Computer Science for High School

(CS4HS) Cybersecurity Virtual Workshop

Google CS[4]HS

Network and Server Security: What's a day at Work?

Presented by

Maria C. Garrity

Senior Systems Administrator

Information Technology

Google CS[4]HS

Network and Systems Administrator

- I am a Senior Systems Administrator specializing in Network and Server security because at Buffalo State security is extremely important for the protection and privacy of faculty, staff and student data.

- My job has many layers to it. I work on maintaining the cybersecurity of over 50 departmental virtual servers using VMware Technology and I work on supervising the installation of software packages on each departmental server as well. Additionally, I facilitate the coordination of special projects. The most recent project is the campus COVID screening & contact tracing system that will be in place for the beginning of the semester .

Duties

My specific network and server related duties include:

1. View system logs and identify potential issues with IT systems.
2. To apply operating system updates, patches, and configuration changes.
3. To apply firewall and antivirus exceptions
4. To install and configure new hardware and software.
5. Make backups or virtual snapshots prior to any application updates, security installs or patches.

Google CS[4]HS

Software

Some Departmental server software includes:

- **Accufund accounting system** for accounts payable and receivables
- **Student medical and immunization system** called medicat for telehealth and mobile health system for touchless student check-ins. Medicat, going forward will include COVID screening app
- **Counseling Center** – teletherapy scheduling system
- **Burchfield Penney Art Center** point of sales CounterPoint system for the café and general store
- **Visix digital signage software** that integrates with our alerting system upon campus issues

Google CS[4]HS

Levels of Security

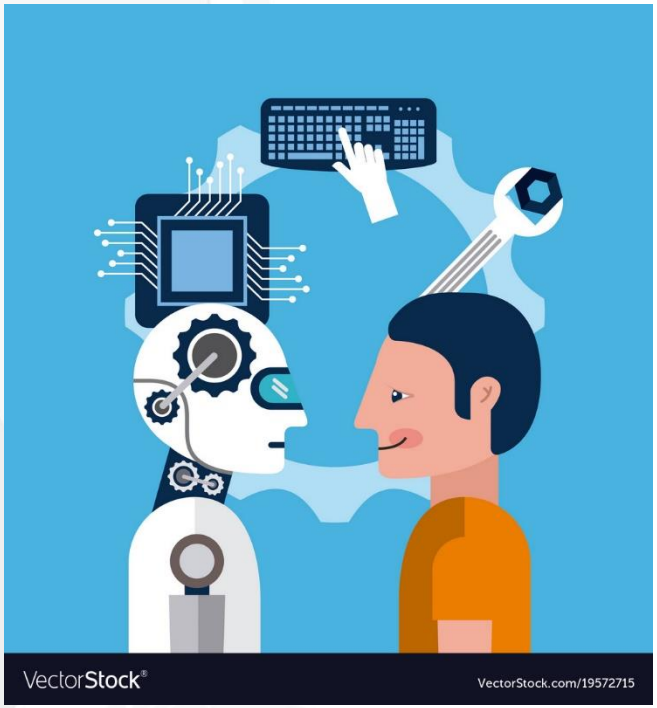
Levels of security

- **Network level** - we have in place to safeguard around the perimeter of our network
- **VM Host level** - make sure our virtual hosts that houses our servers are secure
- **Server level** - make sure the OS is fully patched with firewall and antivirus enabled
- **Client level** - make sure the Windows client OS is fully patched with firewall and antivirus enabled
- **Database Security** – protecting and encrypting important data.
- **Application level on the servers** - make sure the updates are installed from the vendors of the products including Outlook email
- **Application level on the clients** - make sure updates are installed including Microsoft Office suite.

Google CS[4]HS

Cylance Smart Antivirus Protection Technology

- **Cylance –** uses artificial intelligence (AI) based solutions that predict and prevent execution of advanced threats and malware at the endpoint.
- It provides a solution that is proven able to block emerging threats on average 25 months before they are first detected.
- Cylance uses AI approach – predicting and protecting against known and unknown malware and attacks.



https://www.cylance.com/en-us/why-cylance.html

Google CS[4]HS

Fun Activities

Fun activities: Go to **Start** and type **cmd** in the search field to open the command prompt. Or go to *Start > Run type cmd or command – right click and run as administrator*

netstat - The network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices

- Example: **netstat -a** command would give the extended result of ports opened on the server and established connections and their current state for both TCP and UDP connections.
- **netstat -an** command would only show the remote server IP addresses where netstat -a would try to resolve the name for that IP address. Thus netstat -an would be faster than the netstat -a

Google CS[4]HS

More fun activities

Fun activities:

- nslookup - used for querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records. The name "nslookup" means "name server lookup".
- Example: nslookup google.com
- nslookup (your device name.com)

Google CS[4]HS

Even more fun activities

Fun activities:

- Ping- command used to troubleshoot connectivity, reachability, and name resolution.
- Example: ping google.com
- Ping (your device name)
- Ipconfig - Displays all current TCP/IPnetwork configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings
- Example: ipconfig or ipconfig/all

Google CS[4]HS

Questions/ Comments

THANK YOU!

Contact Information

Maria C. Garrity - twitter: @hejnamc

hejnamc@buffalostate.edu

https://it.buffalostate.edu

https://cs4hs.buffalostate.edu/