Rose Restaurant
www.rosrestaurant.com/_vti_log
 Index of /_vti_log. Name - Last modified - Size - Description - Parent Directory, -. Apache Server at www.rosrestaurant.com Port 80.

Rose Restaurant
<https://www.rosrestaurant.com>
 And Find Out Why 11111. Everyone Knows 11111. The Rose!!!1111111. We accept credit cards. Contact US Legal Info [Site Map](#) (c) 2004 TGI Fridays Inc.
 Missing: index- | Must Include: [index-](#)

Index of /_vti_bin - Rose Restaurant
www.rosrestaurant.com/_vti_bin
 Index of /_vti_bin. Name - Last modified - Size - Description - Parent Directory ... _vti_aul/, 2012-11-05 10:37, -. Apache Server at www.rosrestaurant.com Port 80.

Images for site: "rosrestaurant.com" index-of


→ More images for site: "rosrestaurant.com" index-of Report images

Domain Whois Index - Da whois
<https://dawhois.com/domain/index-3064>
 Domain Whois Index ... roseretter.com roseretterjewelry.com roseremovals.co.uk roseresidents.com rosrestaurant.com roseretreat.com roserhapsody.com ...

Restaurants, pizzerias, barbecues, coffee shops locations in ...
<https://restaurants.maps-streetview.com/United-States/Baltimore/page=3>
www.rosrestaurant.com. Rocky Run Tap & Grill. 3105 Saint Paul St, ... Dr # H, Baltimore, MD 21244. 4109449000. Previous page - Page 3 - Next page.

Restaurants, New York, USA (R) - BizExposed.com
https://www.bizexposed.com/New_York-USA/Restaurants
 +1 212 977 7700. Website: www.rosamexicano.com; ... +1 212 759 3000. Website: www.fairmont.com/theplaza/index.htm; ... Website: www.rosrestaurant.com;...

2009 Annapolis Visitor Guide by Holly Maust - issuu
<https://issuu.com/barkleyrei/docs>
 Apr 22, 2009 - Site of Revolutionary and Civil War encampments. Annapolis, MD 21401 410-224-0907 www.geocities.com/aamblers/index.html 6075 Belle Grove Road Baltimore, MD 21225 410-636-0300 www.rosrestaurant.com.



1 2 [Next](#)

Hungary ● **District VIII., Budapest** - From your Internet address - Use precise location - [Learn more](#)

[Help](#)
[Send feedback](#)
[Privacy](#)
[Terms](#)

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance

Bucharest, Romania

11/09/2019

3., Using the proper string will give access to `_vti_pvt`

Google

[All](#) [Images](#) [Videos](#) [Maps](#) [News](#) [More](#) [Settings](#) [Tools](#)

About 31 results (0.27 seconds)

[Index of /_vti_pvt - Rose Restaurant](#)
www.rosrestaurant.com/_vti_pvt
 Index of /_vti_pvt. Name - Last modified - Size - Description ... writeto.cnf, 2012-11-05 10:38, 24. Apache Server at www.rosrestaurant.com Port 80.


[Index of /_vti_bin/_vti_adm - Rose Restaurant](#)
www.rosrestaurant.com/_vti_bin/_vti_adm
 Index of /_vti_bin/_vti_adm. Name - Last modified - Size - Description - Parent Directory, -. Apache Server at www.rosrestaurant.com Port 80.

[Index of /_vti_log - Rose Restaurant](#)
www.rosrestaurant.com/_vti_log
 Index of /_vti_log. Name - Last modified - Size - Description - Parent Directory, -. Apache Server at www.rosrestaurant.com Port 80.

[Rose Restaurant](#)
<https://www.rosrestaurant.com>
 And Find Out Why 11111. Everyone Knows 11111. The Rose!!!1111111. We accept credit cards. Contact Us Legal Info Site Map (c) 2004 TGI Fridays Inc. Missing: index | Must include: [index](#).

[Index of /_vti_bin - Rose Restaurant](#)
www.rosrestaurant.com/_vti_bin
 Index of /_vti_bin. Name - Last modified - Size - Description - Parent Directory ... _vti_aut/, 2012-11-05 10:37, -. Apache Server at www.rosrestaurant.com Port 80.

Images for site: "rosrestaurant.com" index of



[More images for site: \"rosrestaurant.com\" index of](#) [Report images](#)

[Domain Whois Index - Da whois](#)
<https://dawhois.com/domain/index-3064>
 Domain Whois Index ... roseretter.com roseretterjewelry.com roseremovals.co.uk roseresidents.com **rosrestaurant.com** roseretreat.com roserhapsody.com ...

[Restaurants, pizzerias, barbecues, coffee shops locations in ...](#)
<https://restaurants.maps-streetview.com/United-States/Baltimore/page=3>
www.rosrestaurant.com. Rocky Run Tap & Grill. 3105 Saint Paul St, ... Dr # H, Baltimore, MD 21244. 4109449000. Previous page - Page 3 - Next page.

[Restaurants, New York, USA \(R\) - BizExposed.com](#)
https://www.bizexposed.com/New_York-USA/Restaurants
 +1 212 977 7700. Website: www.rosamexicano.com; ... +1 212 759 3000. Website: www.fairmont.com/theplaza/index.html; ... Website: www.rosrestaurant.com;..

[rose ma - gag-daily.com](#)
<https://www.gag-daily.com/search>
 ... grille room A wide variety of menu selections ... www.rosrestaurant.com ... Enter Site www.lavieenroseband.com ... Poème sur la rose - [index](#) de la poesie de marieToi ma rose, jolie de tes atours, De ta fragrance ma dulcinée tu entoures.

Google

1 2 Next

Hungary **District VIII., Budapest** - From your Internet address - Use precise location - Learn more

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance
Bucharest, Romania **11/09/2019**

4., Browse /_vti_pvt folder

Index of /_vti_pvt

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
access.cnf	2012-11-05 10:38	146	
botinfs.cnf	2012-11-05 10:38	24	
bots.cnf	2012-11-05 10:38	24	
deptodoc.btr	2012-11-05 10:38	324	
doctodep.btr	2012-11-05 10:38	16K	
frontpg.lck	2012-11-05 10:38	0	
linkinfo.btr	2012-11-05 10:38	29K	
service.cnf	2012-11-05 10:38	1.1K	
service.grp	2012-11-05 10:38	48	
service.lck	2012-11-05 10:38	0	
service.pwd	2012-11-05 10:38	36	
services.cnf	2012-11-05 10:38	2	
svcacl.cnf	2012-11-05 10:38	2	
writeto.cnf	2012-11-05 10:38	24	

Apache Server at www.rosrestaurant.com Port 80

European Cyber Security Challenge 2019 Understanding cyber kill chain's first step: Information reconnaissance
Bucharest, Romania **11/09/2019**

5., Locate the service.pwd

```
# -FrontPage-  
therose:WK7JNgYcDkzac
```