Using Log Correlation Engine to Monitor DNS

September 6, 2013

(Revision 2)

Table of Contents

Introduction

This document describes strategies to leverage Tenable Network Security's Log Correlation Engine (LCE) to monitor DNS activity on your network. Each section considers the types of DNS logs that can be gathered and how the LCE's set of correlation, anomaly, reporting, dashboard, and alerting functions can be used most effectively.

This document provides users ideas and inspiration to develop new approaches for how the data they are collecting can be used for more effective dashboards, alerts, and reports. In addition, it provides insight into what users *may not* be logging and how this can impact incident detection or compliance monitoring.

For a more advanced discussion of the LCE's correlation functions, please refer to the Tenable Event Correlation paper available on the Tenable Support Portal, which is designed to complement this paper.

Normalized event names reported by the LCE are created from various words indicative of the event and are typically separated by dashes and underscores such as "**Port_Scan**" or "**Cisco-Login_Failure**". However, when referring to the name of the event within this document, the dashes and underscores are often omitted and written with just the base keywords such as "Port Scan" or "Cisco Login Failure". It is assumed that readers are familiar with the LCE's asset creation, asset filtering, log normalization, log compression/search, correlation, and working with LCEs as well as statistical events.

If you have suggestions to further extend this document, please email us at support@tenable.com or post your suggestions and use cases to the Tenable Discussion Forums.

DNS Logs and Passive Monitoring

Converting a domain name to an IP address is the first step in most Internet communications. Tenable's Log Correlation Engine (LCE) can work with logs from devices that provide Domain Name Service (DNS) to network users and with logs from devices that log DNS activity.

DNS Log Categories

LCE processes DNS related logs with the following types:

- **application** – Logs from DNS servers related to the application itself such as the start of a zone transfer between two DNS servers.
- **dns** – Logs that indicate a query from a DNS name to an IP address or vice versa have occurred. Logs can come directly from a DNS server, such as BIND, or they can be passively logged by a product such as the Tenable Passive Vulnerability Scanner (PVS). Queries for DNS names that have failed are also typically logged to this category.
- **error** – Any logs related to the DNS application that indicate an error.
- **startup** – Any logs from a DNS appliance or DNS service that indicate a reboot, restart, or service availability.

LCE will also make use of certain "**web-access**" and "**file-access**" events that have logged an HTTP query for DNS based reporting. A web proxy or a Passive Vulnerability Scanner (PVS) will be able to log or sniff web traffic to URLs such as "http://www.nessus.org/plugins" and treat "www.nessus.org" as a DNS query.

If you have a DNS server, such as BIND, and you are only logging application logs about DNS server activity and are not logging actual DNS queries, you will have limited forensic or reporting ability for DNS. If you are only logging perimeter web proxy logs, you do not have visibility into email, FTP, and many other non-web DNS queries. If you have a PVS sensor and have only configured it to sniff vulnerabilities, you will not have access to real-time DNS query (and web transaction) logs.

Benefits of Logging DNS Queries

Configuring your system to log DNS queries provides the following benefits:

- The ability to search DNS records for malicious names as well as names of interest.
- The ability to summarize the queries to understand what sort of web sites and network resources a given node has used.
- The ability to log DNS query errors can help identify misconfigured and compromised endpoints.

Example DNS Logs

Following is a log from DNS BIND that indicates a zone transfer is starting:

```
Oct 15 14:24:12 ve-du0c named[03043]: [ID 424333 daemon.info] zone
       someplace.net.dk/IN/internal: Transfer started
```

This would be normalized to an event name of “**Bind Zone Transfer Started**” and an event type of “**application**”.

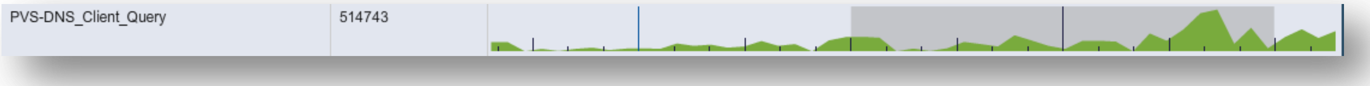
Following is a log that indicates that a DNS query has occurred:

```
<134>named[7273]: queries: client 192.168.0.16#52742: query: spamalot.someplace.org IN
       A +
```

This log would be normalized to an event name of “**Bind Query IPv4**” an event type of “**dns**”.

Benefits of Monitoring Passive DNS Logging

Following is a screen capture of DNS lookup events observed by Tenable’s Passive Vulnerability Scanner (PVS) at an active university of 2,500 students:



PVS-DNS_Client_Query 514743

There are multiple DNS servers on campus, but none of them have been configured to log DNS transactions or send their logs to the LCE. The screen capture shows that 514,743 DNS lookups have been observed in a 24 hour period.

All of these events have been normalized to an event type of “**dns**” and the PVS event name of “**PVS DNS Client Query**”. If DNS queries were present from other log sources such as BIND, they would also be present in this view.

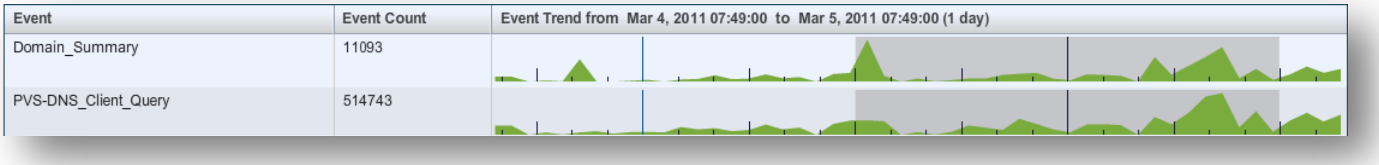
PVS not only sees DNS queries from these DNS servers, it also sees DNS queries that have been made directly to the Internet. For example, a system compromised as part of a botnet may have its own list of DNS servers to query.

DNS Summary Reporting

In the screen capture above, there were more than half a million DNS queries in a 24 hour period. This sort of data is useful from a statistical anomaly point of view or to forensically review each DNS query performed by a host. The next section describes strategies for searching DNS query logs. For now, it is sufficient to note that LCE summarizes all DNS and Web queries.

LCE analyzes DNS query logs from PVS, from DNS servers and also from web queries logged by PVS or web proxy devices. LCE uses an efficient in-memory storage system to automatically create summary alerts.

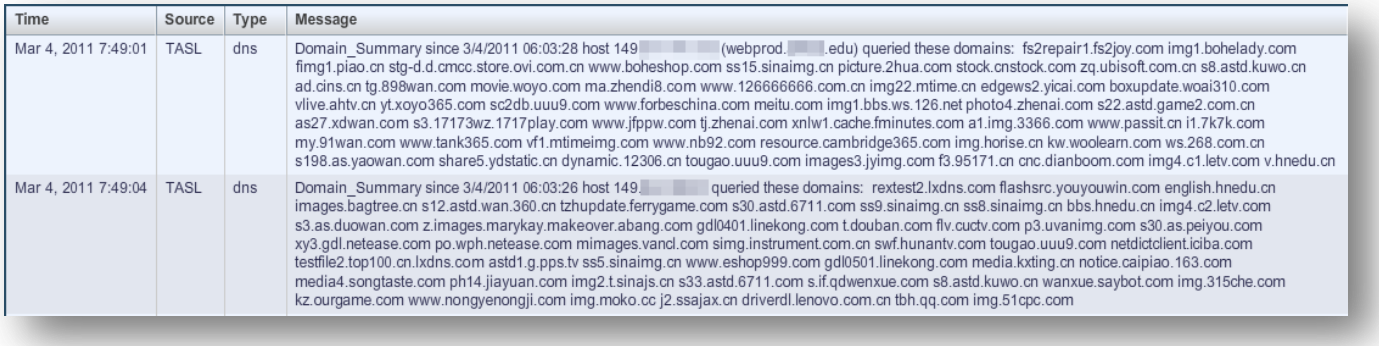
Following is a screen capture from the same university with the half million DNS queries in one day:



Event	Event Count	Event Trend from Mar 4, 2011 07:49:00 to Mar 5, 2011 07:49:00 (1 day)
Domain_Summary	11093	
PVS-DNS_Client_Query	514743	

The "**Domain Summary**" event is generated any time LCE reaches capacity for the amount of data it is tracking. Once a domain is seen, possibly from a host performing a DNS lookup for "cnn.com", that domain will only be reported once until LCE encounters so many unique host DNS pairs that it needs to reset itself. How often this occurs depends on the number of total unique queries.

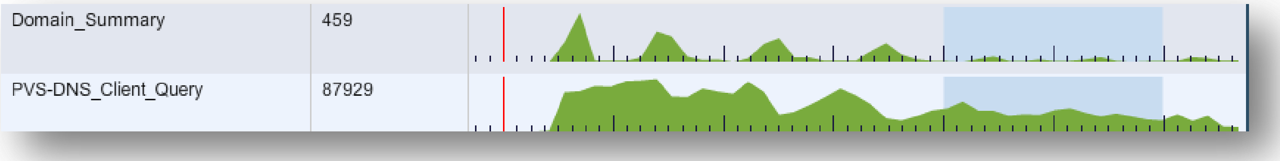
Following is a sanitized screen capture of what a "Domain Summary" event log looks like:



Time	Source	Type	Message
Mar 4, 2011 7:49:01	TASL	dns	Domain_Summary since 3/4/2011 06:03:28 host 149[redacted](webprod.[redacted].edu) queried these domains: fs2repair1.fs2joy.com img1.bohelady.com fimg1.piao.cn stg-d.d.cmcc.store.ovi.com.cn www.boheshop.com ss15.sinaimg.cn picture.2hua.com stock.cnstock.com zq.ubisoft.com.cn s8.astd.kuwo.cn ad.cins.cn tg.898wan.com movie.woyo.com ma.zhendi8.com www.126666666.com.cn img22.mtime.cn edgews2.yicai.com boxupdate.woai310.com vlive.ahtv.cn yt.xoyo365.com sc2db.uuu9.com www.forbeschina.com meitu.com img1.bbs.ws.126.net photo4.zhenai.com s22.astd.game2.com.cn as27.xdwan.com s3.17173wz.1717play.com www.jfppw.com tj.zhenai.com xnlw1.cache.fminutes.com a1.img.3366.com www.passit.cn i1.7k7k.com my.91wan.com www.tank365.com vf1.mtimeimg.com www.nb92.com resource.cambridge365.com img.horise.cn kw.woolearn.com ws.268.com.cn s198.as.yaowan.com share5.ydstatic.cn dynamic.12306.cn tougao.uuu9.com images3.jyimg.com f3.95171.cn cnc.dianboom.com img4.c1.letv.com v.hnedu.cn
Mar 4, 2011 7:49:04	TASL	dns	Domain_Summary since 3/4/2011 06:03:26 host 149.[redacted] queried these domains: rextest2.lxdns.com flashsrc.youyouwin.com english.hnedu.cn images.bagtree.cn s12.astd.wan.360.cn tzhupdate.ferrygame.com s30.astd.6711.com ss9.sinaimg.cn ss8.sinaimg.cn bbs.hnedu.cn img4.c2.letv.com s3.as.duowan.com z.images.marykay.makeover.abang.com gdl0401.linekong.com t.douban.com flv.cuctv.com p3.uvanimg.com s30.as.peiyou.com xy3.gdl.netease.com po.wph.netease.com mimages.vancl.com simg.instrument.com.cn swf.hunantv.com tougao.uuu9.com netdictclient.iciba.com testfile2.top100.cn.lxdns.com astd1.g.pps.tv ss5.sinaimg.cn www.eshop999.com gdl0501.linekong.com media.kxting.cn notice.caipiao.163.com media4.songtaste.com ph14.jiayuan.com img2.t.sinajs.cn s33.astd.6711.com s.if.qdwenxue.com s8.astd.kuwo.cn wanxue.saybot.com img.315che.com kz.ourgame.com www.nongyenongji.com img.moko.cc j2.ssajax.cn driverdl.lenovo.com.cn tbh.qq.com img.51cpc.com

This summary is useful for forensic analysis, employee monitoring and creating reports. For this particular network, LCE has taken the half million DNS queries and reduced this to around 11,000 "Domain Summary" reports that consider all previous DNS queries that occurred before this 24 hour period.

The following is a screen capture that is typical of a network where users frequently go to the same destinations. You can see a general downward trend in "**Domain Summary**" events. Even if a user visits gmail.com, facebook.com, or yahoo.com hundreds of times a week or day, it will only get reported in the "**Domain Summary**" log once.



Domain_Summary	459	
PVS-DNS_Client_Query	87929	

Searching, Alerting, and Reporting on DNS Logs

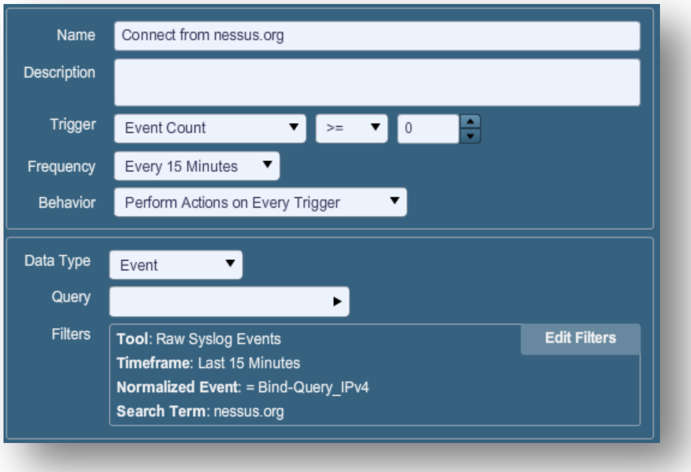
Generally, there are two types of searches conducted on DNS events: those looking for specific DNS entries, and those looking for keywords.

Searching for Specific DNS Names

Entering a domain name into the LCE's "**Raw Logs**" search tool can help you identify occurrences of it in any log. This is useful because domain names often show up in logs associated with logins, transmission of email, web logs, and more.

If you want to look for a domain name while working with normalized events, you can filter on a set of events you want, such as a “**Bind Query IPv4**” event, and then choose the “**Raw Syslog Events**” filter with an additional “**Syslog Search Terms**” filter for your domain of interest.

If you would like to alert when activity to a certain domain occurs, consider scheduling an LCE alert that leverages an event such as “**Bind Query IPv4**” analyzed with the “**Raw Syslog Events**” tool with an additional filter to generate an alert on the domain name. The following screen capture uses the Bind IPv4 DNS event lookup filtered for “nessus.org” every 15 minutes:



Name: Connect from nessus.org

Description:

Trigger: Event Count >= 0

Frequency: Every 15 Minutes

Behavior: Perform Actions on Every Trigger

Data Type: Event

Query:

Filters:

Tool: Raw Syslog Events

Timeframe: Last 15 Minutes

Normalized Event: = Bind-Query_IPv4

Search Term: nessus.org

As with most LCE scheduled alerts, we have aligned our query of 15 minutes with a schedule of 15 minutes to avoid over or under-counting potential DNS activity.

It is important to note that if you have **User ID to IP** address tracking enabled on your LCE, you can combine the “**Domain Summary**” log with a user ID query to create a report for all the domain names that user has visited.

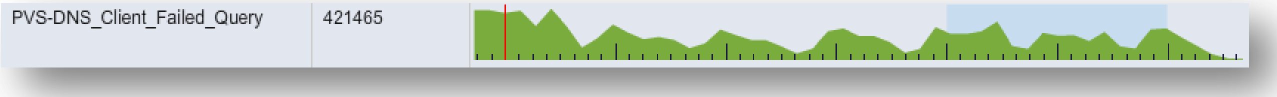
Searching for Keywords

The second type of DNS search is to look for keywords that indicate the presence of websites and activity that should not be occurring on your network. There are many different types of Internet destinations that may be not authorized for your network. Adult content, drug use, political blogging, gambling, video games, terrorism, visits to competitor websites, visits to social networking sites, and visits to potentially suspicious countries are just some of the types of items that can be searched for in DNS logs.

When working with large user populations of DNS queries, it is important to note that simple keyword searches in DNS logs can have false positives. For example, searching for sexually explicit terms could result in hits for visits to adult websites as well as medical websites. Searching for short keywords such as “sex” could match on sites that contained the word, such as “MSExhange”, but do not really have anything to do with the searched topic. Finally, put yourself in the position of the user you may be monitoring. Visits to Facebook, Gmail, and even CNN can present users with advertisements that cause questionable DNS lookups. Just because it appears that a user that has had some queries for some potentially interesting or suspicious domains, it does not mean the user intended to go there.

Failed DNS lookups

We have all typed in an address for a web site or an email incorrectly at some point. This likely resulted in a query to the DNS servers for a domain name that did not exist. These types of events are logged by DNS servers and can also be passively discovered with PVS. Following is a screen capture of seven days of “**PVS DNS Client Failed Query**” events from a small ISP:



PVS-DNS_Client_Failed_Query 421465

Identifying Source of Failed Queries

Having a record of failed DNS queries is not as interesting as knowing which hosts on your network are doing this and the frequency with which they are performing these queries.

When a node is infected with malware that can be used to attack other computers or send spam email, it is very likely that the computer will perform many DNS lookups for websites and email servers that do not exist.

A key principle of botnets is that their command and control nodes are constantly moving to new locations. DNS is primarily used to allow compromised nodes to find new command and control resources. In the process of communicating with these nodes, it is likely that DNS queries for various parts of the botnet infrastructure fail.

With spam, if a compromised node is sending out many emails, it is possible that the attempts to connect to the email servers fail because they do not exist. This usually results in a DNS query failure.

Finally, you may have a network that has a computer on it that has not been compromised, but is not correctly configured for DNS. It may be pointing to DNS servers that are out of date or are no longer in production.

Passively Tracking DNS Lookup Failures

LCE's tracking of DNS lookups via the **Domain_Summary** report was recently updated to process failed DNS logs observed by the Passive Vulnerability Scanner. The ability to quickly browse a list of unique failed DNS lookups provides insight into misconfigured systems and potential malware. Tracking malware queries is important for malware investigation because DNS names and domains are often taken down once they become known.

Following is an example log of a sniffed DNS lookup failure from the Passive Vulnerability Scanner:

```
<36>Aug 15 15:48:44 pvs: 192.168.1.56:0|192.168.1.56:0|17|7027|DNS Client Failed
       Query|version: $Revision: 1.13 $ PVS has observed this host perform a failed
       DNS lookup for: b._dns-sd._udp.0.36.168.192.in-addr.arpa from the DNS server at
       192.168.1.1|NONE
```

This log is normalized by the LCE to an event type of **PVS-DNS_Client_Failed_Query** and type of "**dns**".

LCE will aggregate these events and create reports of unique domain lookup failures for each host. Following are some example logs:

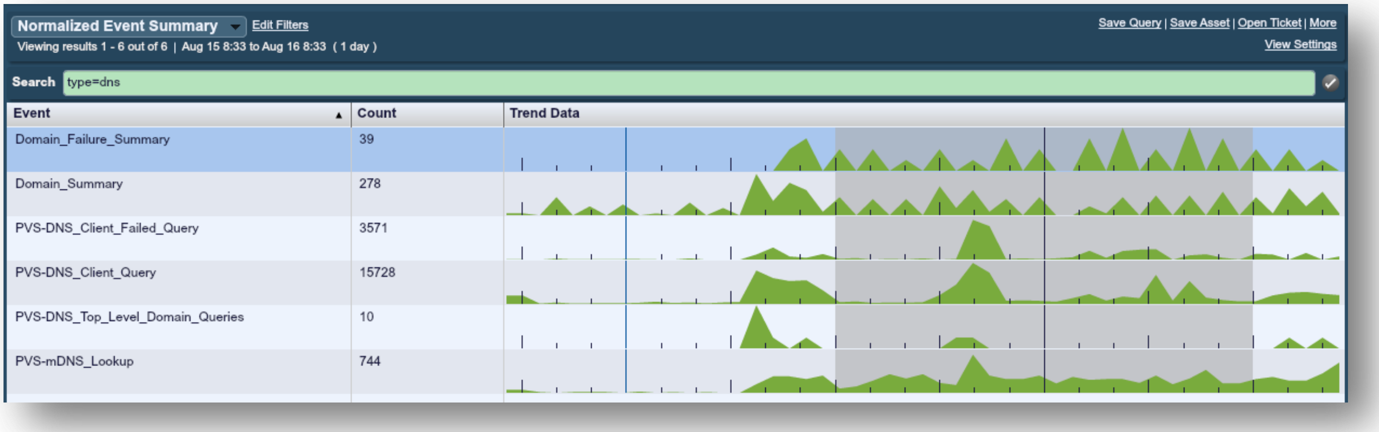
```
Domain_Failure_Summary since 8/16/2013 01:09:52 host 192.168.1.14 failed to query
       these domains: b._dns-sd._udp.0.1.168.192.in-addr.arpa db._dns-
       sd._udp.0.1.168.192.in-addr.arpa r._dns-sd._udp.0.1.168.192.in-addr.arpa
       dr._dns-sd._udp.0.1.168.192.in-addr.arpa lb._dns-sd._udp.0.1.168.192.in-
       addr.arpa
```

```
Domain_Failure_Summary since 8/16/2013 02:55:57 host 192.168.1.61 failed to query
       these domains: zfxumrtgrg.lab
```

These logs are normalized to the **Domain_Failure_Summary** event name and are also part of the "**dns**" class of LCE events.

The **Domain_Failure_Summary** event can also dramatically speed your searches for malware or failed DNS queries of interest. Since the LCE stores these names in a summary table, there are actually fewer logs for queries to be run against, speeding up your reports and analytics.

Below is a screen capture where all PVS and DNS traffic has been viewed for the past 24 hours.



Normalized Event Summary

Viewing results 1 - 6 out of 6 | Aug 15 8:33 to Aug 16 8:33 (1 day)

Search type=dns

Event ▲	Count	Trend Data
Domain_Failure_Summary	39	
Domain_Summary	278	
PVS-DNS_Client_Failed_Query	3571	
PVS-DNS_Client_Query	15728	
PVS-DNS_Top_Level_Domain_Queries	10	
PVS-mDNS_Lookup	744	

DNS Query Anomaly Activity

The LCE **`stats`** daemon will report on any DNS spike. This includes both DNS query logs as well as DNS lookup failures. The following event types can be generated by the **`stats`** daemon regarding DNS queries:

- Statistics-DNS_Minor_Anomaly
- Statistics-DNS_Anomaly
- Statistics-DNS_Medium_Anomaly
- Statistics-DNS_Large_Anomaly

When analyzing these types of events, consider splitting your analysis into two groups: servers and assets that perform a lot of DNS lookups and those that do not. An email server makes lots of DNS lookups compared to a corporate desktop driven by a user.

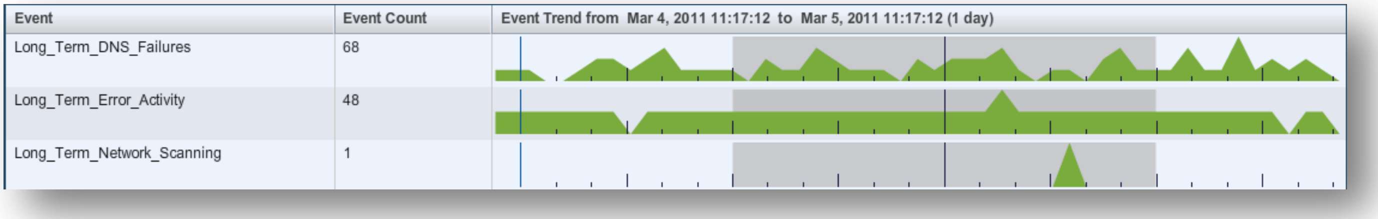
Based on volume of users and activity, the **`stats`** daemon will likely detect changes in DNS activity that reflect changes in legitimate email message volume, web site popularity, and even employee workload. However, a spike could also be associated with activity from compromised servers, malicious email campaigns targeted at your organization, and denial of service attacks.

When analyzing a non-server spike in DNS activity, see if you can corroborate any type of other activity on the host. For example, if a user installs an RSS reader and then regularly starts reading RSS feeds from 100 new web sites every day, this could generate a large spike in DNS lookups compared to traditional email and web browsing. Such activity would likely be reported by the **`stats`** daemon as a minor or regular anomaly.

If the spike on any host is the result of DNS lookup failures, inspect a sample of the DNS lookup failure logs to see what was occurring. If they are for internal resources, you likely have a misconfigured system, domain controller, or DNS server. If the domains are random, outside of your network and/or highly random in nature, you may have a compromised system that is sending spam, or attacking other computers.

Detecting Continuous DNS Lookup Errors

LCE identifies when an internal or external host generates continuous intrusion, scanning, error, DNS lookup error, hung applications, virus, or social-network event types. From the LCE's perspective, a continuous event is one that occurs at least once for two 20 minute periods. This may seem arbitrary, but it has been shown to be very effective at a variety of customer sites in finding systems that have had a number of issues. Following is a screen capture showing multiple different types of events from the "**continuous**" event type category:



Event	Event Count	Event Trend from Mar 4, 2011 11:17:12 to Mar 5, 2011 11:17:12 (1 day)
Long_Term_DNS_Failures	68	
Long_Term_Error_Activity	48	
Long_Term_Network_Scanning	1	

Continuous events are all labeled with the tag "Long Term". By default, LCE watches for activity from a host in periods of 20 minutes. It will reissue an alert as the activity continues for 20 minutes, 40 minutes, etc. In the above screen capture, the DNS lookup errors occurring continuously are related to the "**Long Term DNS Failures**" events. Below is an example log generated by LCE:

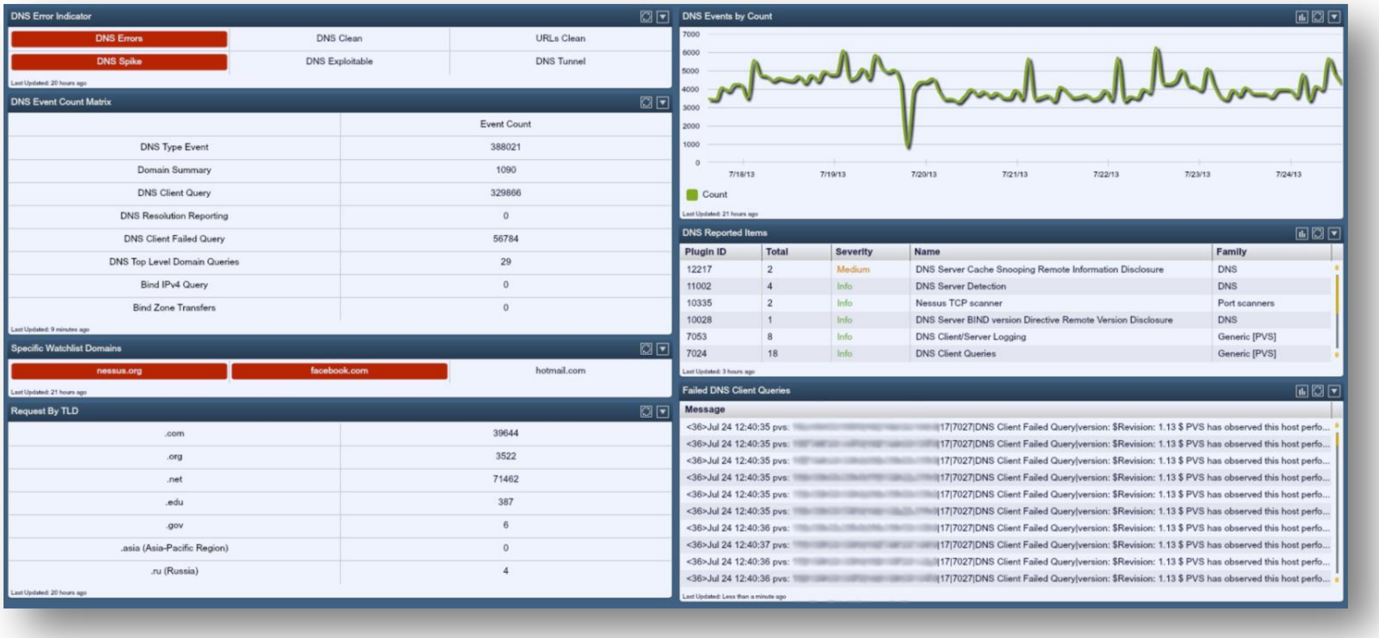
```
Long_Term_DNS_Failures - There has been 140 minutes of continuous failed DNS activity
      from host 192.168.1.58 (lap11109.home) and the most recent event was failed-
      query towards host 192.168.1.1 (Wireless_Broadband_Router.home) at 2/7/2011
      03:21:09
```

We can see that the level of DNS lookups has been continuing for 140 minutes. In this case, 192.168.1.1 is the local DNS server and it does not know how to use the ".home" domain name suffix.

When issues like this occur on live networks, use a similar analysis approach as that recommended for statistical anomalies. Continuous DNS lookup failures for servers are analyzed differently than for a desktop. It is likely that your email gateway performs a lot of DNS lookups that fail while sending email on a daily basis. However, this may not be true for a desktop, a router, or a wireless access point.

Using LCE to View DNS Events at a Glance

Using a SecurityCenter dashboard, it is possible to review everything discussed in this guide at a glance. The dashboard displayed below uses data collected from Nessus vulnerability scans, and also utilizes data from PVS. The information below focuses specifically on the usage of LCE normalized data in the dashboard.



DNS Error Indicator

DNS Errors	DNS Clean	URLs Clean
DNS Spike	DNS Exploitable	DNS Tunnel

Last Updated: 20 hours ago

DNS Event Count Matrix

	Event Count
DNS Type Event	388021
Domain Summary	1090
DNS Client Query	329866
DNS Resolution Reporting	0
DNS Client Failed Query	56784
DNS Top Level Domain Queries	29
Bind IPv4 Query	0
Bind Zone Transfers	0

Last Updated: 9 minutes ago

Specific Watchlist Domains

nessus.org	facebook.com	hotmail.com

Last Updated: 21 hours ago

Request By TLD

.com	39644
.org	3522
.net	71462
.edu	387
.gov	6
.asia (Asia-Pacific Region)	0
.ru (Russia)	4

Last Updated: 20 hours ago

DNS Events by Count

Last Updated: 21 hours ago

DNS Reported Items

Plugin ID	Total	Severity	Name	Family
12217	2	Medium	DNS Server Cache Snooping Remote Information Disclosure	DNS
11002	4	Info	DNS Server Detection	DNS
10335	2	Info	Nessus TCP scanner	Port scanners
10028	1	Info	DNS Server BIND version Directive Remote Version Disclosure	DNS
7053	8	Info	DNS Client/Server Logging	Generic [PVS]
7024	18	Info	DNS Client Queries	Generic [PVS]

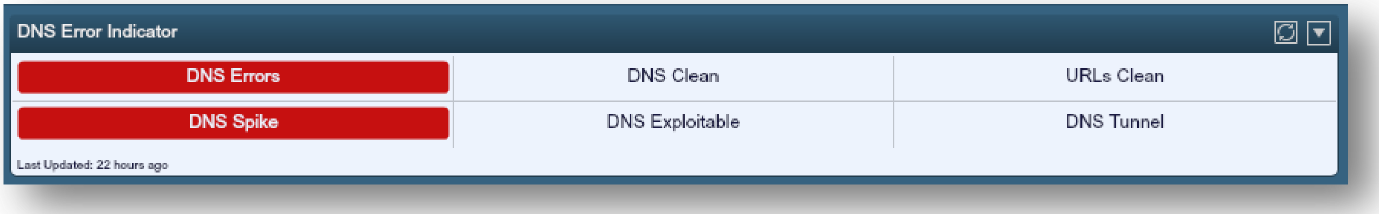
Last Updated: 3 hours ago

Failed DNS Client Queries

```
Message
<36>Jul 24 12:40:35 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:35 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:35 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:35 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:35 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:35 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:36 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:37 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:36 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 12:40:36 pvs: [redacted]|17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
```

Last Updated: Less than a minute ago

The "**DNS Error Indicator**" section of the dashboard displays "**DNS Errors**", which uses the "**Long Term DNS Failures**" normalized event to show failed DNS errors from the last 48 hours. Also, the "**DNS Spike**" feature uses the "**Statistics DNS Large Anomaly**" normalized event to show an abnormal increase in DNS queries in the same 48 hour period. Finally, the dashboard utilizes information received by LCE from PVS to show DNS tunnel activity in the last 48 hours.

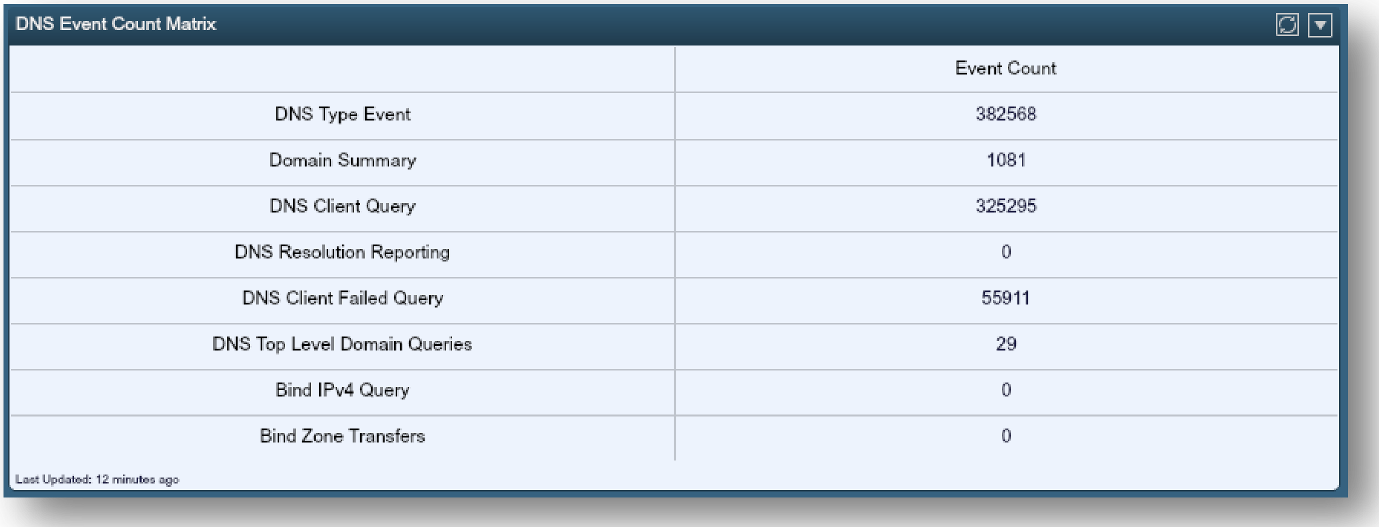


DNS Error Indicator

DNS Errors	DNS Clean	URLs Clean
DNS Spike	DNS Exploitable	DNS Tunnel

Last Updated: 22 hours ago

In the "**DNS Event Count Matrix**" section of the dashboard, the event count is shown that includes the count of DNS related events of various types using LCE normalized event data. This section of the dashboard uses normalized data from LCE "**Domain Summary**", "**PVS DNS Client Query**", "**PVS DNS Resolution Reporting**", "**PVS DNS Client Failed Query**", "**PVS DNS Top Level Domain Queries**", "**Bind IPv4 Query**", and "**Bind Zone Transfer Started**".

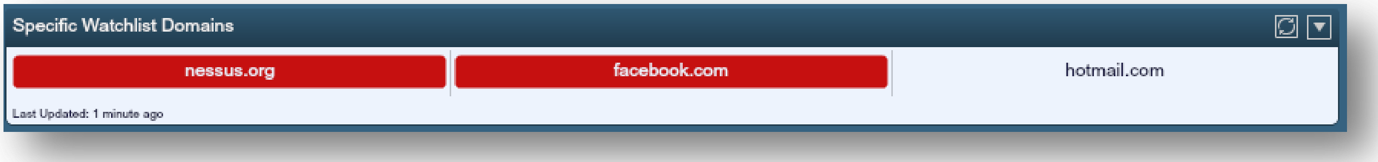


DNS Event Count Matrix

	Event Count
DNS Type Event	382568
Domain Summary	1081
DNS Client Query	325295
DNS Resolution Reporting	0
DNS Client Failed Query	55911
DNS Top Level Domain Queries	29
Bind IPv4 Query	0
Bind Zone Transfers	0

Last Updated: 12 minutes ago

The next section of the dashboard is “**Specific Watchlist Domains**”, which checks for DNS queries to specific domains in the last 24 hours. The DNS name shown in the dashboard will change to red when the DNS name is found and when the dashboard updates at the end of the 24 hour period. The normalized event type of “**PVS DNS Client Query**” is utilized for this part of the dashboard. The domains listed in this section can be changed if desired.

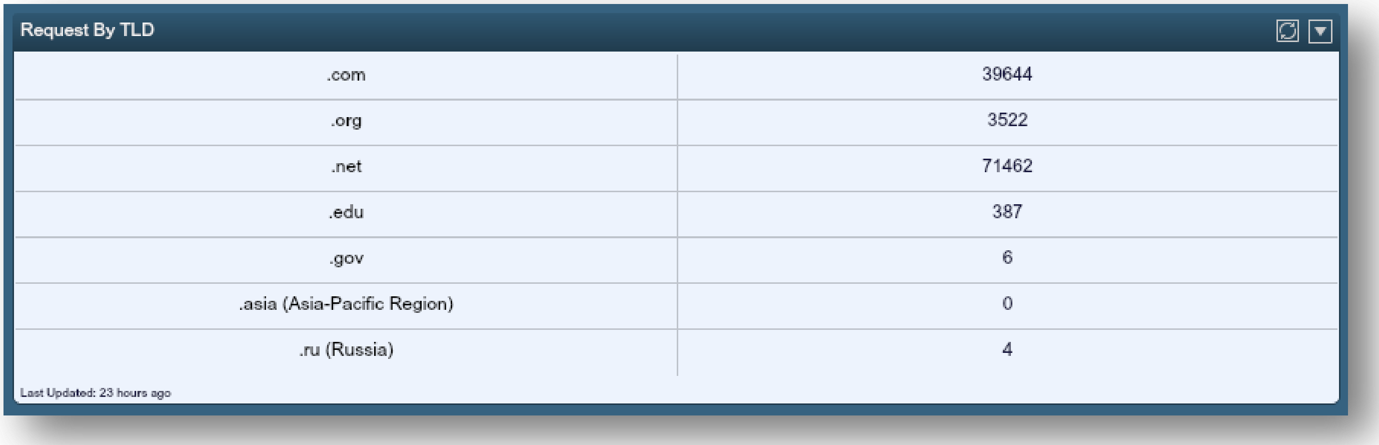


Specific Watchlist Domains

nessus.org	facebook.com	hotmail.com

Last Updated: 1 minute ago

Another component of this dashboard is “**Request by TLD**”, which again used the “**PVS DNS Client Query**” normalized event to show the amount of DNS requests made to each top level domain.

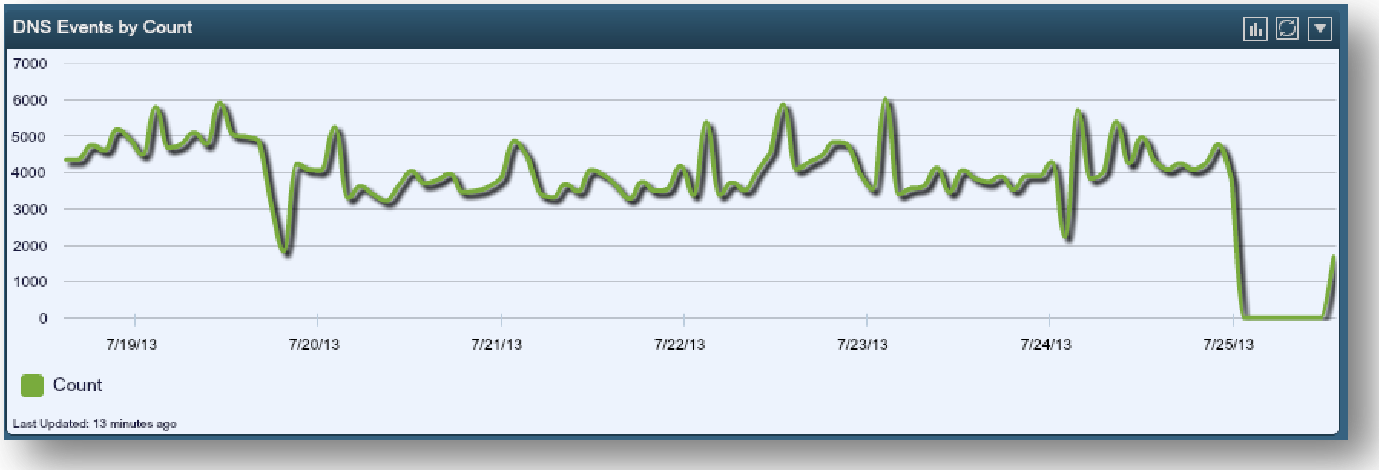


Request By TLD

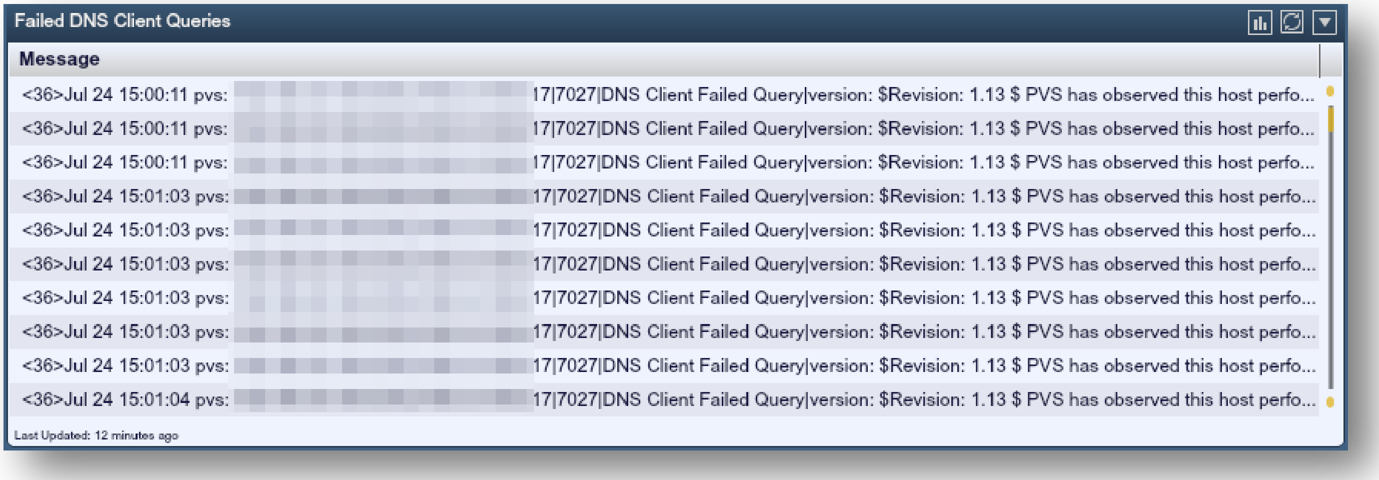
.com	39644
.org	3522
.net	71462
.edu	387
.gov	6
.asia (Asia-Pacific Region)	0
.ru (Russia)	4

Last Updated: 23 hours ago

The next section of the dashboard is “**DNS Events by Count**”, which tracks all DNS queries over a period of 7 days. This graph will show if there has been a dramatic increase in DNS queries on a given day, which may suggest botnet activity.



Finally, the “**Failed DNS Client Queries**” section of the dashboard utilizes the “**PVS DNS Client Failed Query**” normalized event type to display failed DNS client queries.



```
Message
<36>Jul 24 15:00:11 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:00:11 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:00:11 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:03 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:03 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:03 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:03 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:03 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:03 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
<36>Jul 24 15:01:04 pvs: [redacted] 17|7027|DNS Client Failed Query|version: $Revision: 1.13 $ PVS has observed this host perfo...
```

Conclusion

As noted in the introduction, each DNS server generates a set of logs that are normalized into the LCE event types of application, error, login/login-failure, and startup. The underlying operating system will also contribute its logs to the LCE event categories of error, login/login-failure, process, startup, and system.

There are many approaches to analyzing these events and monitoring them for their impact to compliance, security, and availability.

For More Information

Tenable has produced a variety of additional documents detailing the LCE’s deployment, configuration, user operation, and overall testing. These documents are listed here:

- Log Correlation Engine Architecture Guide – provides a high-level view of LCE architecture and supported platforms/environments.

- Log Correlation Engine Administrator and User Guide – describes installation, configuration, and operation of the LCE.

- Log Correlation Engine Quick Start Guide – provides basic instructions to quickly install and configure an LCE server. A more detailed description of configuration and management of an LCE server is provided in the “LCE Administration and User Guide” document.

- Log Correlation Engine Client Guide – how to configure, operate, and manage the various Linux, Unix, Windows, NetFlow, OPSEC, and other clients.

- LCE High Availability Large Scale Deployment Guide – details various configuration methods, architecture examples, and hardware specifications for performance and high availability of large scale deployments of Tenable's Log Correlation Engine (LCE).

- LCE Best Practices – Learn how to best leverage the Log Correlation Engine in your enterprise.

- Tenable Event Correlation – outlines various methods of event correlation provided by Tenable products and describes the type of information leveraged by the correlation, and how this can be used to monitor security and compliance on enterprise networks.

- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner.

- Log Correlation Engine Log Normalization Guide – explanation of the LCE’s log parsing syntax with extensive examples of log parsing and manipulating the LCE’s **.prm** libraries.

- TASL Reference Guide – explanation of the Tenable Application Scripting Language with extensive examples of a variety of correlation rules.

- Log Correlation Engine Statistics Daemon Guide – configuration, operation, and theory of the LCE’s statistic daemon used to discover behavioral anomalies.

- Log Correlation Engine Large Disk Array Install Guide – configuration, operation, and theory for using the LCE in large disk array environments.

- Example Custom LCE Log Parsing - Minecraft Server Logs – describes how to create a custom log parser using Minecraft as an example.

Documentation is also available for Nessus, the Passive Vulnerability Scanner, and SecurityCenter through the Tenable Support Portal located at https://support.tenable.com/.

There are also some relevant postings at Tenable’s blog located at http://blog.tenable.com/ and at the Tenable Discussion Forums located at https://discussions.nessus.org/community/lce.

For further information, please contact Tenable at support@tenable.com, sales@tenable.com, or visit our web site at http://www.tenable.com/.

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CSIS, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com