DNS Search Techniques

More search techniques for everyday Splunkers

The Pavo team at Aplura wanted to highlight a commonly requested search technique that can help polish and tune a Splunk Use Case. In this post, we will talk about DNS resolution in the searches themselves!

DNS is becoming increasingly important in correlating events and incidents; however in many cases logs do not have both an IP and DNS name. We can use the feature "lookup dnslookup " in order to resolve an IP address or vice versa.

Here are some starter examples you might have run into:

- Your boss needs a report of system names accessing the VPN, but the VPN only logs the IP address. Use this lookup to find the host names in that report.
- You need to correlate the IPs of systems in IDS logs to the names of systems in the authentication logs. Use this lookup to find the host names, then search those names in the authentication logs.
- Your vulnerability data has the names of systems, but you need to have both the names and IP addresses for your report. Use the reverse lookup to output the IP addresses for those names.

Of course, all commands have a few things to keep in mind. This lookup tries to resolve each value it is passed when the search runs. This could add more information, but it also slows down the search. Also, if the name or IP does not resolve, you won't have a value.

Now that we know how useful it is, let's take a look at the syntax. Splunk ships configurations out of the box with this external lookup ready. You do not have to add configurations to it.

This search performs a DNS lookup on the field named "IP_data_field" and outputs the results in "host_data_field."

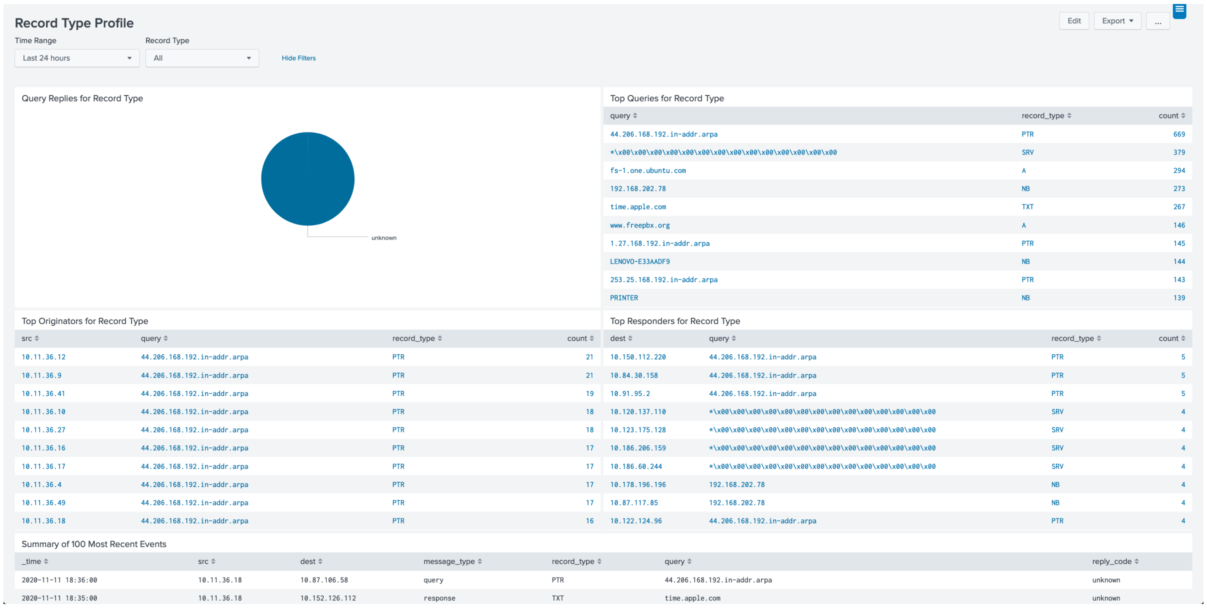
```
index=gogo sourcetype=gaga | lookup dnslookup clientip as IP_data_field OUTPUT clienthost as host_data_field
```

This search performs a reverse DNS lookup on the field named "host_data_field" and outputs the results in "IP_data_field."

```
index=happy sourcetype=joyjoy | lookup dnslookup clienthost as host_data_field OUTPUT clientip as IP_data_field
```

Maybe you don't need to resolve fields in your current use case but instead need to explore, analyze, and report on the DNS logs directly. Our PAVO DNS App for Splunk can help do just that. Download today.

The app uses Splunk CIM normalized data and can help you quickly find a breakdown of queries to non-existent domains; maybe you need to highlight anomalies of DNS record types; or you need to add transparency to where all the DNS data is coming from, and much more.



Record Type Profile

Time Range: Last 24 hours

Record Type: All

Query Replies for Record Type

Top Queries for Record Type

query	record_type	count
44.206.168.192.in-addr.arpa	PTR	669
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	SRV	379
fs-1.one.ubuntu.com	A	294
192.168.202.78	NB	273
time.apple.com	TXT	267
www.freepbx.org	A	146
1.27.168.192.in-addr.arpa	PTR	145
LENOVO-E33AADF9	NB	144
253.25.168.192.in-addr.arpa	PTR	143
PRINTER	NB	139

Top Originators for Record Type

src	query	record_type	count
10.11.36.12	44.206.168.192.in-addr.arpa	PTR	21
10.11.36.9	44.206.168.192.in-addr.arpa	PTR	21
10.11.36.41	44.206.168.192.in-addr.arpa	PTR	19
10.11.36.10	44.206.168.192.in-addr.arpa	PTR	18
10.11.36.27	44.206.168.192.in-addr.arpa	PTR	18
10.11.36.16	44.206.168.192.in-addr.arpa	PTR	17
10.11.36.17	44.206.168.192.in-addr.arpa	PTR	17
10.11.36.4	44.206.168.192.in-addr.arpa	PTR	17
10.11.36.49	44.206.168.192.in-addr.arpa	PTR	17
10.11.36.18	44.206.168.192.in-addr.arpa	PTR	16

Top Responders for Record Type

dest	query	record_type	count
10.150.112.220	44.206.168.192.in-addr.arpa	PTR	5
10.84.30.158	44.206.168.192.in-addr.arpa	PTR	5
10.91.95.2	44.206.168.192.in-addr.arpa	PTR	5
10.120.137.110	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	SRV	4
10.123.175.128	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	SRV	4
10.186.206.159	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	SRV	4
10.186.60.244	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	SRV	4
10.178.196.196	192.168.202.78	NB	4
10.87.117.85	192.168.202.78	NB	4
10.122.124.96	44.206.168.192.in-addr.arpa	PTR	4

Summary of 100 Most Recent Events

_time	src	dest	message_type	record_type	query	reply_code
2020-11-11 18:36:00	10.11.36.18	10.87.106.58	query	PTR	44.206.168.192.in-addr.arpa	unknown
2020-11-11 18:35:00	10.11.36.18	10.152.126.112	response	TXT	time.apple.com	unknown