OAK RIDGE NATIONAL LABORATORY

SANSR

Situational Awareness of Network System Roles

Industry Challenge

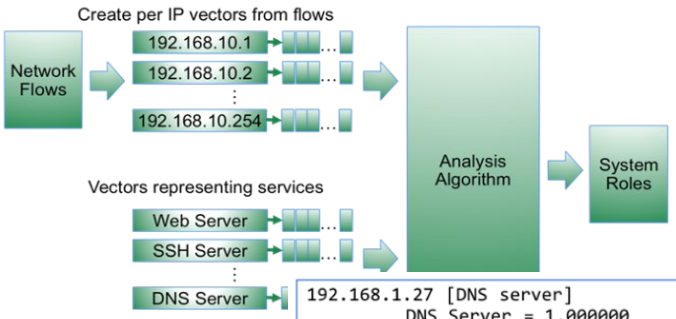
In large enterprises, security analysts struggle to identify what services and roles — file server, domain name server, email server, etc. — each machine on their network is performing. Not knowing what roles machines play makes it difficult to achieve situation awareness and to adequately diagnose or prioritize an attack.

Analysts could run a port scan on all of a networks machines, but this slow process only results in a yes or no answer as to whether a particular service is running at the time of the port scan and does not consider how much traffic a service consumed or generated.

ORNL Solution

ORNL's network flow analysis method, known as SANSR, will indicate a system's role based upon the amount of traffic it generates and consumes for well-known services. No network traffic need be generated, and it operates on data already collected in most enterprises.

SANSR queries for network flow data, creates a temporal behavior model of each system, uses machine learning to cluster the models with a set of labeled temporal behavior models, and outputs to the console or JSON-format the likelihood that a machine has a labeled role.




```
192.168.1.27 [DNS server]
          DNS_Server = 1.000000

192.168.20.20 [Server providing
HTTP,SSH,SMB services]
          Web_Server = 0.678460
          NETBIOS_Server = 0.001692
          SSH_Server = 0.000523
          NTP_Server = 0.000096
          DNS_Server = 0.000083
          NNTP_Server = 0.000083

192.168.10.101 [Server hosting www sites]
          Web_Server = 0.948978
          SSH_Server = 0.000127
          SMTP_Server = 0.000013
          FTP_Server = 0.000012
          DNS_Server = 0.000008
          NNTP_Server = 0.000008
```

The figure at right shows an example of the results output by SANSR. The square brackets next to the IPs are the known services that the machine provides. The list below each IP identifies the services SANSR found to be most similar to the machine's behavior and the similarity score associated with that service.

Benefits

The ORNL-developed SANSR tool provides cybersecurity analysts with quick, accurate situational awareness of the roles each machine on their network is performing. Among its benefits and features:

- No upfront training is required.
- Enterprise network IPs of interest can be modified as the network changes.
- Temporal behavior models can be adjusted for various timeframes, allowing analysts to monitor a system's role changes over time, which may indicate a cyber attack

CONTACT | Joel Reed | Research Staff Member | reedjw@ornl.gov

Oak Ridge National Laboratory is managed by UT-Battelle LLC for the US Department of Energy

2022-G00224

OAK RIDGE National Laboratory | U.S. DEPARTMENT OF ENERGY | Office of Science

NATIONAL SECURITY SCIENCES