SYNACKTIV

Gotta Log 'Em All!

Bière Sécu Rennes

2026/01/27

Whoami

SYNACKTIV

- Worty
- Pentester / Researcher @ Synacktiv
- ~200 employees
- Offices at Paris, Rennes, Bordeaux, ...
- We're hiring (developer, pentester, reverser, ...) !

Blue team tools used in Red Team

SYNACKTIV

- Blue team tools are more whitelisted than red team ones
  - LOLBlue : Living Off the Land with Blue Team tools - hack.lu 2025 - Synacktiv
- Accessed by employees with privileged access
- Contains sensitive information (logs, alerts, ...)

Our target : Graylog

SYNACKTIV

- Centralizes logs
- Makes logs searchable
- Alerting & Security Monitoring
- Based on OpenSearch and MongoDB

What's inside MongoDB ?

SYNACKTIV

- Users
- Sessions
- API Tokens
- Cluster configurations
- ...

MongoDB - In depth security measures

SYNACKTIV

- Hashed passwords, sessions tokens, ... are stored in MongoDB
- However, they're signed with a secret stored on the FS
- Even with an access to MongoDB => impossible to create or modify passwords, etc


AU MOINS PERSONNE GUESSERA MES CREDS
AHA ILS SONT RANDOM ?
COMMENT CA Y'EN A PAS PAR DÉFAUT ?
imgflip.com

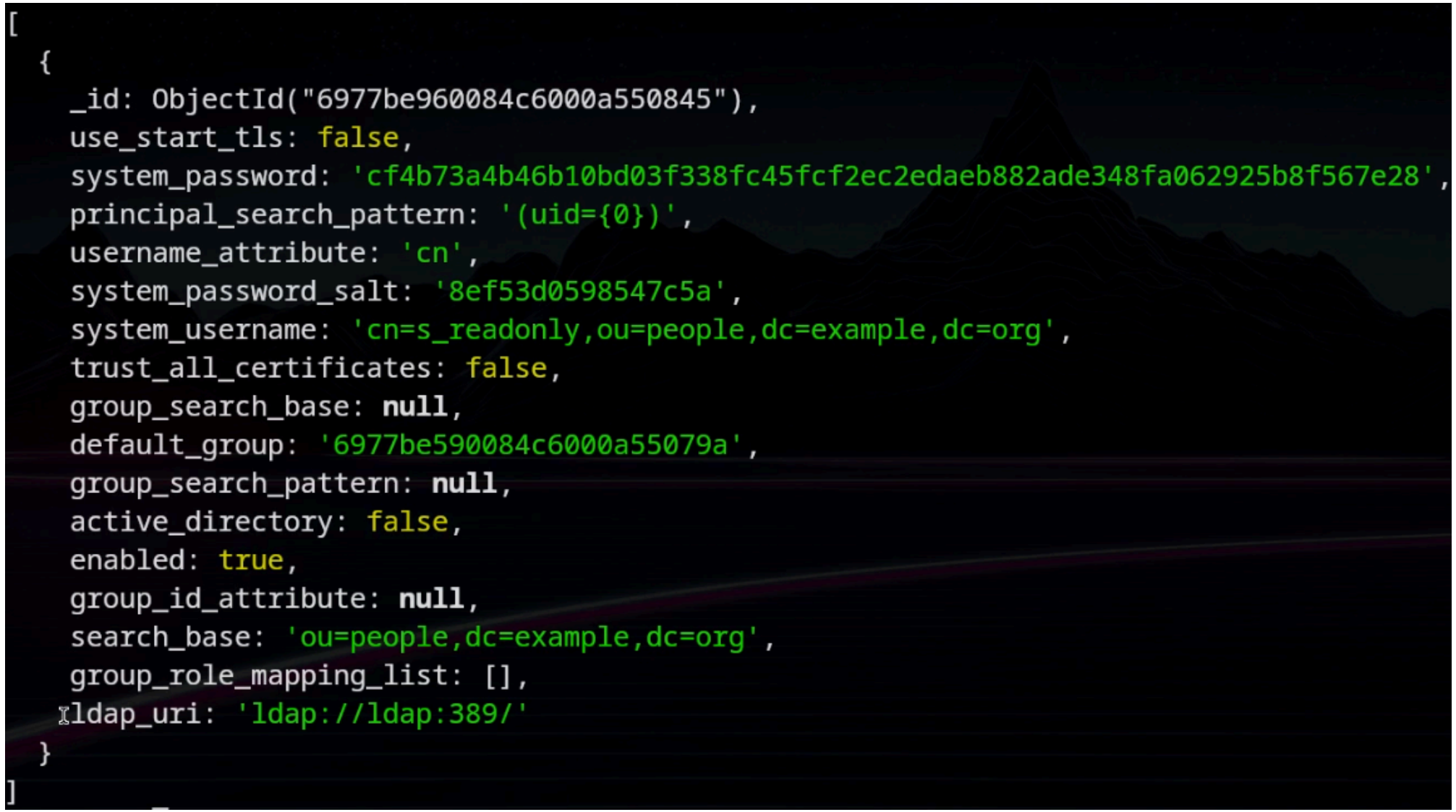
Scenario

SYNACKTIV

- Exposed Graylog stack (including MongoDB)
- LDAP authentication is enabled on Graylog
- Version is 2.X or 3.X (does not work for 4.X and 5.X)
- No hardening on the MongoDB configuration

What's REALLY inside MongoDB ?

SYNACKTIV




LDAP_URI NOT SIGNED
imgflip.com

Attack plan

SYNACKTIV

- Open MongoDB instance storing graylog's information
- Inside the `ldap_config` table:
  - Modify the `ldap_uri` to attacker controlled one
  - Modify the `trust_all_certificates` to `true`
  - (optional) Modify the `use_start_tls` to `false`
- Create a Rogue LDAP server to intercept and log all LDAP queries

Attack plan

SYNACKTIV

```
/home/worty> curl http://internal-app.local/search -X POST --data "username='"
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual tha
utils.php:27
Stack trace:
#0 /var/www/html/db_utils.php(27): mysqli->query('SELECT * FROM use...')
#1 {main}
  thrown in /var/www/html/db_utils.php on line 27
```

Attack plan

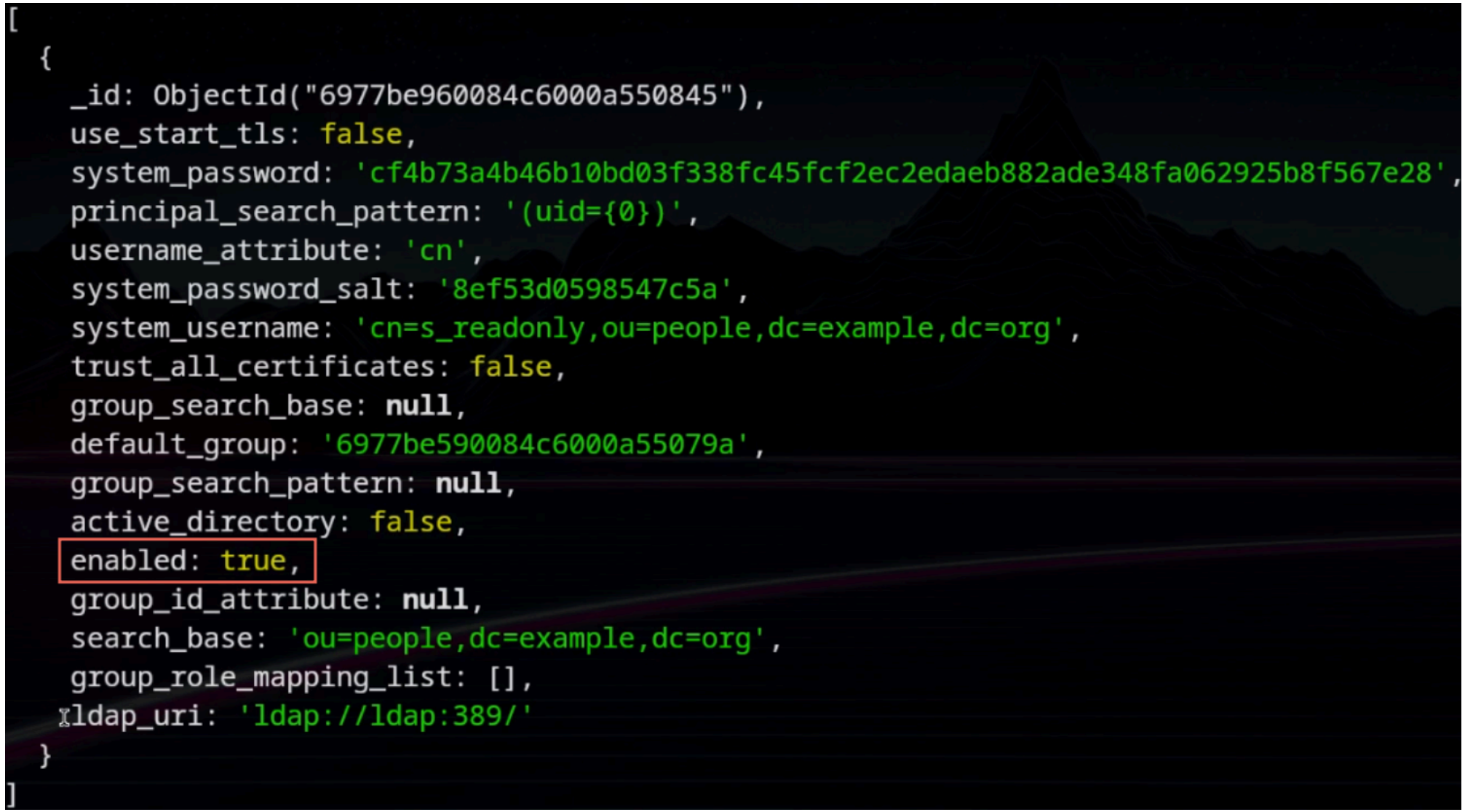
SYNACKTIV

```
while true;
do curl http://internal-app.local/search -X POST --data "username='";
done
```

Demonstration

Going further...

SYNACKTIV



Going further...

SYNACKTIV

```
@SuppressForbidden("Deliberate use of ObjectInputStream")
public Map<Object, Object> getAttributes() {
    final Object attributes = fields.get("attributes");
    if (attributes == null) {
        return null;
    }
    final ByteArrayInputStream bis = new ByteArrayInputStream((byte[]) attributes);
    try {
        // FIXME: This could break backward compatibility if different Java versions are being used.
        final ObjectInputStream ois = new ObjectInputStream(bis);
        final Object o = ois.readObject();
        return (Map<Object, Object>) o;
```

Going further...

SYNACKTIV

- LDAP attributes in MongoDB : **Serialized Java Objects**
- If JVM < 18, CommonsCollections3 are available in Graylog (so free RCE)
- If JVM > 18:
  - Gadgets must be found in graylog's source code
  - You must adapt CommonsCollections3 to work on JVM > 18

SYNACKTIV

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

https://twitter.com/synacktiv

https://synacktiv.com