What's in a (user|host) name?

•••

That which we call a rose, by any other name, would still prick your fingers.

Logs 101: the basics

Logs - observable effects of an operation

Field - discrete components of a log

Parsing - identifying fields

Enrichment - adding information based on parsed values

Logstash - the one true log processor; log geeks want it, log software wants to be it

Translate - a logstash plugin that lets us do dictionary-style lookups based on field type/values

Logs 102: formats

Syslog - the devil, or at least his anarchist cousin; unstructured, arbitrary, ubiquitous

XML - the format used by Windows, highly structured

JSON - the only appropriate logging format

YAML - represents objects by a keyed value (multidimensional array++)

Logs 103: syslog and fields

20/11 10:30 10.10.15.18 password accepted for ceabhain

<date> <time_utc> <host_ip> <login_type> <login_status> for <username>

- date: “20/11”
- time_utc: “10:30”
- host_ip: “10.10.15.18”
- login_type: “password”
- login_status: “accepted”
- username: “ceabhain”

Why do I *really* like JSON?


```
{
        “date”: “20/11”,
        “time_utc”: “10:30”,
        “host_ip”: “10.10.15.18”,
        “login_type”: “password”,
        “login_status”: “accepted”,
        “username”: “ceabhain”
}
```

ceabhain, we hardly knew ye...

LDAP, Active Directory

- first/last name
- last password change
- certificate info
- department/division
- phone number
- building/office number
- photograph
- date created
- preferred/nicknames

- computer name (they're in AD, right?!)
- asset tag/information
- group memberships - "memberOf"
- email address
- hardware vendor
- primary user
- pretty much any other attribute you want to store

ldapsearch, getad-user, getad-computer, python + ldap3, powershell, pick your language

Build a User's Lookup Table (this is yaml)

```
ceabhain:
  dn: CN=Just A. Charlatan,OU=osg_users,DC=osg,DC=local
  displayname: Just A. Charlatan
  memberof:
          - CN=InfoSec,DC=osg,DC=local
conaire:
  dn: CN=Conaire MacLeoid,OU=osg_users,DC=osg,DC=local
  displayname: Conaire MacLeoid
  memberof:
          - CN=Mergers and Acquisitions,DC=osg,DC=local
```

https://github.com/kevinwilcox/python-elk/blob/master/crawl_ad_ldap/get_ad_users.py

Sample logstash “translate” Config

```
filter {
  if [username] {
    translate {
      field => “username”
      destination => “user_info”
      dictionary_path => “ldap_users.yml”
    }
  }
}
```

What Would That Login Log Look Like?


```
{
  "date": "20/11",
  "time_utc": "10:30",
  "host_ip": "10.10.15.18",
  "login_type": "password",
  "login_status": "accepted",
  "username": "ceabhain",
  "user_info": {
    "dn": "CN=Just A. Charlatan,OU=osg_users,DC=osg,DC=local",
    "displayname": "Just A. Charlatan",
    "memberof": "CN=InfoSec,DC=osg,DC=local"
  }
}
```

TELL ME MORE, TELL ME MORE!

(aka, what about the computer?)

Suppose an Inventory

```
10.10.14.1:
  hostname: infosec-paw-1
  mac_address: 00:12:34:56:78:90
10.10.15.18:
  hostname: mergers-01
  mac_address: 00:00:15:36:19:86
10.10.15.36:
  hostname: clancy-01
  mac_address: 00:00:10:05:09:70
  system_type: FreeBSD bastion host (headless)
```

With a Little Help From the User Script

```
infosec-paw-01:
  dn: CN=infosec-paw-01,OU=osg_paws,DC=osg,DC=local
  assigned_to: ceabhain
  location: 36.216, -81.682
mergers-01:
  dn: CN=mergers-01,OU=Mergers and Acquisitions,DC=osg,DC=local
  assigned_to: conaire
  location: 56.869687, -5.438271
  ups_connected: true
```

Two Logstash Translate Filters…

```
filter {
  if [host_ip] {
    translate {
      field => "host_ip"
      destination => "inv_info"
      dictionary_path => "inv_computers.yml"
    }
  }
}
```

```
filter {
  if [inv_info][hostname] {
    translate {
      field => "[inv_info][hostname]"
      destination => "ldap_computer_info"
      dictionary_path => "ldap_computers.yml"
    }
  }
}
```

And one filter for the GPS info...

```
filter {
  if [ldap_computer_info][location] {
    mutate {
      add_field => {
        "g_maps" => "https://www.google.com/maps/@%{[ldap_computer_info][location]},15z?hl=en"
      }
    }
  }
}
```

The enriched log!


```
{
  "date": "20/11",
  "time_utc": "10:30",
  "host_ip": "10.10.15.18",
  "login_type": "password",
  "login_status": "accepted",
  "username": "ceabhain",
  "user_info": {
    "dn": "CN=Just A. Charlatan,OU=osg_users,DC=osg,DC=local",
    "displayname": "Just A. Charlatan",
    "memberof": "CN=InfoSec,DC=osg,DC=local"
  },
  "inv_info": {
    "hostname": "mergers-01",
    "mac_address": "00:00:15:36:19:86"
  },
  "ldap_computer_info": {
    "dn": "CN=mergers-01,OU=Mergers and Acquisitions,DC=osg,DC=local",
    "assigned_to": "conaire",
    "location": "56.869687, -5.438271",
    "ups_connected": "true"
  },
 "g_maps": "https://www.google.com/maps/@56.869687,-5.438271,15z?hl=en"
}
```

With just one log entry, automated enrichment from existing systems and *one click* from an analyst...

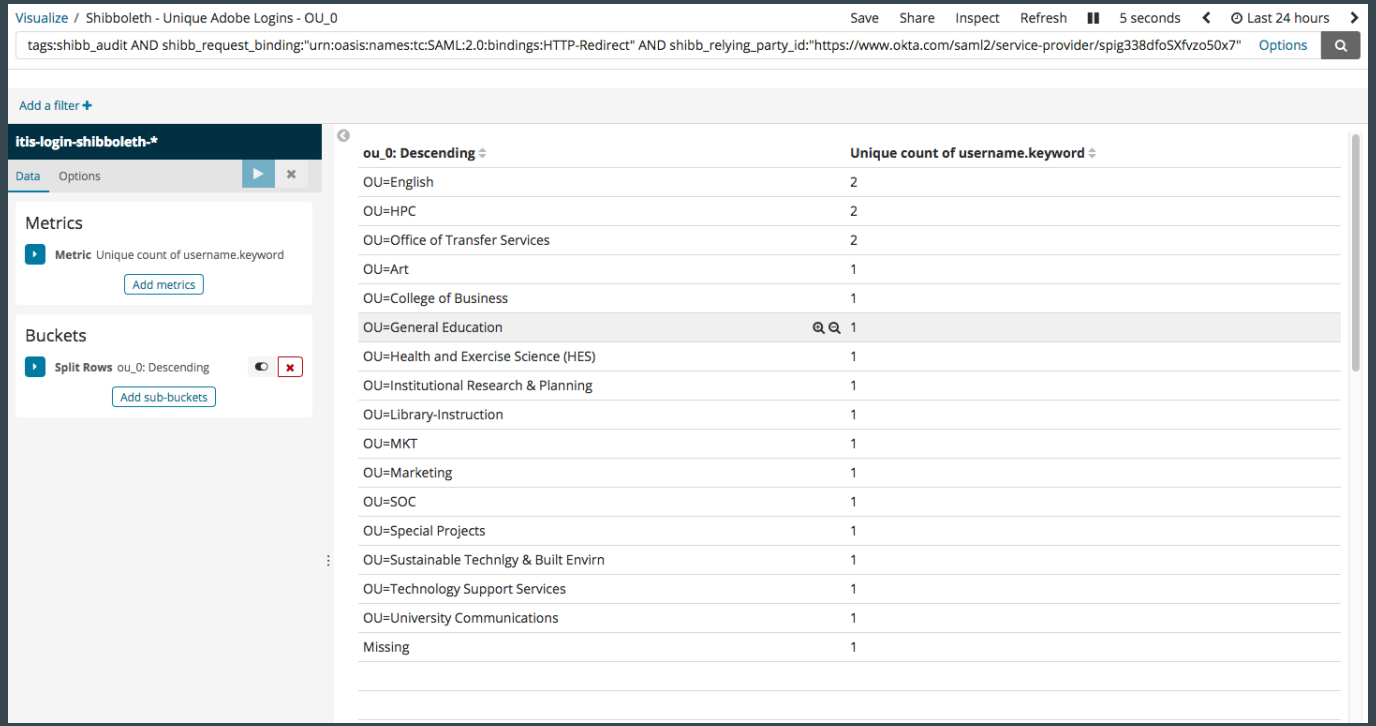
The story “in words”

From the log: on 20th November at 10.30 AM UTC, “ceabhain”’s username and password were used to login to a computer.

From enrichment: “ceabhain” is an InfoSec account and accessed a system in Mergers & Acquisitions that is powered via UPS. The system “ceabhain” logged into is assigned to Conaire MacLeoid, has a IP ending in 15.18, in the village of Gleann Fhionnain, on the shores of Loch Seile.

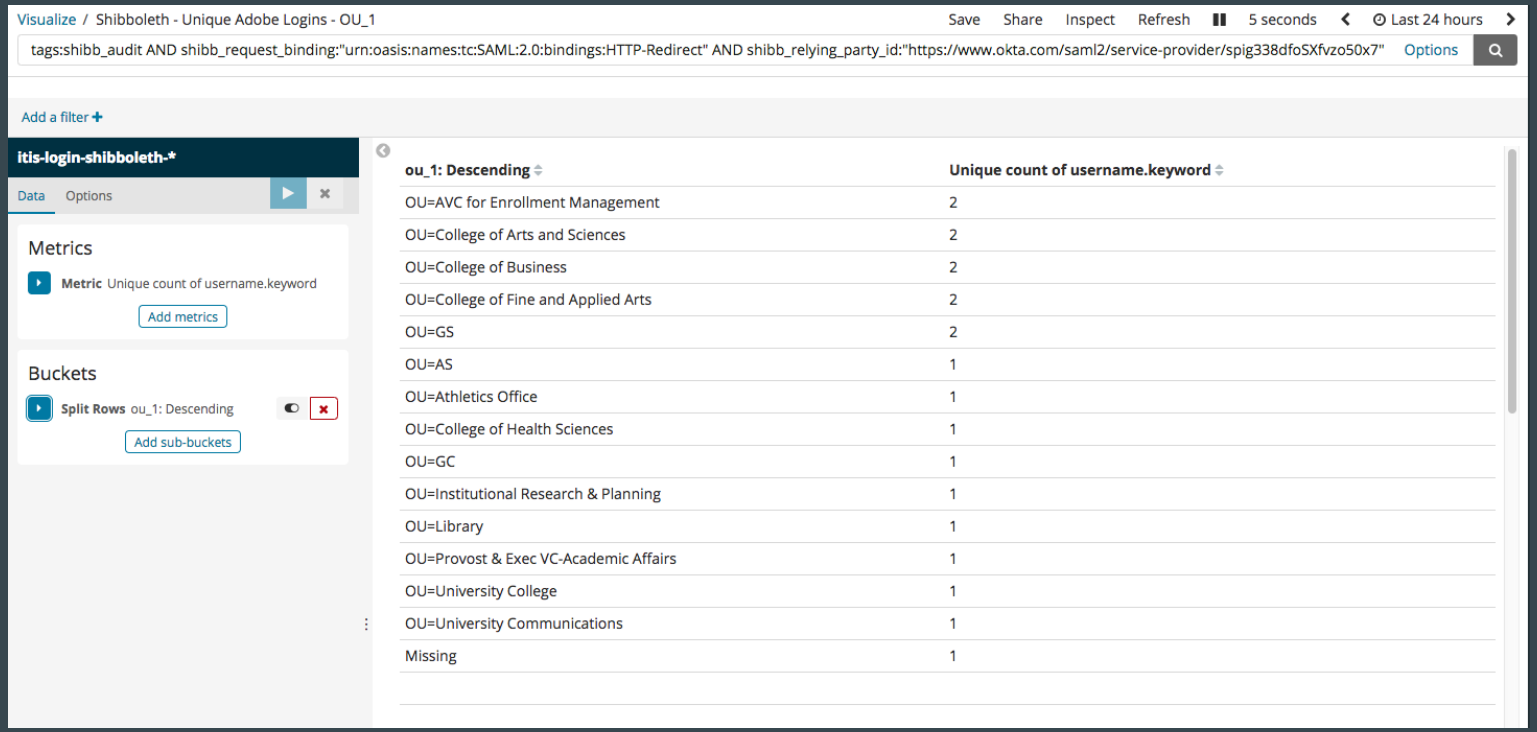
And it is immortal (at least until the UPS dies).

Real-life scenario



ou_0: Descending	Unique count of username.keyword
OU=English	2
OU=HPC	2
OU=Office of Transfer Services	2
OU=Art	1
OU=College of Business	1
OU=General Education	1
OU=Health and Exercise Science (HES)	1
OU=Institutional Research & Planning	1
OU=Library-Instruction	1
OU=MKT	1
OU=Marketing	1
OU=SOC	1
OU=Special Projects	1
OU=Sustainable Technlgy & Built Envirn	1
OU=Technology Support Services	1
OU=University Communications	1
Missing	1

Real-life 2



ou_1: Descending	Unique count of username.keyword
OU=AVC for Enrollment Management	2
OU=College of Arts and Sciences	2
OU=College of Business	2
OU=College of Fine and Applied Arts	2
OU=GS	2
OU=AS	1
OU=Athletics Office	1
OU=College of Health Sciences	1
OU=GC	1
OU=Institutional Research & Planning	1
OU=Library	1
OU=Provost & Exec VC-Academic Affairs	1
OU=University College	1
OU=University Communications	1
Missing	1

Search... (e.g. status:200 AND extension:PHP) Options

ou_0: "OU=Information Technology Service" tags.keyword: "user_lockout, login_failure" Add a filter + Actions

All filters: Enable Disable Pin Unpin Invert Toggle Remove

Visualise - AD Authentication Statuses

No results displayed because all values equal 0.

Visualise - AD Computer Logon

No results found

Visualise - AD User Lockouts

username.keyword: Descending	Count
mcdonnelltp	218

Visualise - AD User Logon

No results found

Search - Account Lockouts

1–50 of 218

Time	username	ad_display_name
9th November 2018, 15:18:24.040	mcdonnelltp	McDonnell, Tom
9th November 2018, 14:58:22.675	mcdonnelltp	McDonnell, Tom
9th November 2018, 14:37:05.922	mcdonnelltp	McDonnell, Tom
9th November 2018, 14:08:24.813	mcdonnelltp	McDonnell, Tom
9th November 2018, 13:44:31.002	mcdonnelltp	McDonnell, Tom
9th November 2018, 13:04:36.065	mcdonnelltp	McDonnell, Tom
9th November 2018, 12:47:27.238	mcdonnelltp	McDonnell, Tom
9th November 2018, 12:29:47.094	mcdonnelltp	McDonnell, Tom

Search - Aruba Failed Logins

1–50 of 11,033

Time	username	ad_display_name	ou_0	usermac	apname
21st November 2018, 10:58:37.450	hodgesji	Hodges, Josh	OU=Information Technology Service	b0:19:c6:bf:18:e8	AP_COE_505_Hall
21st November 2018, 10:58:33.803	hodgesji	Hodges, Josh	OU=Information Technology Service	b0:19:c6:bf:18:e8	AP_COE_504C_Hall
21st November 2018, 10:58:31.367	hodgesji	Hodges, Josh	OU=Information Technology Service	b0:19:c6:bf:18:e8	AP_COE_504C_Hall
21st November 2018, 10:33:05.473	hodgesji	Hodges, Josh	OU=Information Technology Service	b0:19:c6:bf:18:e8	AP_COE_505_Hall
21st November 2018, 10:33:01.748	hodgesji	Hodges, Josh	OU=Information Technology Service	b0:19:c6:bf:18:e8	AP_COE_505_Hall
21st November 2018, 10:32:59.589	hodgesji	Hodges, Josh	OU=Information Technology Service	b0:19:c6:bf:18:e8	AP_COE_506A_Hall

The Takeaways…

We have multiple sources of information about various names:

- Active Directory
- LDAP
- DNS
- Inventory Databases

By enriching logs from those data sources:

- “business logic” built into SIEM “flow”, increasing value
- analysts get a “big picture” view earlier in the process
- analysts can spend their time more effectively
- group-based reporting is quicker and easier
- mismatches and anomalies start to become more obvious
- seemingly “common” events can become actionable indicators