Oğuz Yarımtepe

Sr. System Engineer

oguzyarimtepe@gmail.com

+90530773162

about.me/oguzy

linkedin.com/in/oguzyarimtepe

github.com/oguzy

twitter.com/oguzy

EDUCATION

PhD in Computer Science
Dokuz Eylul University
2010 - 2020

MSc in Computer Science
Izmir Institute of Technology
2007 - 2009

BSc in Computer Scienc
Canakkale Onsekiz Mart University
2003 - 2007

LANGUAGES

Turkish (Native)

Engilish (Professional)

Spanish (Beginner)

INTERESTS

Aikido

Aquarium

Photography

PERSONAL SUMMARY

I am a Linux system administrator and software developer who is a fan of Linux and open source. Till now, i worked on Linux server systems, software development under Linux, web development and embedded software development. Some more are related with GSoC and mentioned below. I am also a Ph.D student. My research subject was network anomaly detection though security visualization. I had tried to detect network anomalies in an interactive way using visualization techniques and in real-time. After i changed my topic, now i am working on DDoS mitigation.

WORK EXPERIENCE

Senior Site Reliability Engineer

2018 - 2020

GittiGidiyor/EBay, Istanbul/Turkey

Migrating the applications to Kubernetes infrastructure, monitoring & alerting of both Kubernetes clusters and apps, installing and maintaining the clusters, handling deployment issues of apps on K8S, daily system administrator issues, architectural roles on system design and solving system side problems with new technologies, applying solutions to succeed infrastructure as code principle (Ansible, Tower for now), creating Docker images for Kubernetes deployments and handling some DevOps issues

Senior System Engineer

2016 - 2018

GittiGidiyor/Ebay, Istanbul/Turkey

I have three roles. One is site operations that covers linux system administration jobs. We have Centos & Red Hat machines running native/docker java and php apps. Maintaining them, handlind daily release cycle load problems or any othere server related problem is one of my duties. Another one it the orchestration part. I am automating our processes. Using Ansible, Python and Django. Writing UIs and playbooks that are automating our VM lifecycles. And other issue is the improvement issues like migrating to Kubernetes environment, testing and finding solution to our disaster site, creating lightweight Docker images and converting our system apps to Docker. Currently leading the Kubernetes migration project and taking application to production on Kubernetes clusters, with monitoring and logging solutions.

R&D Architect

2013 - 2016

Turksat Uydu Haberlesme Kablo TV ve Isletme AS, Izmir/Turkey

I had worked on auto-deployment of Openstack on bare metal servers. Used Mirantis, Crowbar and Rackspace cookbooks. Also fixed and developed Crowbar source to fullfill our requirements on Ubuntu. Worked on Openstack monitoring. Used logstash, riemann, collectd and graphite for alarming and monitoring. Also tried sensuapp & consul. Wrote an agent with Python that collects metrics and sends it to Influxdb. Also, dealed with Openstack APIs and wrote a middleware for handling requests to Openstack APIs from different sources using Kong and Falcon. So, it was a Rest API that is supporting different authentication methods, rate limiting and IP restrictions. I have been working on implementing a custom hardware appliance to Openstack as a FWaaS, so wrote a driver for Neutron. Also, dealed with the object storage part of Openstack and Ceph. Worken on Intel VSM UI to automate Ceph installation and orchestration. Also, working on Keystone and LDAP integration to handle a domain specific logins, using FreeIPA for now.

System Administrator

2011 - 2013

Canakkale Onsekiz Mart University IT Department, Canakkale/Turkey

Linux server administration: This includes installation and maintenance of all Linux server supplying services to the university campus. We have DNS, DHCP servers serving for internal machines. Also web servers for department and faculty sites, personal homepages and academic staff including their databases. Many of them are configured with PHP-FPM + FastCgi support with Apache2 running. Over ~200 site is hosted and increasing. We have Freeradius and LDAP serving for 802.1x authentication serving to ~40000 students. For some departments, it is served Drupal accounts which is configured with multi site installation. System Programming and Software Development: This includes writing required software for daily server maintenance like web interface to create user accounts on LDAP for wireless access applications. Or creating a central log server to collect vital logs. Security: Servers are watched with Nagios. They are generally Debian based installations. Security updates are applied. I am also observing some installed Honeypots to collect attack information. Attacked IPs are blocked either from firewall policies or or switch configuration. I am not at the switch configuration part. Virtualization: Many servers are hosted on Xen Citrix Server. Some special needed servers are also created day by day, like Moddle. Basical Citrix interface is used to create virtual hosts, backing up and cloning. External Support: It is sometimes given professional support to departments or library. Under this concept, terminal server is installed and configured for thin clients. For general usage a print server system with a web interface and GUI is designed and written with a quota usage.

Software Engineer

2009 - 2011

Near East Universtiy Innovation adn Information Technologies Center, Lefkosa/KKTC

Gave the required software support to fulfill the university Linux migration. Changed the existing softwares or rewrote the equivalent ones for transferring them to be run as a platform independent way. Designed and developed a package manager for the university specific Linux distribution.

Software Engineer - Project Manager

2008 - 2009
VESTEL Electronics, Izmir/Turkey

Developed a library that will be run on DVBs as an embedded way and which will enable animated menus. A prototype that was using EFL libraries was designed and run on STLinux distribution. To secure the update tool of the IP TV project public key encryption support was added to the software. C language with gpgme libraries was used.

Software Design Engineer

2008 - 2008
VESTEL Digital A.S., Izmir/Turkey

Under the scope of netbook project, solved the problems of the netbook that was running Ubuntu Netbook Remix, wrote netbook spesific softwares, adapted test processes, fixed bugs. Used Python and PyQT usually and created deb packages for the distribution.

VOLUNTEER WORK

Planet Site Maintener

2008 - 2010
Turkish Linux Users Group

I maintain the site http://gezegen.linux.org.tr and give seminars related with Linux and free software

AWARDS

Network Analyzer Project Mentor

2013
Google

Network Analyzer is a Google Summer of Code 2013 project proposed by me. It is an enhancement of my previous project that is ovizart (https://github.com/oguzy/ovizart).The aim is to create a network analyzer that will analyze raw traffic data. The tool will have both a CLI and a web interface. By making TCP reassembly human readable info will be extracted from the traffic and the binary data will be analyzed for malwarez. Dynamic protocol detection, cuckoo sandbox integration, JS analzyer and online traffic analysis are the planned features. Honeynet Project Site: http://honeynet.org/gsoc2013/ideas#project7 Slot page for students: http://honeynet.org/gsoc/slot6 http://honeynet.org/gsoc/slot7 Github Repo: https://github.com/honeynet/ovizart-ng

Google Summer of Code 2012

2012
Google

Web based packet analyzer that will aim an automated analyzer for the uploaded pcap files. The aim will be the open alternative for http://netwitness.com/products-services/investigator. The first fulfillments will include visualization of the analyzed traffic, application level information display and the plugin support for the malware and anomalies. Here is the project page for details:http://www.honeynet.org/gsoc2012/slot13

Google Summer of Code 2011

2011
Google

I am accepted to GSoC 2011 for the Honeynet project #4:http://www.honeynet.org/gsoc2011/ideas#project4. Below is the abstract of my proposal: My aim will be to develop a web based visualization that will have 3D mesh structure with heatmap tiles. The visualization will have time based changes so that according to time-series event it will be possible to see the malware distribution/attack geographic distribution. The finished project details can be reviewed from http://www.honeynet.org/gsoc2011/slot4

PROJECTS

Crowbar - This is a bunch of cookbooks written with Chef to install Openstack from a web ui. I sent some fixes for Ubuntu installation. The cookbooks were designed for Suse environment. During testing and using them for Openstack installation, i had to made changes for Ubuntu systems.

VSM - Virtual Storage Manage - Virtual Storage Manager (VSM) is software that Intel has developed to help manage Ceph clusters. VSM simplifies the creation and day-to-day management of Ceph cluster for cloud and datacenter storage administrators. This is a project that i contributed to. I made some fixes for installation errors on Ubuntu.

SEFIR (Secure File Burning On a Remote Machine) - A project that i developed using Python and PyGTK during my summer training at 2005 in Information System Head Office. Details are

PySONDA - A console based application that uses SNMP to communicate and gather information(mainly read the ARP table and log the changes) about the active devices in the network. Written with Python

VENGA (Very Native Galaxy Atmosphere) - VENGA is also my final project that i choosed at my university. There is not a web site for the project yet. Shortly, it is a web site that reads the XML feed (blog entries) and decides the category of the entry by Bayesian Classify and shows it under some category. So a planet that enables the people read entries by cetagories. I used Python as a core language. Used feedparser to parse feeds and Zemberek to parse words according to the Turkish language rules. And i used Django to develop the web interface and database part.

PUBLICATIONS

IPv6 and A General Summary for Security Visualizations

2011
IPv6 Conference in Ankara

Since the Ipv6 supported networks and services is increasing, related security risks started to be argued. Although it is announced as a secure communication protocol with its vast amount of addressing space and IPSec structure, IPv6 is placed in Blachat hackers world with its open security risks. It is well known that using IPv6 does not supply full security. DoS, rogue device defining attacks, application level attacks and social attacks are already known threats for IPv6 networks. Intrusion detection/prevention systems and firewalls are used to protect from possible or current threats. It is required for network analysts to analyze traffic to detect attacks. Generally text based tools are used for such analysis and they should be commented to get a meaning from the analysis. Visualization is helping analysts to see the whole picture and getting information from analysis. This article is summarizing the different security visualizations. Visualization approach is explained via the security perspective and its usage at IPv6 world

A Flow-Based Network Traffic Characterization Tool

2010
ISTSEC

Traffic characterization has a crucial role on network security. As long as the attackers disguise their attacks through well-known services, port-based service recognition or payload-based analysis approaches cannot generate trustworthy characterization results. On the other hand, summary information about the network traffic is more reliable than port number and to obtain this kind of information require less effort than payload-based analysis. This paper presents and implementation of a flow-based network traffic characterization tool. This tool has the capability of reading off-line traffic data and recognize traffic with similarity percent.

Firewall Configuration Management Using XACML Policies

2008
13TH INTERNATİONAL TELECOMMUNİCATİONS NETWORK STRATEGY AND PLANNİNG SYMPOSIUM

This paper proposes an architecture for XACML based management of firewall configurations in large enterprise networks. The goal of this architecture is to allow administrators and end-users to manage their firewalls, while enforcement of organizational policy is ensured to prevent unacceptable traffic gaining access to the private network domain. The central architectural component is the domain policy server which pushes organizational policy down to firewalls deployed in its domain. In addition to its reporting function, the domain policy server monitors and verifies policy changes, i.e. checks for inter- and intra-firewall anomalies, on any firewall within its domain. The proposed architecture includes firewall agent components, where one resides on each firewall, through which coordinated operations on firewall policies are achievable. Firewall policies, topologies, and configuration messages that are stored and exchanged within the architecture are presented in XML. Although available XACML is used for the representation of firewall policies, two DTDs are developed to express topologies and configuration messages. A prototype implementation of this architecture is presented in this paper along with examples of firewall configuration management operations.