Rekall Agent - OSDFCon 2017

We will remember it for you wholesale!

Michael Cohen
mic@rekall-innovations.com

*Rekall is an open source project released under the GPL. It is not an official Google product, and does not necessarily reflect the views of Google.*
Overview

● Why the Rekall Agent?
● Deployment: Rekall in the cloud!
● Authentication
● Flows
● Hunts
● Exporting data
● Post processing
Why endpoint monitoring?

- An enterprise typically has a lot of endpoints (laptops, servers, cloud VMs).
  - Mix of operating systems, configurations and deployments.
  - Systems are not always accessible.
  - Dynamic changing environment.
Existing solutions

- Resource management.
  - System is idle much of the time.
  - But when something happens (e.g. a hunt) QPS load increases.
- Existing systems need to be provisioned in advance to handle maximal load.
Existing solutions

- Flexibility is important
  - Some existing solutions require code changes to be deployed server side or client side.
    - E.g. GRR requires python hacks to run arbitrary code.
  - In a dynamic, rapidly evolving incident we need to be able to get and filter data in creative ways.
    - Sometimes the framework does not provide flexible filtering requiring a lot of extra data to be transferred and the post-processed.
Rekall Everywhere: Collect and preserve forensic evidence at scale, quickly, efficiently and flexibly.
Use the Cloud!

Cloud technologies provide automated scaling. When things get busy, the cloud takes care of scaling up. When things are idle, the cloud scales down to save on cost.
Why Rekall Agent?

- **Endpoint monitoring solution**
  - Rekall is already a sophisticated forensic analysis framework
  - Rekall Agent runs remote analysis at scale.
  - Collection system for results and files.

- **Strong Access controls and auditing.**
  - Role based access control mechanism
  - Peer approval process for gaining access to individual machine's data.
  - Strong auditing managed by the Google Cloud Platform.

- **Easily scalable**
  - The Google Cloud Platform (GCP) manages scaling on demand.
Deploying Rekall Agent

Create GCP project, push AppEngine app.

Step 1

Step 2
Configure App Engine app to allow users access.

Step 3
Create a client config for each OS and deploy client via software management tools.
Deployment - Server.

- Create a new project in the GCP console.
  - Give the project a unique name - the project will be served from https://project-name.appspot.com
  - Rekall Agent relies on SSL for communication security - GCP provides an SSL connection automatically.
- Get a working shell or spin up a virtual machine.
- Checkout the repository using git.
- Run the bootstrap script.
- Deploy the app
- Profit
Create a new project.

Project name

dfrws2017-rekall

Your project ID will be dfrws2017-rekall

Create  Cancel
<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dfrws2017-rekall</td>
<td>dfrws2017-rekall</td>
</tr>
<tr>
<td>Scudette</td>
<td>fourth-carport-147912</td>
</tr>
<tr>
<td>Rekall Test Site</td>
<td>rekall-test-site</td>
</tr>
<tr>
<td>dirr</td>
<td>dirr-158405</td>
</tr>
<tr>
<td>Rekall</td>
<td>crypto-prism-89412</td>
</tr>
</tbody>
</table>
Cloning the Rekall repository for server deployment

Welcome to App Engine

A powerful platform to build web and mobile apps that scale automatically - learn more

Your first app

Learn how to build and deploy on App Engine with a sample "Hello World" app. If you're new to App Engine, then start here.

Select a language

Welcome to Cloud Shell. Type "help" to get started.

(Dev) scudette:~$ git clone https://github.com/rekall-innovations/rekall-agent-server
Cloning into 'rekall-agent-server'...
remote: Counting objects: 1352, done.
remote: Compressing objects: 100% (51/51), done.
remote: Total 1352 (delta 24), reused 48 (delta 22), pack-reused 1277
Receiving objects: 100% (1352/1352), 6.90 MiB | 8 bytes/s, done.
(Dev) scudette:~$ cd rekall-agent-server/
(Dev) scudette:~$
Please choose the region where you want your App Engine application located:

[1] europe-west2 (supports standard and flexible)
[2] us-east1  (supports standard and flexible)
[3] us-east4  (supports standard and flexible)
[4] asia-northeast1 (supports standard and flexible)
[5] australia-southeast1 (supports standard and flexible)
[6] us-central (supports standard and flexible)
[7] europe-west3 (supports standard and flexible)
[8] europe-west (supports standard and flexible)
[9] cancel

Please enter your numeric choice: 6

Creating App Engine application in project [dfrws2017-rekall] and region [us-central]....done.

Services to deploy:

descriptor:  [/home/scudette/rekall-agent-server/app.yaml]
source:      [/home/scudette/rekall-agent-server]
target project: [dfrws2017-rekall]
target service: [default]
target version: [20170806t230849]
target url:  [https://dfrws2017-rekall.appspot.com]

Configurations to update:

descriptor:  [/home/scudette/rekall-agent-server/index.yaml]
type:        [datastore indexes]
target project: [dfrws2017-rekall]
Configurations to update:

descriptor: [/home/scudette/rekall-agent-server/index.yaml]
type: [datastore indexes]
target project: [dfrws2017-rekall]

Do you want to continue (Y/n)?

Beginning deployment of service [default]...
Some files were skipped. Pass `--verbosity=info` to see which ones.
You may also view the gcloud log file, found at
[/tmp/tmp.C25Ew73Fnc/logs/2017.08.06/23.07.59.356239.log].

== Uploading 862 files to Google Cloud Storage ==

--- File upload done.
Updating service [default]...done.
Waiting for operation [apps/dfrws2017-rekall/operations/585e5e6e-6171-4694]
Updating service [default]...done.
Deployed service [default] to [https://dfrws2017-rekall.appspot.com]
Updating config [index]...done.

Indexes are being rebuilt. This may take a moment.

You can stream logs from the command line by running:

$ gcloud app logs tail -s default

To view your application in the web browser run:

$ gcloud app browse
Self Guided Demo

There is a demo application you can use to play with The Rekall Agent Server.

This is a demo application

The demo application is exactly the same as the fully installed application bar for the following restrictions:
- All data is visible to anyone who logs into this installation. Please do not input sensitive information into the app since it is visible to anyone. This includes your Gmail user account which will also be visible to anyone.
- All data will be periodically wiped without warning. Please do not expect data to be retained.
- Anyone can fully interact with this demo installation. This means that anyone else can delete, modify or add any data, including remove data that you add. Please do not expect your data to be protected in any way.
- Please do not abuse the application. Abusers will be banned. Please remember that the application maintains detailed audit logging as well as request logs.
- If you find a problem or bug, please report it at support@rekall-forensic.com.

By using this application you acknowledge that you have read and understood these conditions. Press the below button and follow the login link.

MAKE ME ADMIN
Access management

- **Platform administrators:**
  - Users with AppEngine admin level access.
  - No access control! Can do anything within the App, including update the application, push new code etc.

- **Rekall Users**
  - Rekall does not deal with user accounts/passwords - these are done by GCP.
  - Rekall users are given roles within the application.
    - Investigator - can issue new collection flows.
    - Examiner - Can view existing collections.
    - Hunter - Can propose hunts for the entire fleet.
    - Approver - Can approve collection flows and hunts.
    - Administrator - Can grant other users roles!
Deployment - Users

- Roles are assigned on resources (securable objects):
  - Clients
  - Hunts
  - The Application
- It is possible for a user to have different roles on different resources.
- Client/Hunt approval workflow essentially grants roles on Hunt/Client.
- When the user attempts to access a Client/Hunt for which they have no access:
  - Approval request is sent to Approver.
  - Once approval is granted, the user may access the Client.
Auditing

- Every Action a user makes is being audited.
- Users need the Auditor role to be able to see the audit log.
Deployment - Client

- Prepare a client configuration file.
  - Use the server provided one as a template
- On all clients install the Rekall package, and optionally the Rekall Agent package.
  - Most enterprises have their own software management solution.
  - Endpoint deployment and configuration is an exercise left to the reader.
- One can run the client manually to see the debugging messages.
Client capabilities

- Rekall Agent just runs regular Rekall plugins and collects their results on the server.
  - This means you can test potential plugin invocations in the regular Rekall Console.
  - The Rekall Agent server just manages collection storage and access controls. It does not further analysis by itself.

- Most useful Rekall plugins:
  - EFilter queries - allows for arbitrary combinations of plugins, filtering the output and retrieving only selected information.
  - OSQuery plugin - run the normal OSQuery binary and collect the results.
  - Can run memory analysis but this should not be first option - use API mode first.

- Rekall Agent implement resource limits (total CPU and CPU load).
Example EFiltter queries.
select Hashes.md5, 
Path, 
Path.st_ino, 
Path.st_mode, 
Path.st_uid.uid, 
Path.st_gid.gid, 
Path.st_size, 
timestamp(Path.st_atime) as a, 
timestamp(Path.st_mtime) as m, 
timestamp(Path.st_ctime) as c from hash(paths: ( 
    select path from glob("/bin/*") 
).path.filename, hash: "md5")

Mactimes timeline output
## PluginAction(Search)

### Log Entries

<table>
<thead>
<tr>
<th>md5</th>
<th>Path</th>
<th>st_ino</th>
<th>st_mode</th>
<th>uid</th>
<th>gid</th>
<th>st_size</th>
<th>a</th>
<th>m</th>
<th>c</th>
<th>t</th>
</tr>
</thead>
<tbody>
<tr>
<td>004df9b650f2d2dfcd3378ee6c99bb5c</td>
<td>/bin/vdir</td>
<td>5031</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>118280</td>
<td>2015-03-14 15:47:04Z</td>
<td>2015-03-14 15:47:04Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>0097b50c0ef76c8d68f67ad1abc4fzzc0</td>
<td>/bin/dir</td>
<td>5005</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>118280</td>
<td>2015-03-14 15:47:04Z</td>
<td>2015-03-14 15:47:04Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>00f3823d41636686812020c08104672e</td>
<td>/bin/findmnt</td>
<td>5042</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>45216</td>
<td>2015-03-29 22:34:08Z</td>
<td>2015-03-29 22:34:08Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>03343bf5ba2365cd37f58109121b827</td>
<td>/bin/netstat</td>
<td>5022</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>120200</td>
<td>2014-11-08 18:09:08Z</td>
<td>2014-11-08 18:09:08Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>0643ad77bb207ac42ba4ebf6dcbcc42b3</td>
<td>/bin/grep</td>
<td>210</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>202936</td>
<td>2015-02-14 01:27:29Z</td>
<td>2015-02-14 01:27:29Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>08bc332b1d68296206d6d55f1cb6e6</td>
<td>/bin/pidof</td>
<td>4973</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>14</td>
<td>2015-04-06 18:44:32Z</td>
<td>2015-04-06 18:44:32Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>0a5dfab797000c147246b58df5167932</td>
<td>/bin/lsblk</td>
<td>4962</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>64552</td>
<td>2015-03-29 22:34:07Z</td>
<td>2015-03-29 22:34:07Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>0b54de9ff1f78e0b6802b691d3553c</td>
<td>/bin/run-parts</td>
<td>262</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>19312</td>
<td>2014-11-08 13:49:45Z</td>
<td>2014-11-08 13:49:45Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>10a5a0be2ad3f47ff1f2daaf1c0256c5</td>
<td>/bin/bzexe</td>
<td>4966</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>4877</td>
<td>2015-03-27 19:24:22Z</td>
<td>2015-03-27 19:24:22Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
<tr>
<td>12ba858a706f0e80095791f095ec382a</td>
<td>/bin/ps</td>
<td>5027</td>
<td>r-xr-x</td>
<td>0</td>
<td>0</td>
<td>930</td>
<td>2015-03-06 21:13:12Z</td>
<td>2015-03-06 21:13:12Z</td>
<td>2017-10-20 20:19:30Z</td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 120 entries

Search: 

Show 10 entries

1 of 12 pages

PREVIOUS 1 2 3 4 5 6 7 8 9 10 11 12 NEXT
Find **authorized_keys**.

A user left the company and we want to see if their SSH keys are still installed somewhere:

```sql
select * from file_yara(paths: (  
    select path.filename.name  
    from glob("/home/*/\.ssh/authorized_keys")  
).name,  
yara_expression: "rule r1 {strings: $a = \"T6qsh0WEh8pRvEKL/aZOBTKjr7d\" condition: any of them}"  
)  
```
Long running process from WebShell

A compromised webserver was found to contain a webshell. Which resource hungry processes were launched by the webshell?

```
select proc, proc.cpu_times.user from pslist() where proc.environ.HTTP_COOKIE =~ "WebShell-cwd"
```
Find out more!

The Rekall Agent White paper

Rekall's home on Github https://github.com/rekall-innovations

Rekall's site http://www.rekall-forensic.com/

Mailing list rekall-discuss@googlegroups.com