Cyber Defense Organization

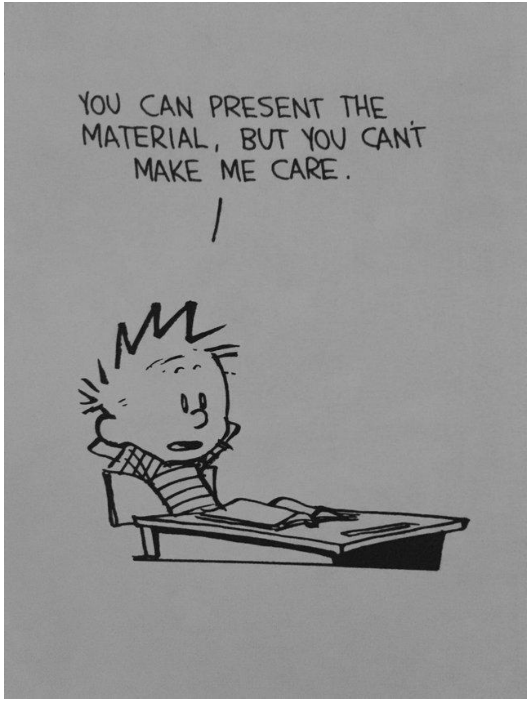
Fall 2018 - Intro to InfoSec

Purpose of today

Introduce the basics of Information Security

Semi-Accurate Agenda

- Frameworks
- Identity and Access Management (IAM)
- Authentication
- Authorization
- Accounting
- Introduction to some networking terms
- Physical Security
- Network Security
- Application Security
- Technology and Cyber Security Trends
- CCDC - Competitions
- Questions



Disclaimer

We are students...so yeah.

Fact check us all you want! =)

Why are we doing this?

In order to understand the technical side of all Cyber Security aspects. It’s best to get an idea of the conceptual side of things.

Information Security is massive area one that is constantly changing everyday as new technology is released.

Throughout this semester we intend to slowly introduce you to new topics via lectures and workshops, so that you can become passionate about this field and strive to learn more each day.

Key Definition

Information Security - Information security, sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical.

Security Provision	Information Assurance Compliance	Software Engineering	Enterprise Architecture	Technology Demonstration	Systems Requirements Planning	Test and Evaluation	Systems Development			
Operate & Maintain	Data Administration	System Security Analysis	Knowledge Management	Customer & Technical Support	Network Services	System Administration	Systems Security Analysis	Radio Frequency Teleport	Telephony / Telecoms Management	Space Payload Operation
Protect & Defend	Computer Network Defense (CND) Analysis	Incident Response	CND Infrastructure Support	Security Program Management	Vulnerability Assessment & Management					
Analyze	Threat Analysis	Exploitation Analysis	All Source Intelligence	Targets						
Collect and Operate	Collection Operations	Cyber Operations Planning	Cyber Operations							
Oversee and Govern	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training	Cyberspace Program/ Project Manager	Cyberspace Supervision, Management, and Leadership					
Investigate	Investigation	Digital Forensics								

NICE Framework Workforce Categories

Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Frameworks

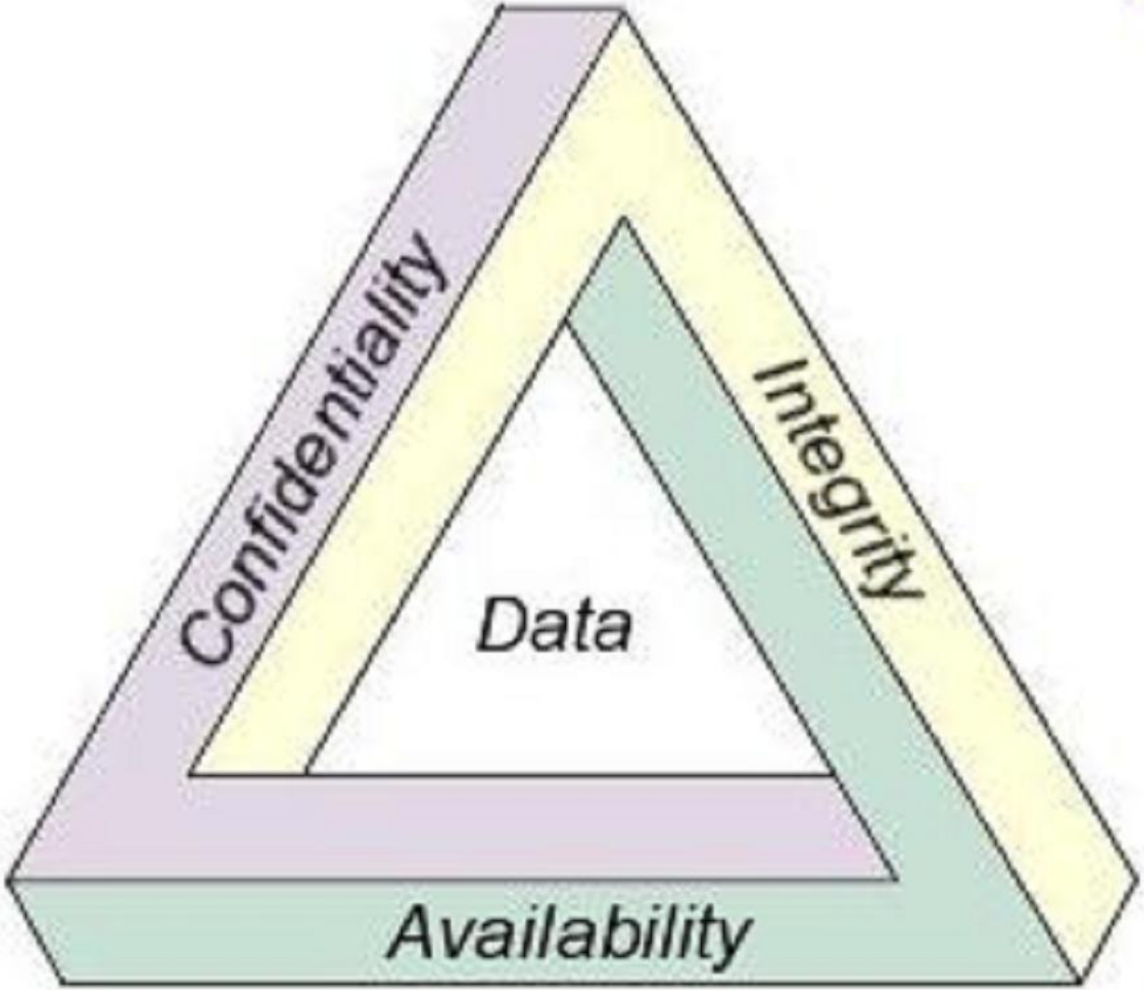
Frameworks allow us to comprehend the massive amount of technology, identify weakness, assess risk, and track progress over time.

NIST Cybersecurity Framework (800-53): Identify, Protect, Detect, Respond, Recover.

ISO 27001 - 14 control categories.

COBIT - Divides enterprise IT into four domains.

Many more, SABSA, TOGAF, ITIL


Confidentiality
Integrity
Data
Availability

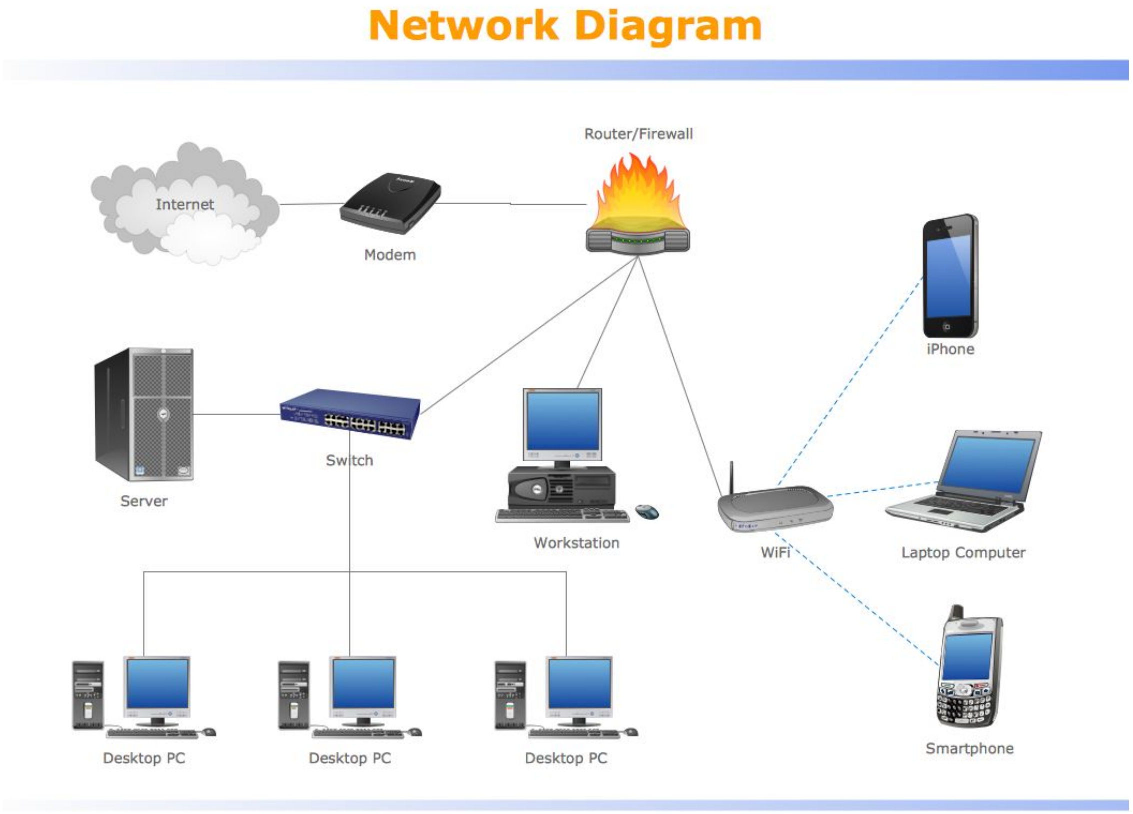
So, what does a network look like?

Users

Endpoints

Servers

Networking Equipment



Slight Tangent

Identity and Access Management

Three Parts

Authentication is the process of verifying who you are.

Authorization is the process of verifying that you have access to something.

Accounting is the process of auditing usage post authorization.

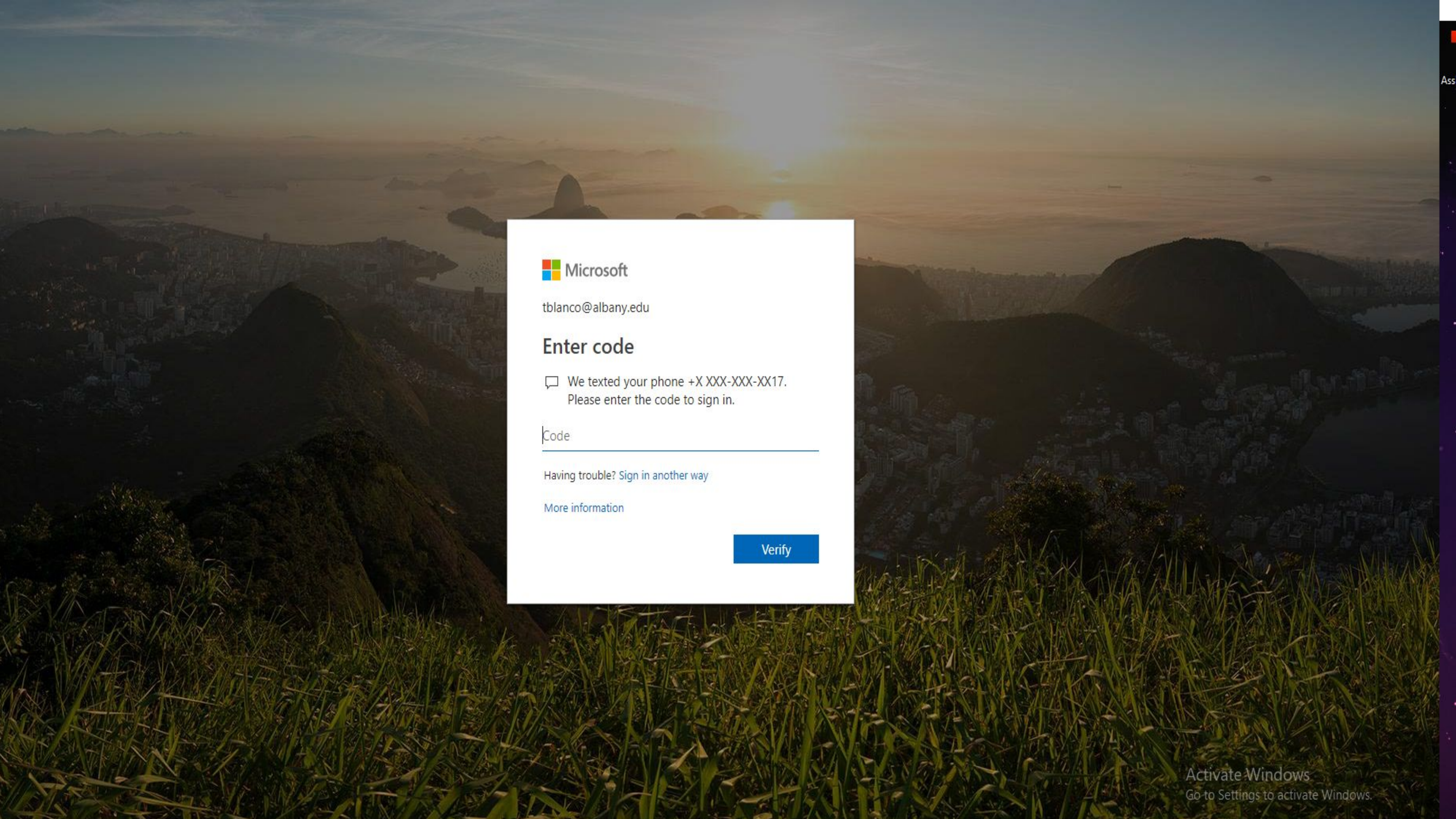
Authentication

Three factors:

- Something you **know**.
- Something you **have**.
- Something you **are**.

Something you know

Something you have



Microsoft

tblanco@albany.edu

Enter code

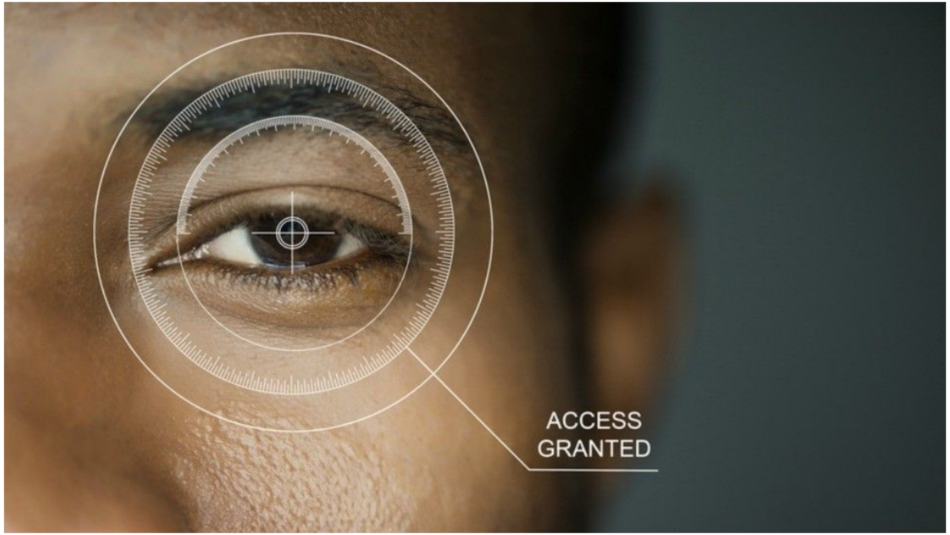
We texted your phone +X XXX-XXX-XX17. Please enter the code to sign in.

Code

Having trouble? Sign in another way

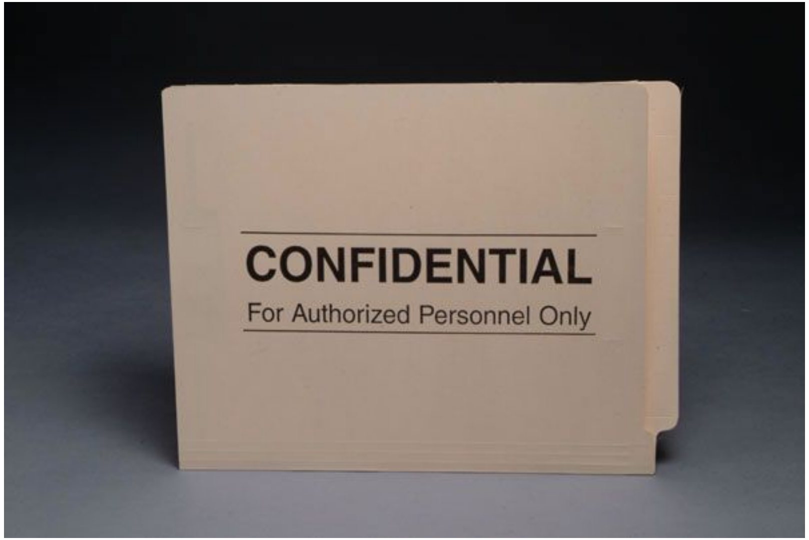
More information

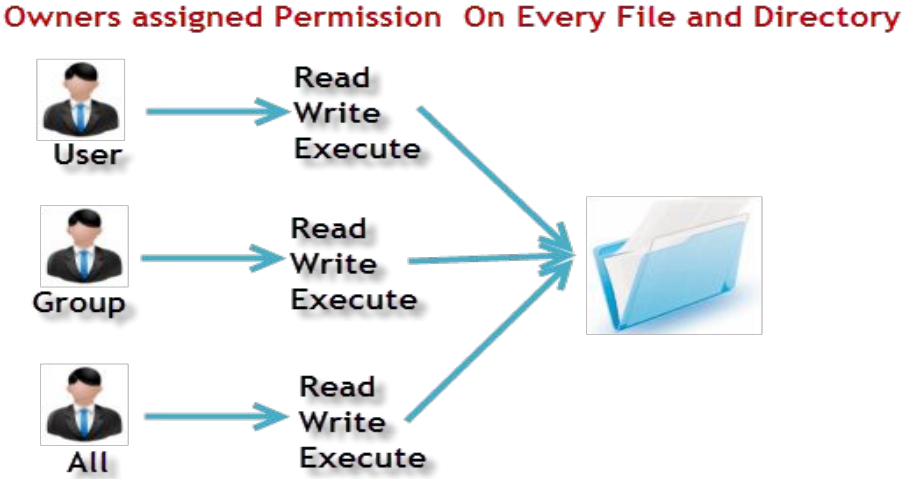
Something you are (Biometrics)

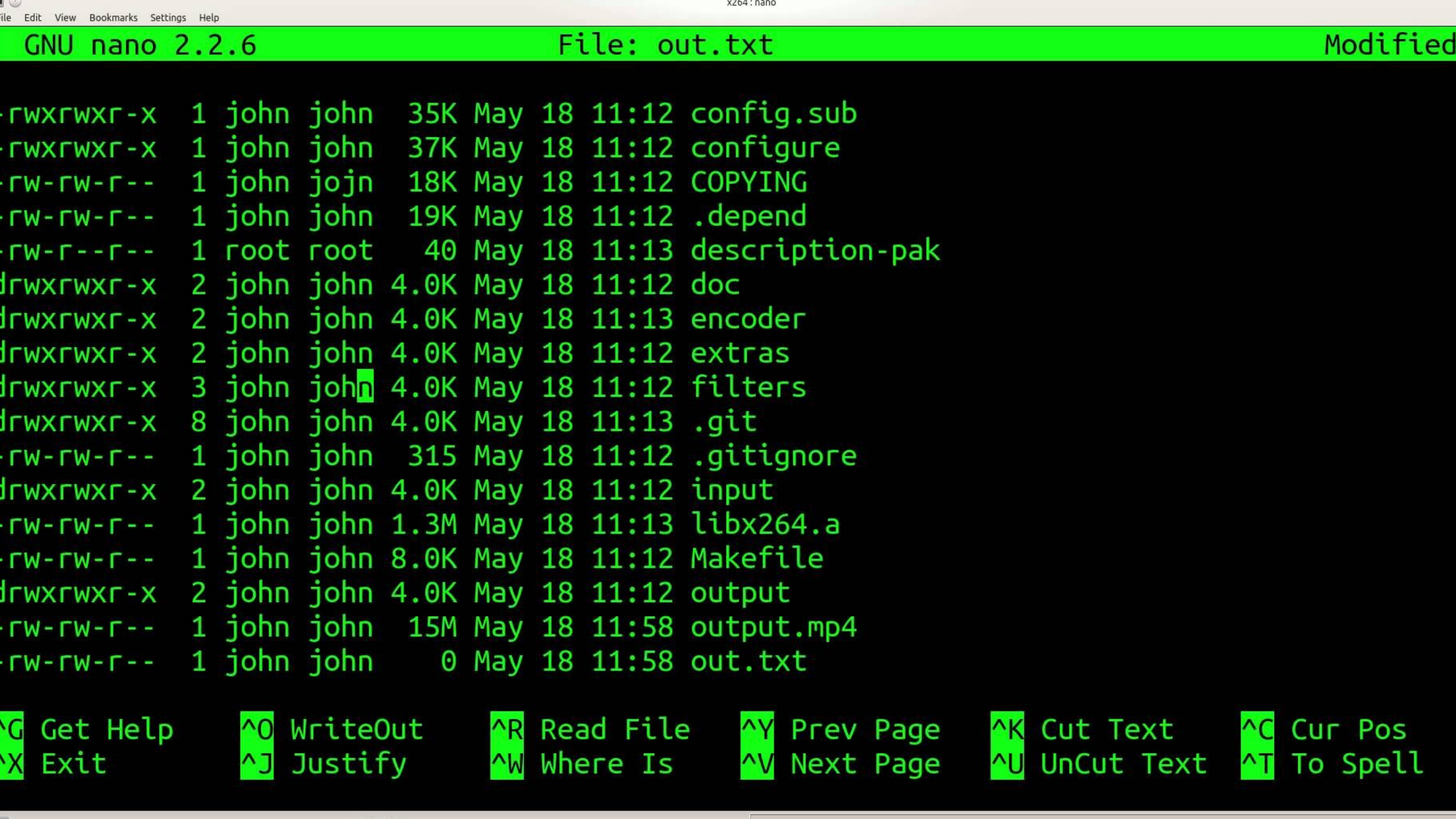


Authorization

- Access Control Lists (ACL). Who is allowed to open or edit a file?



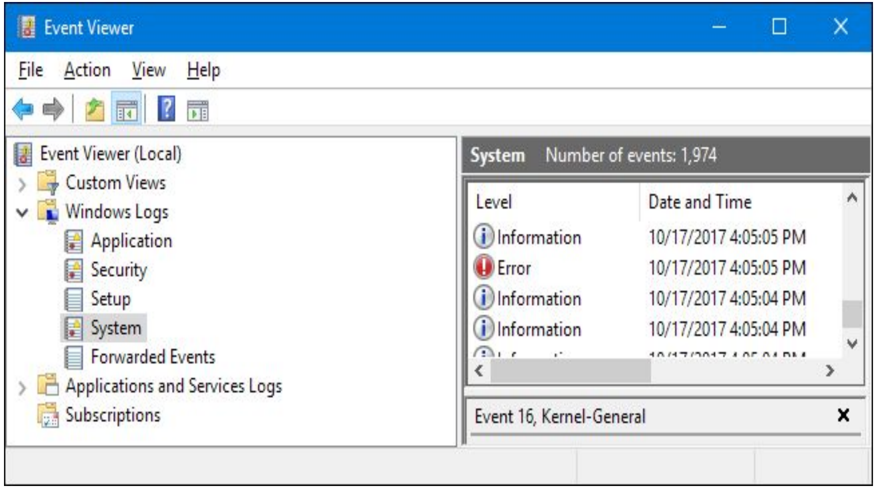




```
  GNU nano 2.2.6              File: out.txt                         Modified

-rwxrwxr-x  1 john john  35K May 18 11:12 config.sub
-rwxrwxr-x  1 john john  37K May 18 11:12 configure
-rw-rw-r--  1 john jojn  18K May 18 11:12 COPYING
-rw-rw-r--  1 john john  19K May 18 11:12 .depend
-rw-r--r--  1 root root   40 May 18 11:13 description-pak
drwxrwxr-x  2 john john 4.0K May 18 11:12 doc
drwxrwxr-x  2 john john 4.0K May 18 11:13 encoder
drwxrwxr-x  2 john john 4.0K May 18 11:12 extras
drwxrwxr-x  3 john john 4.0K May 18 11:12 filters
drwxrwxr-x  8 john john 4.0K May 18 11:13 .git
-rw-rw-r--  1 john john  315 May 18 11:12 .gitignore
drwxrwxr-x  2 john john 4.0K May 18 11:12 input
-rw-rw-r--  1 john john 1.3M May 18 11:13 libx264.a
-rw-rw-r--  1 john john 8.0K May 18 11:12 Makefile
drwxrwxr-x  2 john john 4.0K May 18 11:12 output
-rw-rw-r--  1 john john  15M May 18 11:58 output.mp4
-rw-rw-r--  1 john john    0 May 18 11:58 out.txt
```

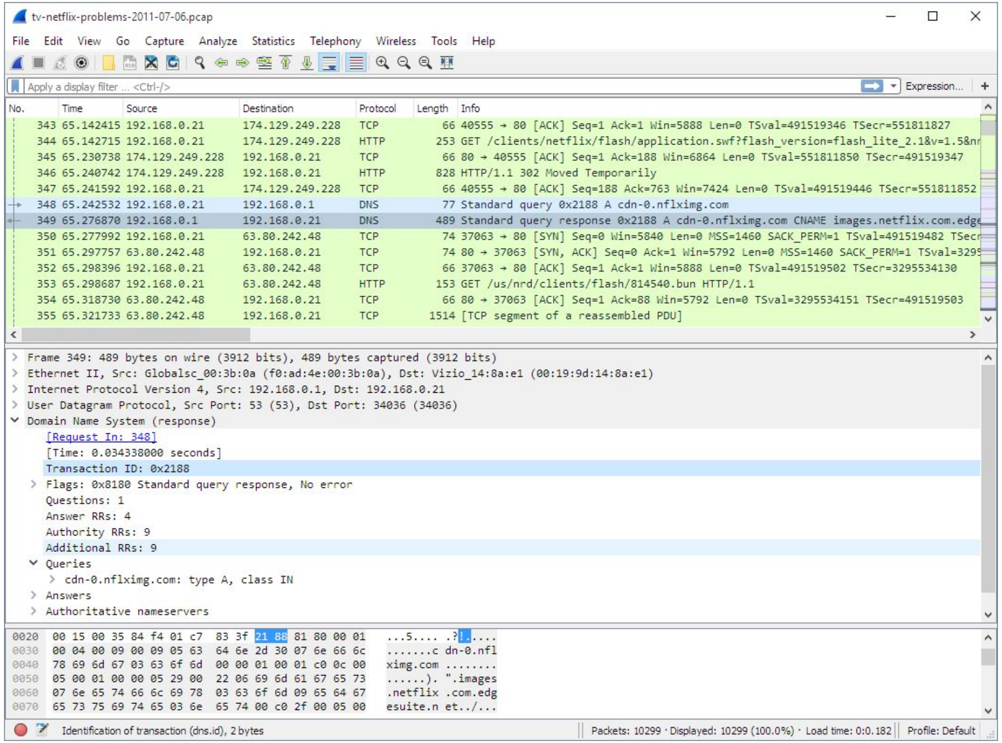
Accounting



System Number of events: 1,974

Level	Date and Time
Information	10/17/2017 4:05:05 PM
Error	10/17/2017 4:05:05 PM
Information	10/17/2017 4:05:04 PM
Information	10/17/2017 4:05:04 PM

Event 16, Kernel-General



tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

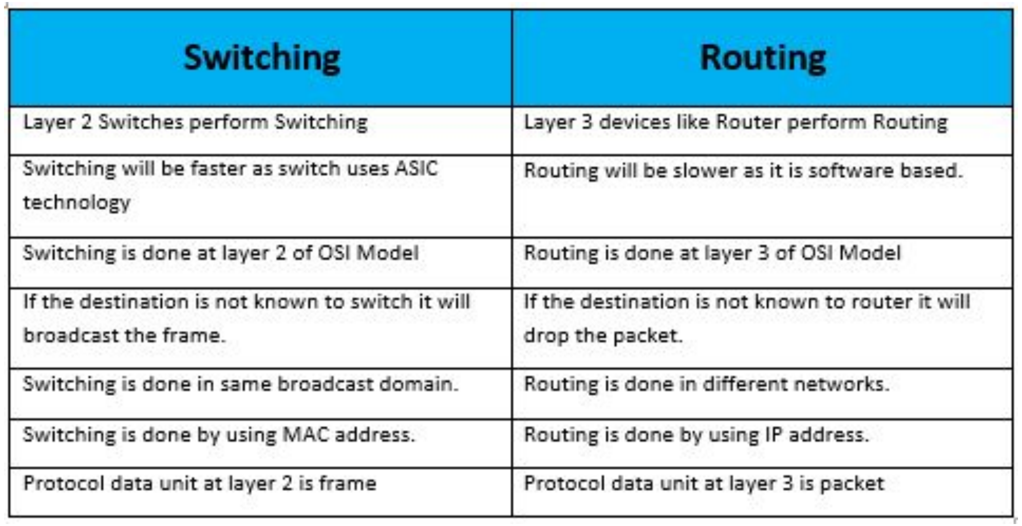
```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Networking

- Router
- Switch
- Hub
- DHCP - Gives you IP Address
- DNS - Gives you other IPs
- ARP
- IP Address
- Subnet mask

Networking

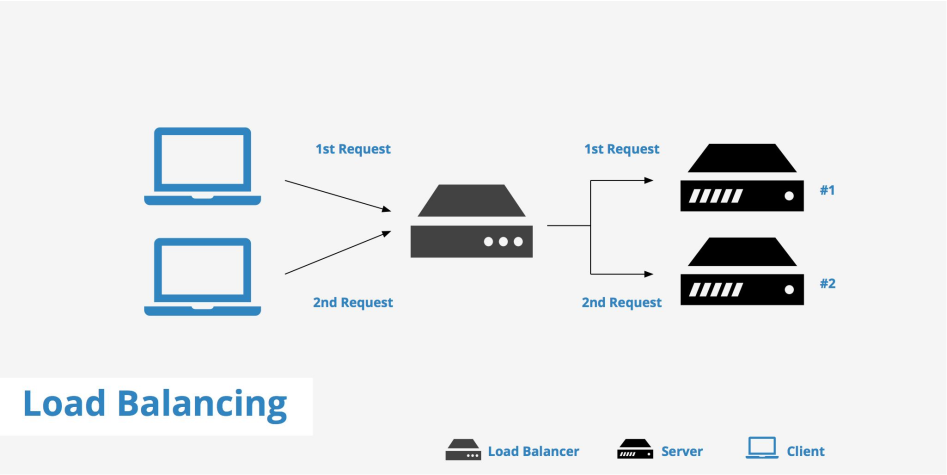


Switching	Routing
Layer 2 Switches perform Switching	Layer 3 devices like Router perform Routing
Switching will be faster as switch uses ASIC technology	Routing will be slower as it is software based.
Switching is done at layer 2 of OSI Model	Routing is done at layer 3 of OSI Model
If the destination is not known to switch it will broadcast the frame.	If the destination is not known to router it will drop the packet.
Switching is done in same broadcast domain.	Routing is done in different networks.
Switching is done by using MAC address.	Routing is done by using IP address.
Protocol data unit at layer 2 is frame	Protocol data unit at layer 3 is packet

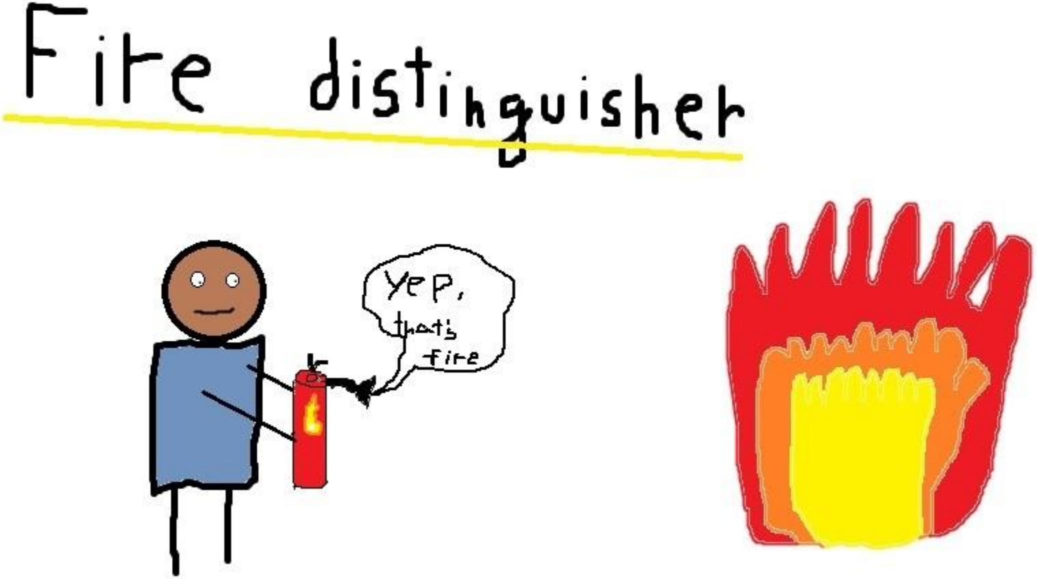
Network Security

NordVPN

- VPN
- NIDS and NIPS
- Security information and event management (SIEM)
- Honeypots



NIDS (Passive)

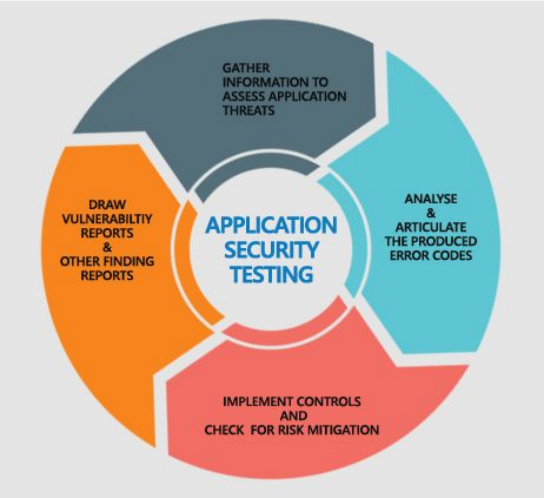


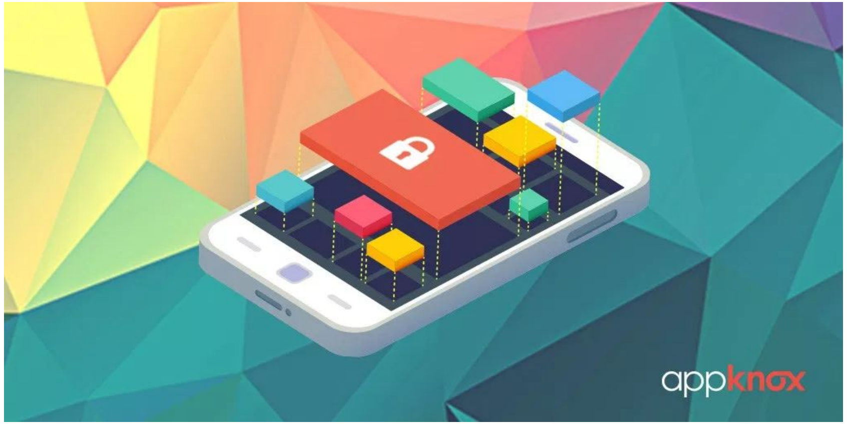
Physical Security

- Lighting
- Signs
- Fencing/gate/cage
- Security guards
- Alarms
- Secure cabinets/enclosures
- CCTV

Application Security

- Proper error handling
- Proper input validation
- Stress testing
- Version control and change management


GATHER INFORMATION TO ASSESS APPLICATION THREATS
ANALYSE & ARTICULATE THE PRODUCED ERROR CODES
IMPLEMENT CONTROLS AND CHECK FOR RISK MITIGATION
DRAW VULNERABILTIY REPORTS & OTHER FINDING REPORTS
APPLICATION SECURITY TESTING



Technology and CyberSecurity Trends

The Trends (kinda in order of hype)

- Block chain
- Artificial Intelligence
- Machine Learning
- Internet of Things (IoT)
- Bring Your Own Device (BYOD)
- Cloud
- Zero Trust Network

Block Chain

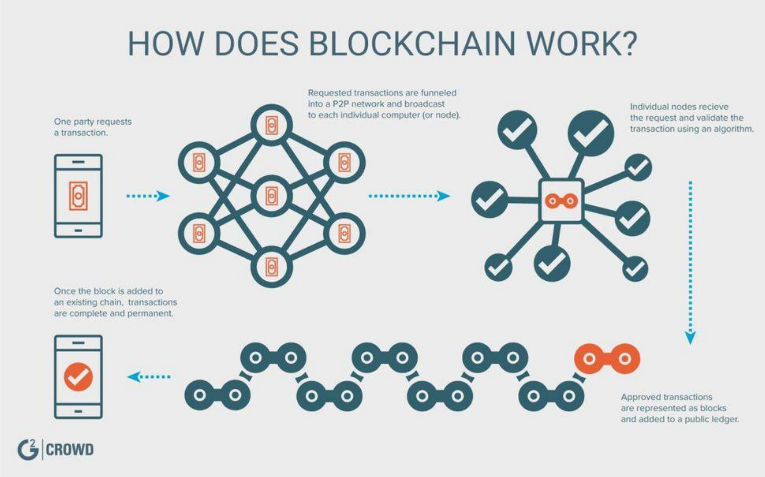
Remember the CIA triad?

Blockchain only cares about integrity. It is a network where transactions (records) are put on a public ledger that all members of the network must agree to.

It is a zero trust environment. It is slow.

It is not magic. It is not the solution to everything.

But it is pretty neat.



HOW DOES BLOCKCHAIN WORK?

One party requests a transaction.

Requested transactions are funneled into a P2P network and broadcast to each individual computer (or node).

Individual nodes recieve the request and validate the transaction using an algorithm.

Approved transactions are represented as blocks and added to a public ledger.

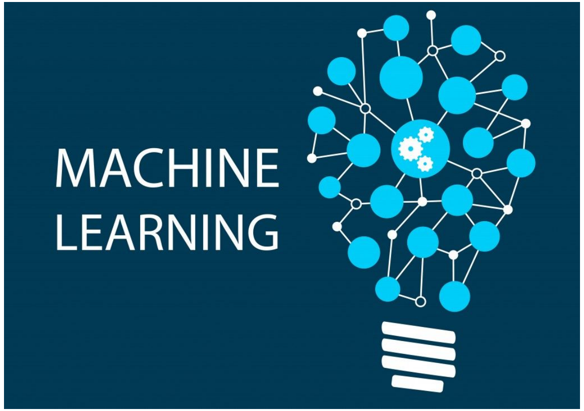
Once the block is added to an existing chain, transactions are complete and permanent.

Artificial Intelligence

AI is a broad term, basically anytime a computer is tasked to make a choice, or evaluation.

Computers don't have to be perfect, all they need to be is better than people.

Machine Learning



Building good AI is really hard.

Really hard.

So why not just have machines to it themselves?

How Machines Learn - https://www.youtube.com/watch?v=R9OHn5ZF4Uo

TL;DR you have Builder bots, and Tester bots. (This is why we need so much data).

Internet of Things

The Internet of Things, commonly abbreviated as IoT, refers to the connection of devices (other than typical fare such as computers and smartphones) to the Internet.

Why do we care?

- Built as cheaply as possible.
- Are everywhere.

Bring Your Own Device (BYOD)

- Most businesses nowadays allow employees to connect their own devices to the networks
- Privacy vs security

- Most employees do not want their every move on their personal devices to be monitored
- However, it is harder to secure something if you cannot fully monitor it

Cloud

Applications went from:

Pets - Your own personal machine.

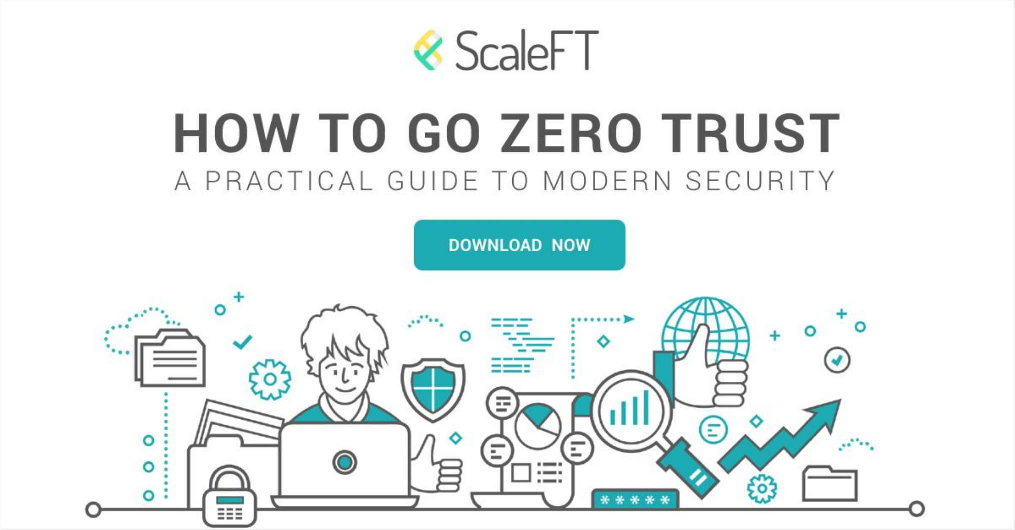
Cattle - Mostly reproducible environments, often in the cloud.

Cells - Very small servers that exist for as short as needed.

https://www.slideshare.net/shivamaan/pets-cattle-rabbits-and-microbes

Zero Trust Networks / Software Defined Perimeter

- Network security model
- Strict policies
- No traffic is trusted
- Minimum needed permissions
- Why?



CCDC Team Selection

Join the Geek Side

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

What We Look For:

- Communication & Collaboration
- Strong Work Ethic
- Writing Skills
- Personal Integrity
- Prior **cyber defense experience** is a bonus, but **not required**

How Do I Join?

Phase 1: Apply! Send your resume and a writing sample to mlim@albany.edu

- You can use something you've already written for the writing sample

Phase 2: Interview with Team Captain (I won't polygraph you, pinkie promise.)

Phase 3: Interview with current team members (see if you like us!)

CCDC Workshops (Dates TBA)

"I'm unable to join the team. Can I still come to workshops?" YES!!

What We'll Do (Tentative, always open to new ideas!)

- UBNetDef Lockdown
  - https://lockdown.ubnetdef.org/about/
- Cyber Defense Learning (like lectures, but we're all clueless. ~~Sort of.~~)
  - https://ubnetdef.org/lectures/
- NSA Codebreaker Challenge (learn to hack the NSA. Kidding.)
  - https://codebreaker.ltsnet.net/challenge

What You'll Get

- Cyber Defense Knowledge & Skills -- We train you!
- Potential for Competition Experience (UBNetDef Lockdown)
- F·R·I·E·N·D·S **(Not after season 3)**

Cya Next week!

Send your resume and a writing sample to mlim@albany.edu

Follow us on Twitter? Add on myInvolvement?

Guest speaker, Brian Dow from DASNY - Tuesday 7:15pm BB129

Top 20 CIS Controls

Thursday 7:30pm BB121

Introduction to Windows Security

- Friday 3pm BB123