Hacking the SAP system

Is it really that easy?

Marcel Rabe
SAP Architect
Agenda

- The why
- The what
- The which
- The how
- The demo
Why

- Single Sign On Cookies vulnerability
- Significant increase in number of users
- Semi-public corporate network
- SAP (finally) goes Web and mobile
Why
Nothing new

Personal Data of 50 Million Turkish Citizens Leaked Online

LinkedIn users targeted in email scam after hack

Washington confirms Chinese hack attack on White House computer

Hacker Apocalypse Strikes World of Warcraft

Bitcoin exchange market hacked for US$250,000 loss

Muslim Cyberfightlers Claim Responsibility for Bank of America and NYSE Hack in Retaliation for Movie

Diginotar failliet na hack

24 November

Sources within Sony report that they have been hacked and blackmailed by a group leaving the message:

Hacked by #GOP. Warning: We've already warned you, and this is just the beginning. We have obtained all your internal data including secrets and top secrets.
But now it’s getting closer to home....

Report: Chinese Breach of USIS Started with SAP

Tara Seals US/North America News Reporter, Infosecurity Magazine

Last fall, it came to light that Chinese hackers had roamed around unnoticed for months inside the network of USIS, the biggest commercial provider of background investigations to the federal US government. In fact, two of the company’s biggest customers are the Department of Homeland Security (DHS) and the Office of Personnel Management (OPM).

Onapsis Research Labs analysis finds that the breach most likely utilized an SAP attack vector that Onapsis has been tracking in the wild and warning enterprises about. It marks the first time an SAP attack against a national security service provider has been publicly uncovered.

“SAP systems have always been a target for hackers as they run the most critical and sensitive processes for the largest companies and government agencies in the world,” said Onapsis researcher Sergio Abraham, in a blog. “Examples such as the USIS breach are showing the importance of protecting our SAP Systems and eradicating the false idea of business critical...
GREEK FINANCE MINISTRY HACK BY ANONYMOUS

Greek finance ministry hack by Anonymous

Hackers Group "Anonymous" with Operation #OpGreece strikes again on Greek Ministry of Finance and claims to leak confidential document including Login and passwords. According to anonymous via the document pasted on Anonpaste - The purpose of the hack was to protest against the worse economic condition in Greece.

They even said "We gained full access to the Greek Ministry of Finance,"

Anonymous posted a compressed file with documents, plus passwords and logins, that the group claimed were valid. Anonymous said it had accessed IBM servers, and that it possessed an SAP zero-day exploit.

"There is an ongoing inquiry," a Ministry of Finance spokeswoman told SC Magazine UK on Tuesday. "We are searching to see if this hack happened." said The Greek Ministry of Finance.
95% of SAP deployments 'vulnerable to cyber attacks'

Severe SAP HANA vulnerabilities allow hackers to take full control
Security flaws within the SAP HANA platform include remote exploits leading to full takeovers of systems.

SAP Encryption Issues Pose Serious Risk to Organizations: Researchers

Security

Some old SAP systems have default kernel user accounts. Guess what happened next?
Infosec bloke pokes hornet’s nest with stick; patch ASAP
How

- SAP vulnerability assessment
  - Scope: all SAP systems, all corporate networks
  - White-box approach
  - Collect data manually / with tooling onsite
  - Build report offsite
  - Share high priority findings early
  - Present general findings
- Extensive 73 page report with findings and steps to mitigate
- Insight in how exploiting different weaknesses combined result in full access
Which

- PRD
- QAS / ACC
- DEV
Start at the weakest link.....
Show

- **SAP Gateway**
  - Use the SAP RFC gateway from UvA guest/student/eduraom networks to create a SAP user with SAP_ALL

- **Default users**
  - Use a ‘forgotten’ default user sap* in a sandbox system to login and gain all password hashes for all clients using DB02

- **Passwords bruteforcing**
  - BCODE
  - OCLhashcat
Taking advantage of the RFC Gateway

What is the RFC gateway? – Quick introduction – Part 3

Scenarios of RFC communication

1. Call to ABAP function modules
2. RFC call to start operating system commands, e.g. tp, sapxpg
3. RFC calls to register and use external RFC servers
- Access to gateway port range 3300-3399
- Default without authentication check (changed as of 7.3 new installations)
- Security through parameters `gw/sec_info` and `gw/reg_info`, but also `gw/sim_mode`

**Attack scenario**
Connect to the RFC gateway and execute operating system commands (e.g. `create SAP_ALL user with SQL client`)

Diagram showing the flow from SAP NetWeaver Application Server ABAP to a database via an RFC gateway, SAP RFC SDK, and SAP JCo, with directions indicating `Start operating system commands`. The diagram also shows a lock symbol, indicating security or access control mechanisms.
Walkthrough 1/2

1. Try to find a SAP server with an unprotected gateway
2. Try to create launch an Operating System command remotely
3. Try to create a user with all authorizations
4. Login with that user
Tooling requires default passwords....

**DSM Client Sync**

flexible copying of subsets of SAP Clients

---

**Protecting Standard Users**

**SAP**, **DDIC**, **EARLYWATCH**

SAP Systems create the standard users **SAP**, **DDIC** and **EARLYWATCH** during the installation process in the clients as shown in the table below.

<table>
<thead>
<tr>
<th>User</th>
<th>Description</th>
<th>Clients</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP</td>
<td>SAP system super user</td>
<td>000, 002, 066</td>
<td>66021052</td>
</tr>
<tr>
<td>DDIC</td>
<td>ABAP Dictionary and software logistics super user</td>
<td>000, 001</td>
<td>19920706</td>
</tr>
<tr>
<td>EARLYWATCH</td>
<td>Dialog user for the Early Watch service in client 066</td>
<td>066</td>
<td>support</td>
</tr>
</tbody>
</table>
Walkthrough 2/2

1. Try to logon with SAP* in any client
2. Capture the table with all passwords
3. Dehash the passwords
4. Login with a compromised user