

ZABBIX



## Introduction

We are passionate ICT Consultants who also are trainers for Zabbix. We have multiple years of experience in Zabbix and providing trainings and always like to share knowledge on the subject.

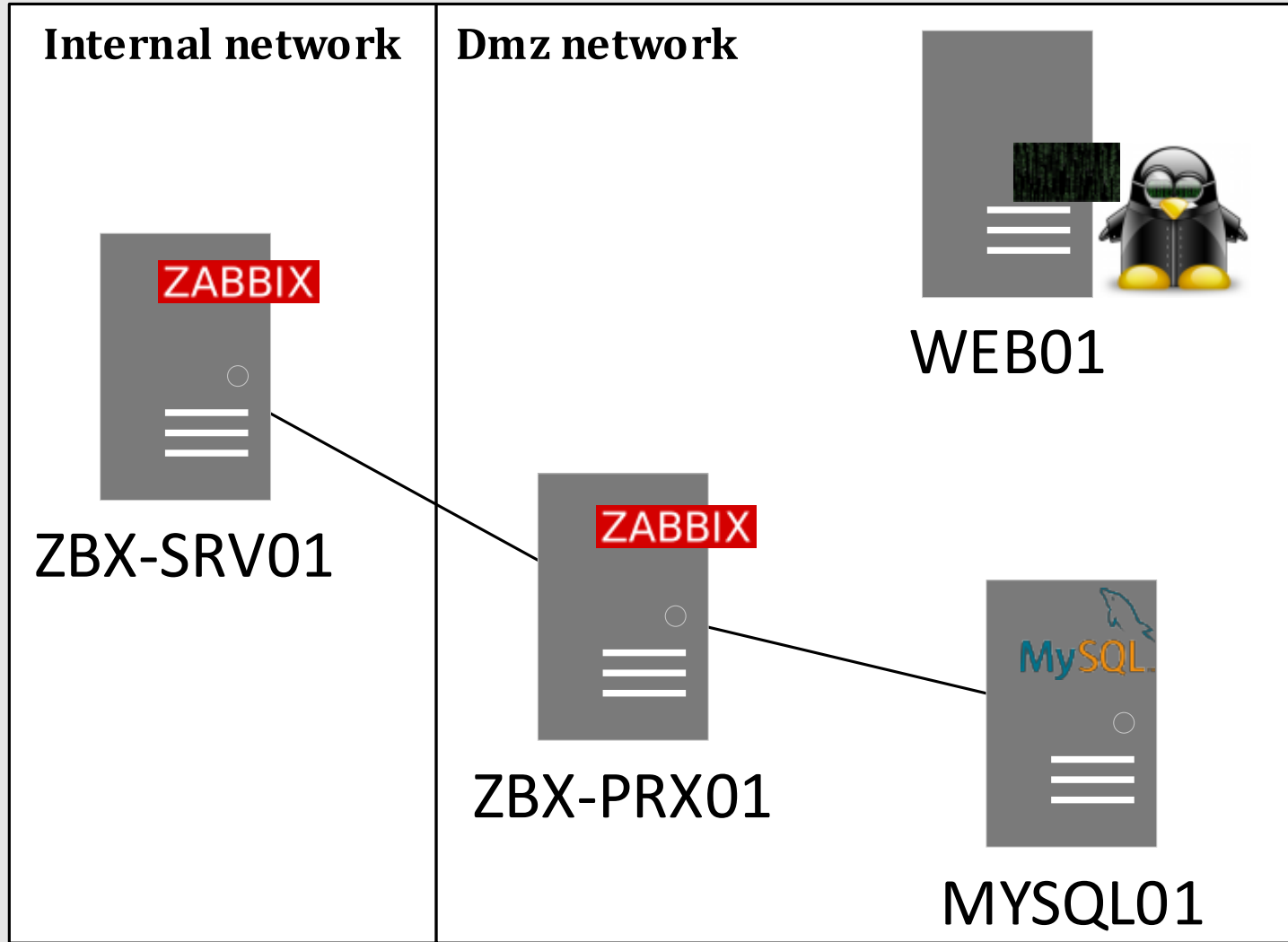
- Robert Hoekstra  
ICT Consultant – Zabbix trainer
- Michael Schouwstra  
ICT Consultant – Zabbix trainer

## Introduction to problem

- Scenario description
  - Zabbix active proxy without IP address/range restriction
  - Zabbix active proxy without encryption.
- Introduction to setup ZBX-SRV01, ZBX-PRX01, MYSQL01, WEB01
  - We created a mysql user with a secret pass..

# ZABBIX



## The setup



Everybody should be using secret macros by now!

Host IPMI Tags **Macros 1** Inventory ● Encryption Value mapping

Host macros Inherited and host macros

Macro	Value	Description
<input data-bbox="461 721 958 768" type="text" value="{\\$SECRETPASSWORD}"/>	<input data-bbox="970 721 1447 768" type="text" value="....."/>  	<input data-bbox="1582 721 2173 768" type="text" value="description"/> <a href="#">Remove</a>

Name ▲	Mode	Encryption	Compression
zabbixproxy	Active	<span>None</span>	<span>On</span>

# ZABBIX

So now we have our passwords secured, right?



# ZABBIX

Let's see what Harry the hacker thinks

*Hello, I am Harry!*  
*"All your Secrets are belong to me"*



## Demo one

- Show zabbix frontend
- Show the database that is monitored
- Show secret that is set
- Switch to console on the web01 host
- Zabbix get command to get proxy configuration
- Show JSON result on screen



## Recap of what happened

We impersonated a zabbix-proxy to get the configuration from the zabbix server. Zabbix server was not able to verify the authenticity of the proxy and just responded to the request.

We were able to see the secret macro that nobody should be able to see.

With this information we can potentially get information out of other systems that we should not be able to get.

## Demo two

- Configure IP address of the active proxy in the front end of Zabbix
- Show that the WEB01 is not able to fetch the configuration anymore
- Show that any user on the proxy host ZBX-PRX01 can still retrieve all configuration in plain text

# ZABBIX

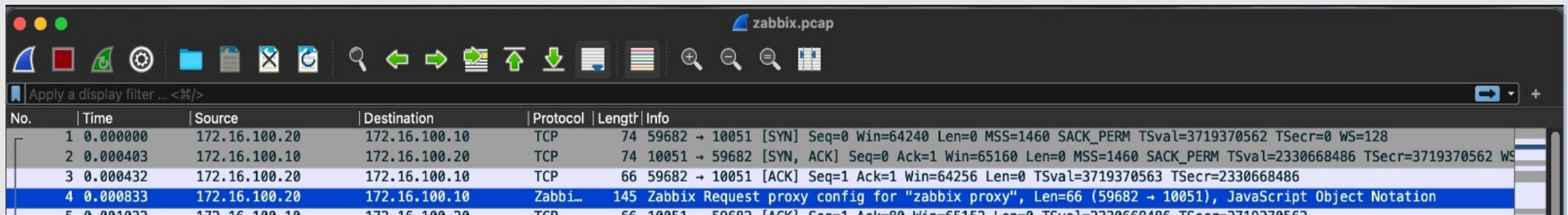
**A lot better, but is it enough though?**

*I Really don't think so!  
"All your Secrets are belong to us"*



# ZABBIX

But what if somebody does a network capture?



The image shows a Wireshark network capture window titled 'zabbix.pcap'. The main pane displays a list of network packets. Packet 4 is highlighted in blue and contains a Zabbix request for proxy configuration. The packet details pane on the right shows the 'Data' field containing a JavaScript Object Notation (JSON) string.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.100.20	172.16.100.10	TCP	74	59682 → 10051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3719370562 TSecr=0 WS=128
2	0.000403	172.16.100.10	172.16.100.20	TCP	74	10051 → 59682 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2330668486 TSecr=3719370562 WS=128
3	0.000432	172.16.100.20	172.16.100.10	TCP	66	59682 → 10051 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3719370563 TSecr=2330668486
4	0.000833	172.16.100.20	172.16.100.10	Zabbix	145	Zabbix Request proxy config for "zabbix proxy", Len=66 (59682 → 10051), JavaScript Object Notation
5	0.001033	172.16.100.10	172.16.100.20	TCP	66	10051 → 59682 [ACK] Seq=1 Ack=0 Win=65160 Len=0 TSval=2330668486 TSecr=3719370563

Plain text ?

Data [truncated]: {"globalmacro":{"fields":["globalmacroid","macro","value","type"],"data":[[2,{"\$

## Demo three

- Create and show command on how to create a PSK key
- Show where to set this in the configuration files of the proxy
- Set proper rights on the PSK key file
- Restart the proxy
- Configure the PSK setting in the front-end
- Zabbix-get command from proxy to show that the data is not available
- Show that if the setting is set on both, you still get all the data



## Recommendations:

### Always use Encryption!

- Limit your Zabbix proxies by using IP
- Configure AT LEAST PSK
- Best: EACH device with a unique PSK ID and key

15 0.018013 10.211.55.7 10.211.55.100 TLSv1... 1799 Application Data

```

84 0a 94 2b cf 28 ce 24 5a cf 97 e1 2c 22 21 f4 .....($ Z...,"!
e9 a0 ec 76 2a 48 66 e0 a4 c6 35 b0 de 50 c8 89 ...v*HF...5.P..
e1 ee bf 52 a6 fb 5a 03 c4 99 30 24 14 ad 46 97 ...R.Z...0$.F.
24 71 aa 38 96 db 79 2f ee ce c6 1d f2 30 c8 0b $q.8.y/.....0..
c5 12 c4 06 3d e9 33 f8 d8 5d 04 4c 5c bf a5 a0 .....=3..]L\..
94 69 58 43 b3 b6 6c f9 f2 07 27 ee 81 2f 2e 24 .iXC.L..."/.$
fa fd 6b 88 90 d6 33 d9 06 d6 f8 ff a4 e9 97 45 ..k..3.....E
de 3d d8 49 4c 8c ac 6b 16 74 b3 28 a9 2c b8 de ..=IL.k.t.(,..
99 fc 8c 80 bb a4 04 27 14 c5 99 60 71 12 2e b2 ..... '...q...
0c 74 53 99 a8 90 8e f9 0b 1e e9 e6 05 2d 13 f9 .tS.....-...
19 19 9a 11 47 74 06 9c 7c a5 41 55 fe 2a 77 69 ...Gt...|AU.*wi
2b 0c cb 70 d6 68 69 4e 3b 7c 1c 41 08 df 53 e4 +..p.hIN;|A.S.
cb 22 2a 70 47 1c 31 c3 86 02 91 47 ad f4 1c a9 ..*pG.1...G...
09 fb ac 51 6e 51 bd 30 ff 0d 99 95 f4 27 10 c2 ...Qn0.0.....
4c ca 47 79 86 35 d2 8d 1c 1a e4 0c 54 88 7e 05 L.Gy.5...T~.
59 42 39 be 65 28 1a de c0 7f 97 41 ce cb 9a 74 YB9.e(...A..t
d1 dc 54 a5 f6 bf 60 15 ab d6 90 c7 70 13 c4 3c ..T... ..p-<
03 71 1d 27 97 2c 0d 32 bb 13 6d 56 04 ba f3 75 ..q'..,2..mV...u
74 03 96 12 28 75 f5 4d 4c f2 bf 9b 9d c3 a0 bb t... (u.M L.....
98 ee a6 18 65 8f 3f 8d 68 1f 36 e2 38 50 e4 6e ...e.?..h.6.8P.n
d0 7e 28 3f 23 a8 22 b4 87 50 08 dd 9f 48 b4 b5 ~{?#. " .P..H..
02 c7 ec c3 72 8a 09 0b 1e 26 34 8c cd 6b aa 30 ..r...64.k.0
ef 6e 82 a0 03 62 22 22 f4 91 16 da b2 bd d6 50 .n..b"".....P
b8 59 7e ac c2 c4 4b 4d 09 d6 79 4c c0 c5 53 d8 .Y~..KM...yL..S.
77 18 34 50 cf bb 20 55 ad cc a3 1e 8d eb 12 a0 w.4P.. U .....
40 3d fb b2 73 30 9c b5 2d 5d b1 01 2c e7 25 06 @=-s0...-]...%.
```

```

v Transport Layer Security
v TLSv1.3 Record Layer: Application Data Protocol: Zabbix Protocol
  Opaque Type: Application Data (23)
  Version: TLS 1.2 (0x0303)
  Length: 1728
  Encrypted Application Data: e878df298cf0aa6087c36a1b28233187d8c253e3397cafd89c78aa193758923b29...
  [Application Data Protocol: Zabbix Protocol]
```



**ZABBIX**

**Questions?**

