SUNY POLYTECHNIC INSTITUTE

College Of Engineering, Department of Network & Computer Security (NCS), Utica, NY

Network and Computer Security(NCS)

Cyber-Security Framework for the University Campus Systems

Akshay S Bhoite and Diwash B Basnet

Advisor: Dr. Hisham A. Kholidy

ABSTRACT

University network incorporates a large number of different networking devices. Security of such a diverse networking recourse demands the effectively designed security framework for identifying vulnerabilities, threats, and risks associated with organizational assets and the controls that can mitigate these threats.

In this poster, we present developed Cybersecurity framework for the University Campus Systems. This framework conducted vulnerability assessment and analyzes security events and provide risk assessment.

1. We created the attack environment to test accuracy of this model by simulating the university campus systems using a small virtual network.
2. We performed vulnerability assessment using this model to detect currently existed vulnerabilities and their impact on the organization.
3. We developed the correlation model for risk assessment.

DEPLOYMENT MODEL

Collecting security events from all internal assets in the organization need properly deployed framework. This deployed model is very effective to detect existing vulnerabilities and threats. Installing this framework along with existing one, will enhance the security of the campus significantly.

Below we can see our deployed model using virtual machines. In that, we have installed server and sensor and deployed NIDS and HIDS agents. We covered 150.156.208.0/20 network.

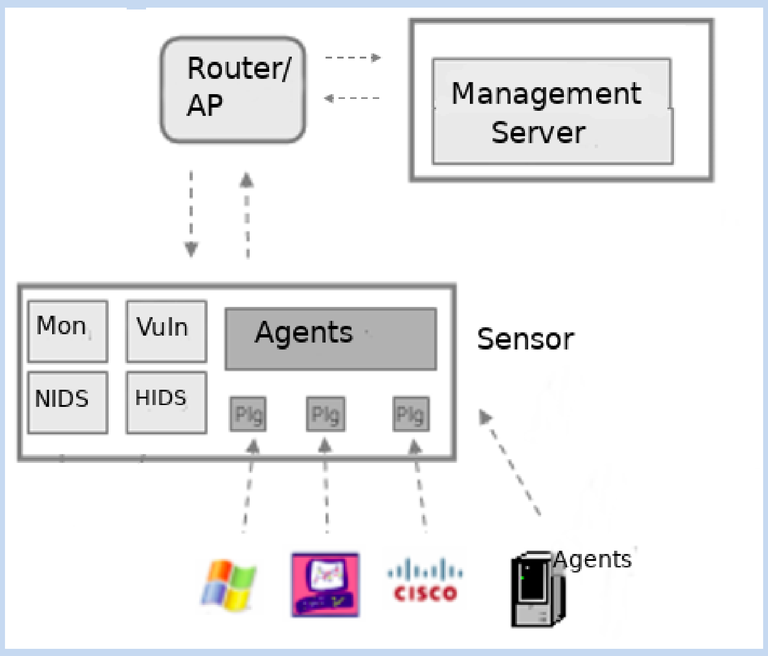

Fig.1

EXPERIMENTAL RESULTS

For evaluating the detection accuracy of our framework against the host and network, we developed an attack environment using the known host and network attacks in Meta-sploit. Which is installed in one of our Virtual Machine. We can see detected attacks here.

```
directive_event: AV-FREE-FEED Web attack, SQL injection attacks detecte
d against DST_IP, Priority: 3 Rule 1 [2018-04-16 20:48:45] [7060:31103]
[Rel: 6] 150.156.214.45:0 -> 0.0.0.0:0
```

```
AV - Alert - "1523850394" --> RID: "5716"; RL: "5"; R
G: "syslog,sshd,authentication_failed,"; RC: "SSHD au
thentication failed."; USER: "root";
SRCIP: "150.156.214.45"; HOSTNAME: "OSSIM"; LOCATION:
"/var/log/auth.log"; EVENT: "[INIT]Apr 15 23:46:33 OS
SIM sshd[102009]: Failed password for
root from 150.156.214.45 port 34123 ssh2[END]";
```

We can see top five security and multiple host events detected by the security framework. It also gives us report of security events trend daily as well as weekly.

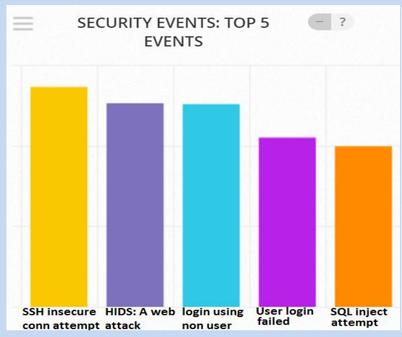

Fig.3

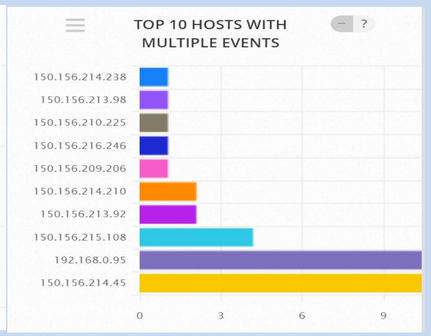

Fig.4

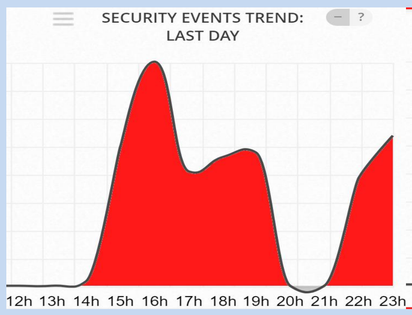

Fig.5

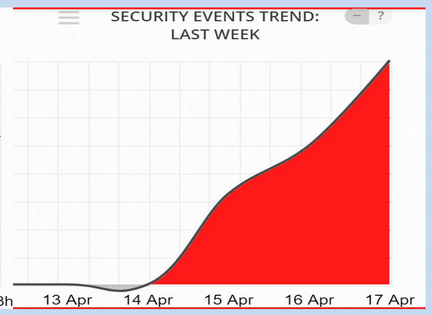

Fig.6

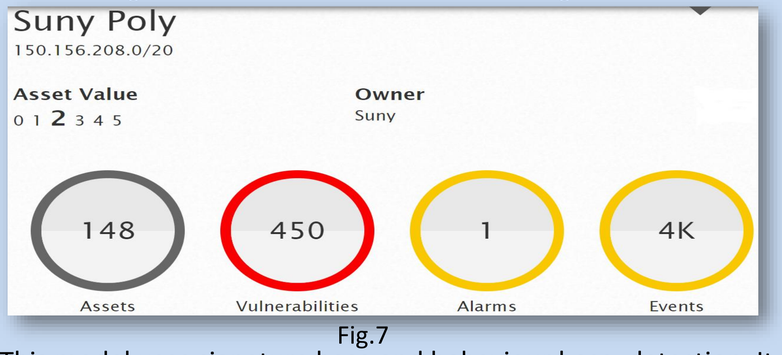

Fig.7

This model uses signature base and behaviour base detection. It used security information and event management (**SIEM**) service which includes security information management (SIM) and security event management (SEM).

VULNERABILITY ASSESSMENT

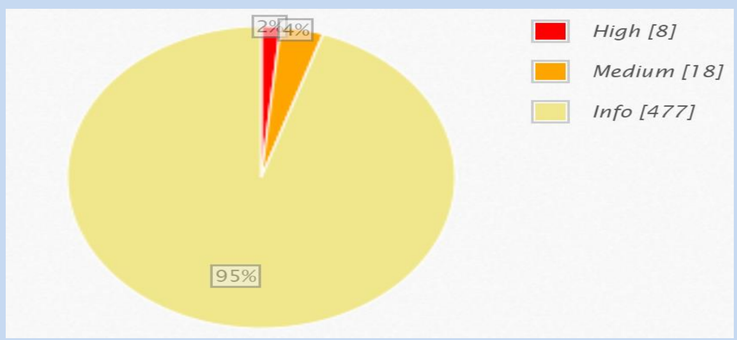

Fig.11

1)Malformed ICMP Packets May Cause a Denial of Service (SCTP) -This flaw is present if SCTP support is enabled on the remote host. Linux Kernels older than version contains a bug which may allow an attacker to cause a NULL pointer deference by sending malformed ICMP packets, thus resulting in a kernel panic. An attacker to make this host crash continuously, thus preventing legitimate users from using it. Upgrading the OS and disabling SCTP may prevent this attack [5]. The estimated average cost to recover from this is **$10000**

2)Mongoose Web Server Remote Buffer Overflow Vulnerability - exploitation will allow remote hackers to execute malicious code to the affect application. Failed exploit attempts as well cause a denial-of-service.

3)'SPANK' - when the machine received a TCP packet coming from a multi cast address cause denial of service. An attacker might use this condition to shut down this server and crash your network. So, this preventing you from working properly. **$2000** for data recovery

4) Bad-Blue invalid GET Dos - exploiting a known vulnerability to crash resources on Bad-Blue Web server. Attackers send a crafted HTTP GET request to the Bad-blue Web server to crash it. An attacker may exploit this vulnerability to make the web server crash continuosly. Cost to recover is about **$1000 to $2000.**

CONCLUSION

In this poster, we presented our security framework. It is a effective model for analyzing CyberSecurity status of the university campus. Sensors deployment increase Its scalable for full deployment architecture. It is a flexible model because we can define our own policy and own risk assessment model. Real time event collection allow us to analyze vulnerabilities, threats and risks in the network. When an attack occurs, it calculates the risk. if the risk is higher than one i.e. threshold value, it fires the alarm . It detects SQL, DoS, DDoS and other network and host based attacks with a high accuracy.

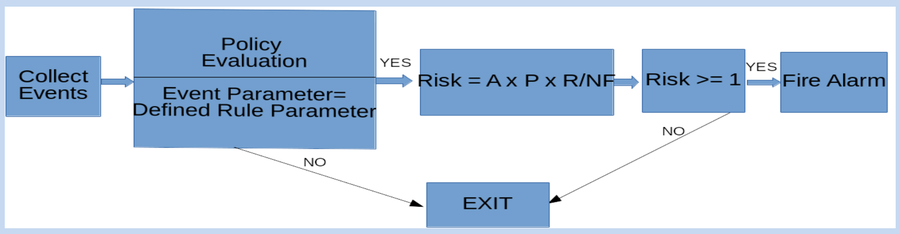

Fig.8

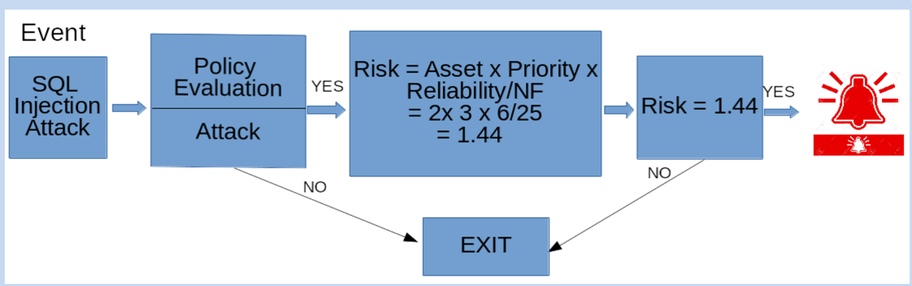

Fig.9

RISK ASSESSMENT

Here, Asset (0-A), i.e. value of the asset. Priority (0-P), i.e. The alert severity level. Reliability (0-R), i.e. the probability that the attack is real. NF is a normalized factor.

RISK= (Asset Value*Alert Priority*Detection Reliability)/NF

Fig 10

REFERENCES

1. Adrian Munteanu, 'Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma', Managing Information in the Digital Economy: Issues & Solutions.
2. Luis Miguel Ferreira, 'A multi-level model for risk assessment in SIEM', Department of Informatics, Faculty of Sciences, University of Lisbon.
3. 'Correlation Reference Guide' by AlienVault Unified Security Management™ for Government v4.12 & RT Logic CyberC4:Alert v4.12.
4. AlienVault LC. AlienVault Open Source Security Information and Event Management.
5. https://www.acunetix.com/vulnerabilities/network/vulnerability/malformed-icmp-packets-may-cause-a-denial-of-service-sctp/