## **Tech Research:**

Cloud computing

SaaS models

Bgp border gateway protocol

Arp cache poisoning

TCPs three way handshake: syn synack ack

Electronic frontier foundation (EFF)

setup ipv6 after flashing router

what is windows sharepoint

[Bingit.io](http://Bingit.io/) search engine

502 - Web server received an invalid response while acting as a gateway or proxy server.

There is a problem with the page you are looking for, and it cannot be displayed. When the Web server (while acting as a gateway or proxy) contacted the upstream content server, it received an invalid response from the content server.

AP Computer Science Principles (exam by the college board)

Archive.org

Vx heaven

Asic

>Install custom firmware on your router(not modem) that can spoof MAC addresses. Very simple n00b technique to get a new IP address. Tomato is an older but very functional custom FW.

Download old viruses into a VM and see what they do

<https://marsconference.com/>

<https://en.wikipedia.org/wiki/Extended_Display_Identification_Data>

***Wolfram:***

<https://www.wolfram.com/>

<https://www.wolfram.com/technologies/>

<https://www.wolfram.com/language/>

<https://writings.stephenwolfram.com/category/computational-thinking/>

<https://writings.stephenwolfram.com/2012/03/the-personal-analytics-of-my-life/>

<https://www.christopherwolfram.com/>

<https://writings.stephenwolfram.com/2016/04/my-life-in-technology-as-told-at-the-computer-history-museum/>

A new kind of science book: <https://www.wolframscience.com/nks/>

<https://www.stephenwolfram.com/publications/>

<https://www.wolframalpha.com/>

https://resources.wolframcloud.com/FunctionRepository

https://demonstrations.wolfram.com/

Open source alternative to discord

Proprietary Driver binaries

<https://developers.google.com/android/drivers>

Open source android OS:

<https://replicant.us/>

<https://replicant.us/supported-devices.php>

<https://microg.org/>

<https://lineage.microg.org/>

a cookie is a small file that a website stores on your computer

tracking pixel stores information on your web server, a 1x1 transparent image that tracks how a user reacts to your web pages

Mastodon social media

Degoogling your phone will require buying an old android phone that’s supported

You can’t use email, or youtube on your phone if you degoogle your phone

You can’t play music unless it’s locally downloaded

If a tech service is free, you’re the product.

<https://www.reddit.com/r/degoogle/>

Silicone carbide

Modchip center .com

Tableau reporting

What is AS/400 Used For? AS/400 architecture is often used for ERP and other mission-critical tasks, particularly in industries that require extreme reliability, such as manufacturing. IBM Power Systems are popular with SAP users, as well as competing database management systems, such as Oracle Database.

<https://en.m.wikipedia.org/wiki/IBM_i>

IBM Power Systems

Windows/SQL

Linux/Oracle

Processor-dependent and processor-independent code

Flat virtual memory called single-level store

Hardware abstraction

Machine interface code (MI) or Microcode

Technology independent machine interface (TIMI)

System licensed internal code (SLIC) / kernel

Kornshell, bourne shell, C shell

Binary code compatibility

Source code compatibility

Research different forms of input and an input method that is superior to the keyboard

Inductive charging

**Growing Instagram (**quotesconnoisseur**):** Take the ideas you've jotted down, and plug them into Instagram's search bar as hashtags. From there, you'll see which ones are most popular on Instagram--prioritize them accordingly. Grow your list of hashtags through “Related Items”

Software performance testing

Find when poking a website or server starts becoming suspicious

What is DOS?

What are pipe commands?:

allows you to pass the output of one cmdlet to the input of another cmdlet

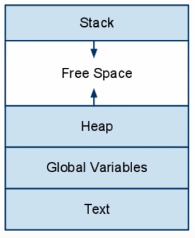
Memory protection: Abstraction and arbitration

OS must ensure that a process cannot access memory that does not belong to it

Segmentation

valid/invalid pages

**Memory Stack:**



<https://www.howtogeek.com/163127/how-powershell-differs-from-the-windows-command-prompt/>

<https://www.howtogeek.com/126265/how-to-troubleshoot-internet-connection-problems/>

<https://www.howtogeek.com/111859/how-to-batch-rename-files-in-windows-4-ways-to-rename-multiple-files/>

<https://www.howtogeek.com/138121/geek-school-learning-powershell-objects/>

<https://www.howtogeek.com/114344/5-cmdlets-to-get-you-started-with-powershell/>

<https://www.howtogeek.com/138121/geek-school-learning-powershell-objects/>

What is the system registry?  
What are cmdlets in powershell?  
WMI (Windows Management Instrumentation)

What is a DOS system?

write a script to automate various system administration tasks with powershell

PXE boot needs a boot server

Software configuration management systems: perforce, concurrent version system, Microsoft visual source safe, ibm rational

Windows Preinstallation environment (WinPE)

Windows assessment and deployment kit (ADK)

ZAP: Zscaler application profiler

Mobile phone logs:

Apple: xcode

Android: logcat

2019 study from blancco and ontrack - Storage devices

DBAN darik's boot and nuke

Routerpasswords.com

Girdles theorem

Lambda calculus

Computational representations

Kioptrix

Windows came from MSDOS

Hackthebox.eu

Enumeration is the most important pentesting skill

Nikto

Burp suite

Shell commands?:

* Grep
* Awk

What does curl do?

The difference between redteaming and pentesting

OSINT

TheHarvester

Bluto (using this will get you noticed on the network you target)

Crt.sh

Fingerprinting:

Wappalyzer

Whatweb

Explain the three way handshake

NMAP scan:

Nmap -T4 -p- <ip address>

Kioptrix

Steal handshake / stealth scanning

Nmap scanning

Nessus home

Cybrary

Packet squirrel

SoC

ESN (similar to IMEI)

Phiber optik and acid freak

Machine learning

High temp and low temp searches

Certs:

eWPT, OSCP, OSWP, CEH, CCNA, Pentest+,

Token impersonation

Linux:

/etc/passwd

/etc/shadow

Sudoers file

Auth.log

systemctl

How to MiTM somebody:

Volunteer to be an exit node

ARP cache poisoning

Become an access point

room 641a

The nsa installing backdoors in to encryption algorithms

Symmetric encryption

Symmetric authentication

Private (public key) encryption

Private (public key) authentication

Heartbleed 2014 attack

302 redirect

Ssl strip

HSTS

3d Printing

Research the digital nomad lifestyle

Cloudflare: hosting without censorship

How do email servers actually work?

<https://packetlife.net/blog/>

Research the history of IT

Ethan Zuckerman

What is ISDN PRI?: Primary Rate Interface

In the US we have a T1

* 24 channels: 23 voice (beta) channels and 1 delta channel

Internationally we have a E1

* 31 channels: 30 voice (beta) channels and 1 delta channel

Delta channels are used to set up at take down calls, and deliver name and number information

Advantages of PRI: reduced cost. Provides a circuit chart, multiple phone lines on one PRI circuit

ISDN is a digital version of traditional analog PSTN. PSTN was designed for analog phone calls

With digital data transmission, voice data remained the same. For computers, modems were developed to allow digital exchanges over existing analog PSTN networks. Digital signals are modulated to analog signals and transmitted over the PSTN network, then remodeulated when they arrive.

Analog signal disadvantages compared to digital signals:

1. Over the long distance, analog signals cannot maintain high quality
2. Analog signals carry less information per second than digital signals
3. Analog signals are not so flexible as digital signals in terms of data rate service and support

This is why ISDN was created. ISDN is a set of international communication standards designed in the 1980s and improved in the 1990s. It is a digital network to transmit voice, image, video and text over the existing circuit-switched PSTN telephone network

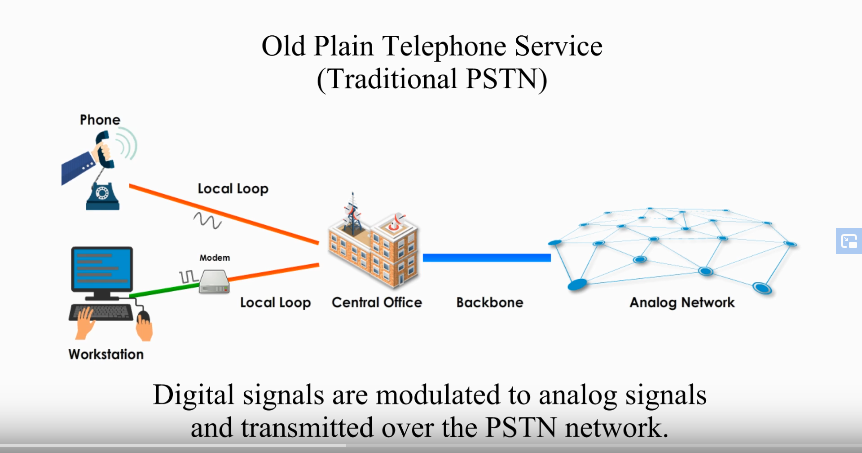
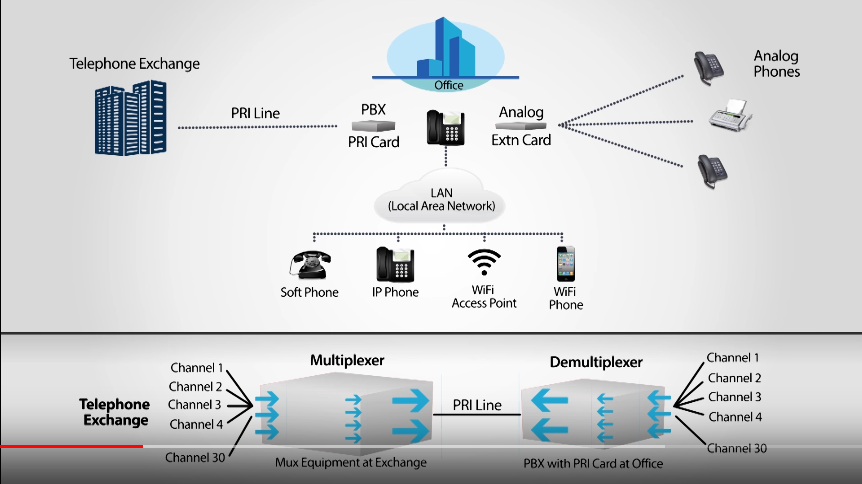
Two ISD options: Basic Rate Interface (BRI) and Primary Rate Interface (PRI)

DID (Direct Inward Dialing): individual phone line assigned to a particular user

DOD (Direct Outward Dialing): used for a call center

Call hunting. Asequential, desequantial

The PRI card is inside the PBX



Or at least he might gain a tool to monitor the number and location of infected machines, a move that malware analysts call “sinkholing.”