**va03.z3.lv**

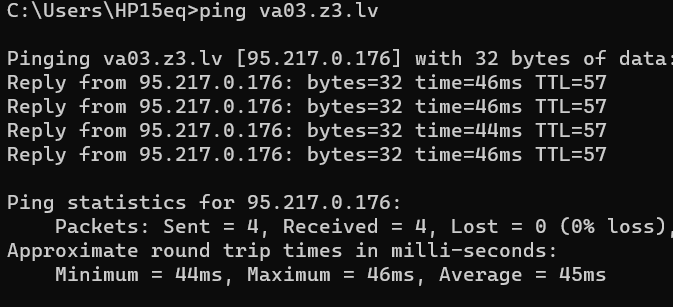
Internet based penetration test

Produced by:

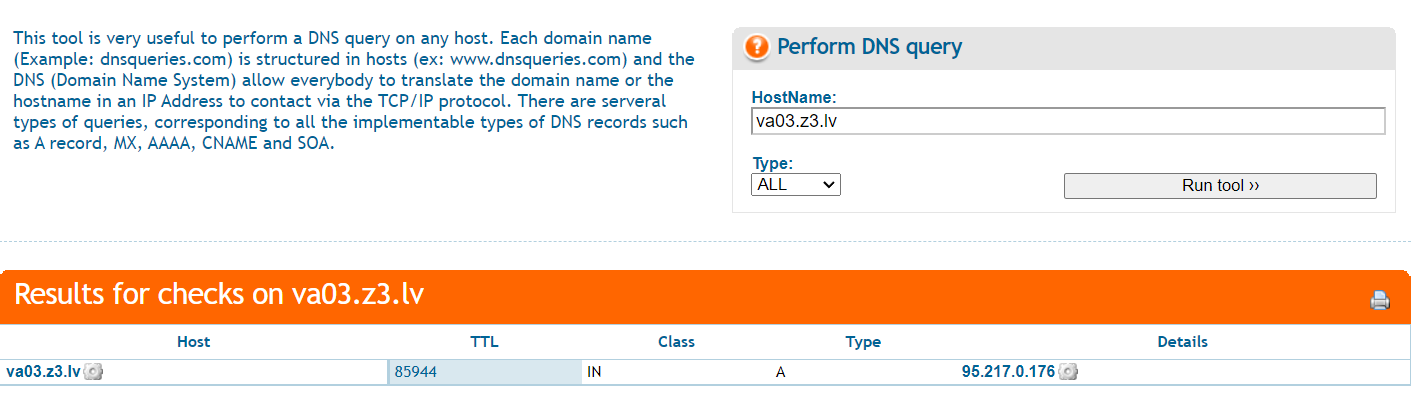
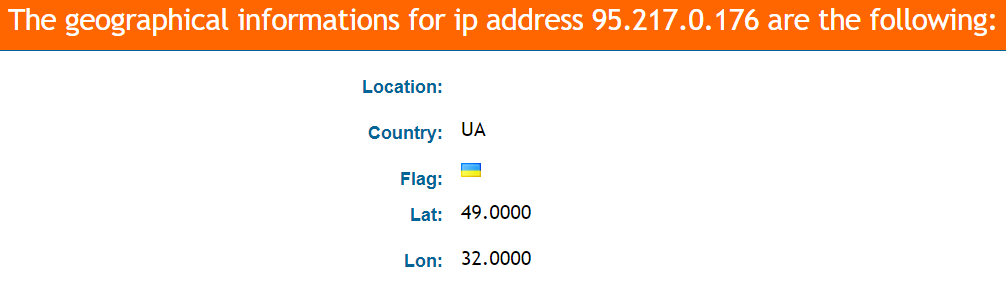
Denys Shabelnyk  
ViA-KI-2022

18.05.2023

# Management summary and description of tested system

The target is a remote host which has DNS name va03.z3.lv. The host is available through the Internet. The host is accept ICMP requests and has **TTL = 57**  


This value of TTL means that the target host **is not Windows machine**.

Next step, trying to get information from DNS name. If we use only free available tools from Internet we can get some useful information about **IP address** and where the target host **geographically located**. Let’s look at result from www.dnsqueries.com  
  
  
The IP address is 95.217.0.176. This information can help us to know about internet service provider, about size of company, etc. Small companies use not wide range of Ips, but big companies do.   
  
If we look at GeoLocation we can know that the target post is located on Ukraine.

# 

The objective of current test was vulnerability assessment of the given host name va03.z3.lv. Testing was conducted during the time period from 18/05/2023 to 05/06/2023.

As I explored before, the target machine is not Windows machine. It has IP 95.217.0.176 and located in Ukraine

Interesting information gets **whois** about target IP  
  
**inetnum: 95.216.0.0 - 95.217.255.255**

**netname: DE-HETZNER-20090224**

**country: FI**

**org: ORG-HOA1-RIPE**

admin-c: HOAC1-RIPE

tech-c: HOAC1-RIPE

status: ALLOCATED PA

notify: ripe-mntner@hetzner.de

mnt-by: RIPE-NCC-HM-MNT

mnt-by: HOS-GUN

mnt-lower: HOS-GUN

mnt-domains: HOS-GUN

mnt-routes: HOS-GUN

created: 2009-02-24T07:39:38Z

last-modified: 2017-11-02T11:54:31Z

source: RIPE

abuse-email: abuse@hetzner.com

abuse-c: HOAC1-RIPE

abuse-org: ORG-HOA1-RIPE

organisation: ORG-HOA1-RIPE

org-name: Hetzner Online GmbH

country: DE

org-type: LIR

address: Industriestrasse 25

address: D-91710

address: Gunzenhausen

address: GERMANY

phone: +49 9831 5050

fax-no: +49 9831 5053

e-mail: info@hetzner.de

admin-c: MF1400-RIPE

admin-c: GM834-RIPE

admin-c: HOAC1-RIPE

admin-c: MH375-RIPE

admin-c: SK2374-RIPE

admin-c: SK8441-RIPE

abuse-c: HOAC1-RIPE

mnt-ref: RIPE-NCC-HM-MNT

mnt-ref: HOS-GUN

mnt-by: RIPE-NCC-HM-MNT

mnt-by: HOS-GUN

created: 2004-04-17T11:07:58Z

last-modified: 2022-11-22T18:32:44Z

source: RIPE

role: Hetzner Online GmbH - Contact Role

address: Hetzner Online GmbH

address: Industriestrasse 25

address: D-91710 Gunzenhausen

address: Germany

phone: +49 9831 505-0

fax-no: +49 9831 505-3

e-mail: ripe@hetzner.com

abuse-mailbox: abuse@hetzner.com

remarks: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

remarks: \* For spam/abuse/security issues please contact \*

remarks: \* abuse@hetzner.com, or fill out the form at \*

remarks: \* abuse.hetzner.com, thank you. \*

remarks: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

remarks:

remarks: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

remarks: \* Any questions on Peering please send to \*

remarks: \* peering@hetzner.com \*

remarks: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

org: ORG-HOA1-RIPE

admin-c: MH375-RIPE

tech-c: GM834-RIPE

tech-c: SK2374-RIPE

tech-c: MF1400-RIPE

tech-c: SK8441-RIPE

tech-c: DD15478-RIPE

nic-hdl: HOAC1-RIPE

notify: ripe-mntner@hetzner.com

mnt-by: HOS-GUN

created: 2004-08-12T09:40:20Z

last-modified: 2022-11-22T18:33:55Z

source: RIPE

route: 95.216.0.0/16

org: ORG-HOA1-RIPE

descr: HETZNER-DC

origin: AS24940

mnt-by: HOS-GUN

created: 2017-08-12T12:01:36Z

last-modified: 2018-01-10T08:47:33Z

source: RIPE

organisation: ORG-HOA1-RIPE

org-name: Hetzner Online GmbH

country: DE

org-type: LIR

address: Industriestrasse 25

address: D-91710

address: Gunzenhausen

address: GERMANY

phone: +49 9831 5050

fax-no: +49 9831 5053

e-mail: info@hetzner.de

admin-c: MF1400-RIPE

admin-c: GM834-RIPE

admin-c: HOAC1-RIPE

admin-c: MH375-RIPE

admin-c: SK2374-RIPE

admin-c: SK8441-RIPE

abuse-c: HOAC1-RIPE

mnt-ref: RIPE-NCC-HM-MNT

mnt-ref: HOS-GUN

mnt-by: RIPE-NCC-HM-MNT

mnt-by: HOS-GUN

created: 2004-04-17T11:07:58Z

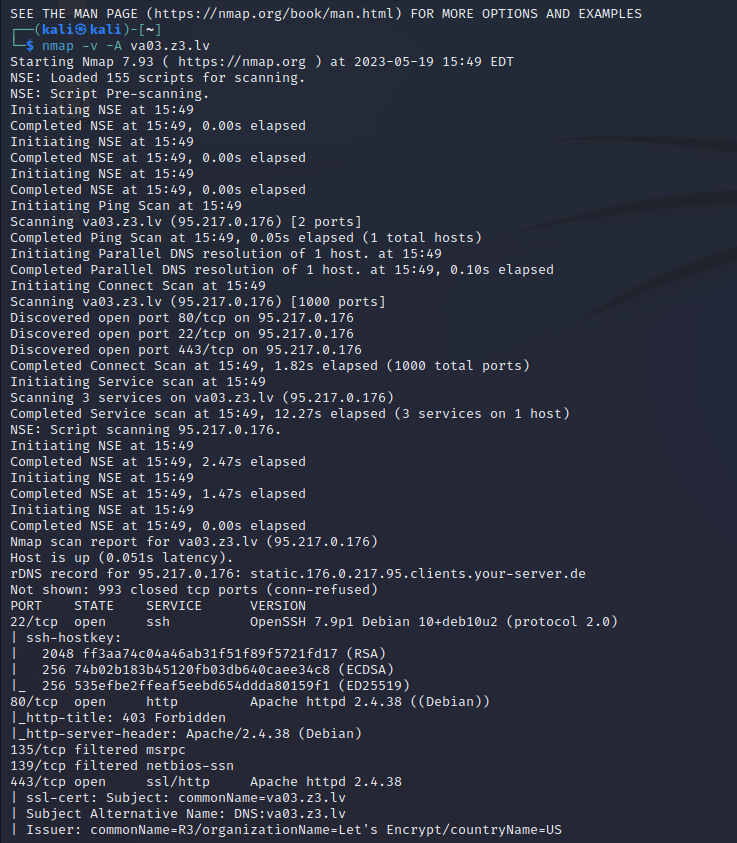
last-modified: 2022-11-22T18:32:44Z

source: RIPE

Whois gets information about domain name owner, its juridical address.  
Also, whois shows us information about IP range in section **inetnum.**   
This information is taken us ability to perform port scanning on particular range.

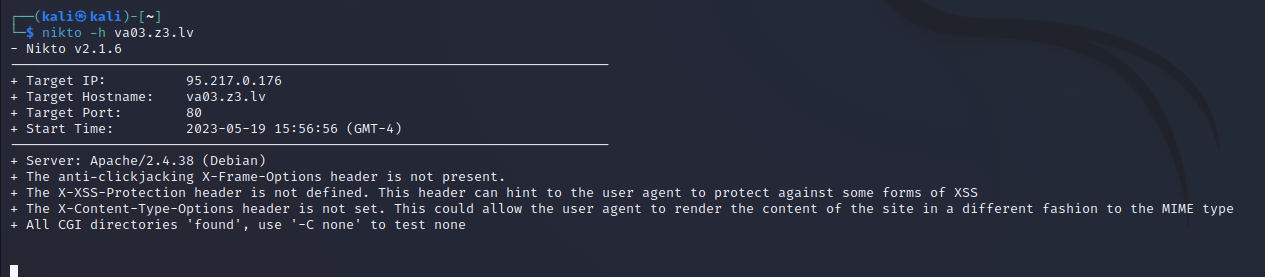
There are no result on public databases like **Bing.com** and **Shodan.io** with filters **:ip** and **:net**

About port scanning using **nmap.**  A lot of interesting information below:



We cam see that ports 80, 22 and 443 are open ports

# Interesting information I have got through **Nikto**

All vulnerabilities are available on the screen.