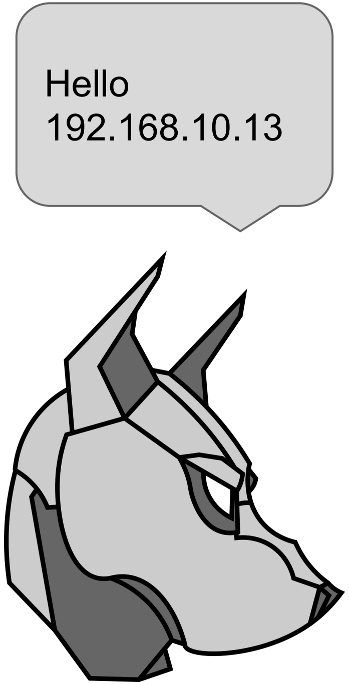
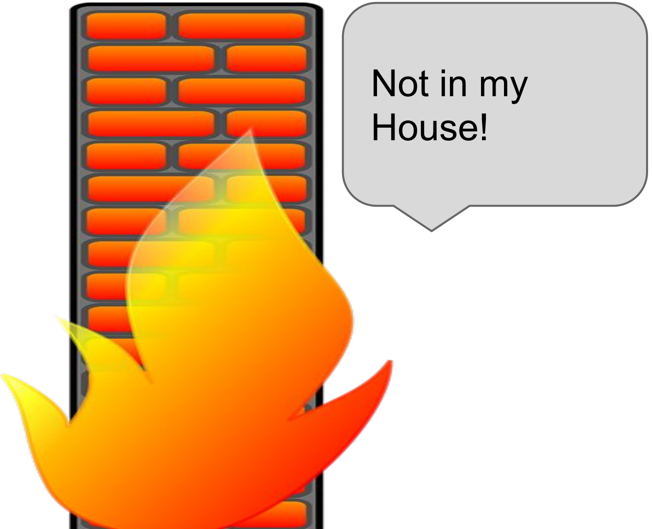
Cyber Defense Organization

Fall 2019 - Firewall





Word of the Week

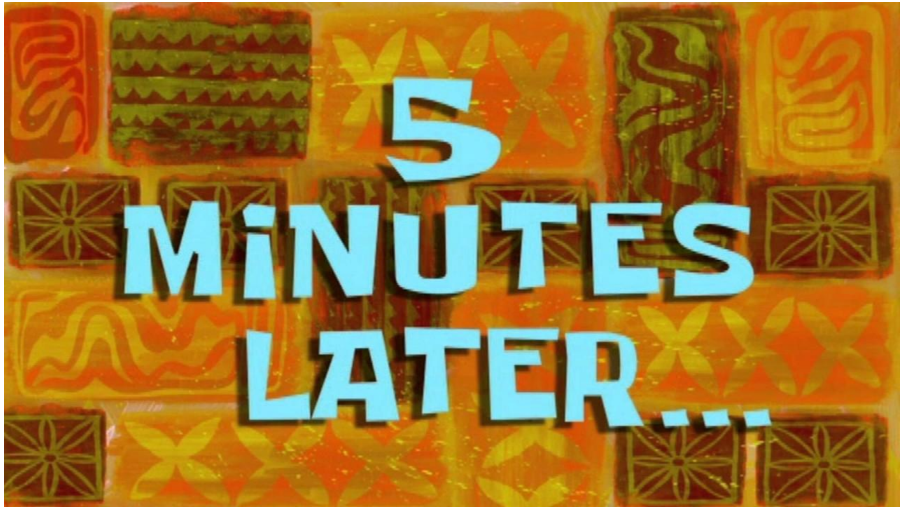
“5 Minute Plan“

5 Minute Plan

This is a great starting document for securing a computer quickly within a competition.

Goals:

1. Get your bearings
2. Get tools downloaded (Red team might kill your internet).
3. Initial Hardening
4. ???
5. Profit.



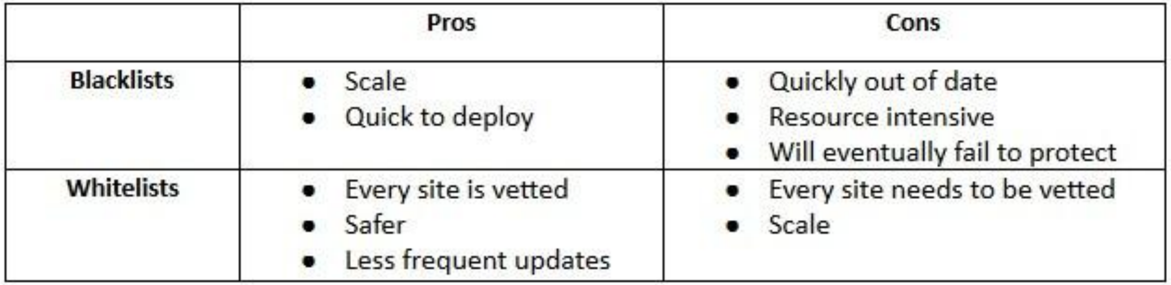
Firewalls

What is a firewall?

- The bouncers of the network
- Filters outgoing and ingoing packets based on a set of rules
- Nowadays, firewalls can filter based on application data as well as by ports and ips
- Some firewalls double as a router

White Lists VS Black Lists

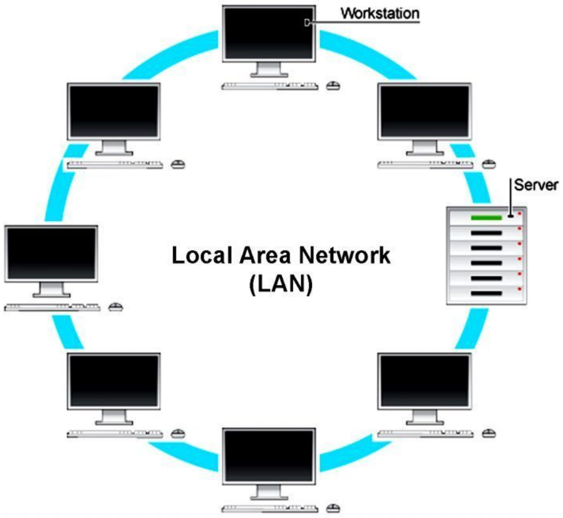
- White lists: Only allow traffic that is explicitly allowed
- Blacklists: Allows all traffic unless it is explicitly blocked
- White lists are the better option



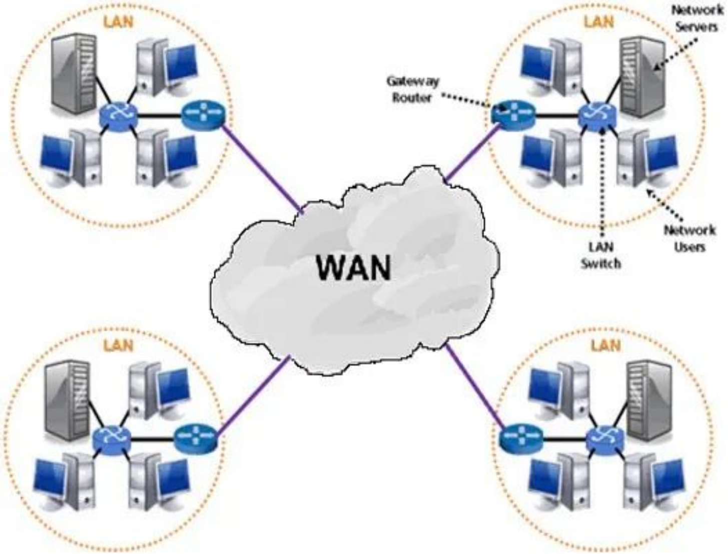
	Pros	Cons
Blacklists	• Scale • Quick to deploy	• Quickly out of date • Resource intensive • Will eventually fail to protect
Whitelists	• Every site is vetted • Safer • Less frequent updates	• Every site needs to be vetted • Scale

Lan VS WAN

A Local Area Network (LAN) is a group of computers and other network connected devices that fit within the scope of a single physical network. (EX. office building)

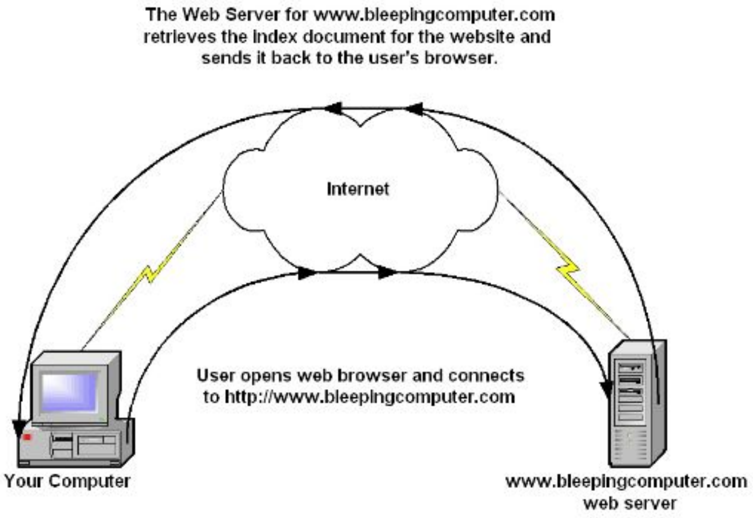


A Wide Area Network (WAN) is a internetwork that connects multiple LANs over a large area



Rule Placement

- Think of where the traffic originates
- Lan: when you connect to google.com
- Wan: Anyone outside of your network trying to start a connection with you

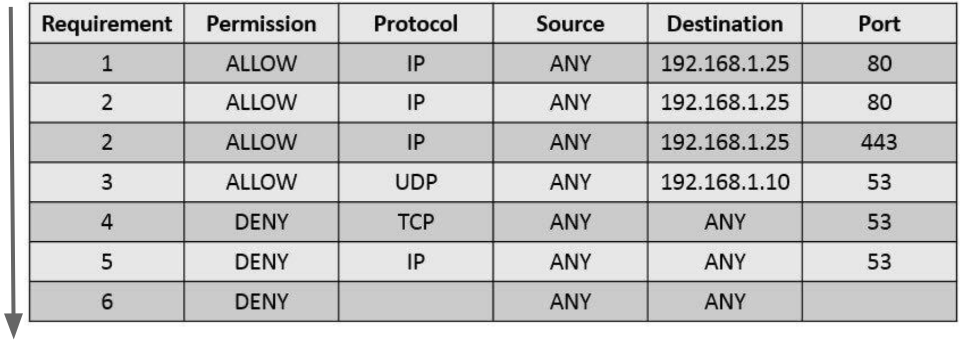


The Web Server for www.bleepingcomputer.com retrieves the index document for the website and sends it back to the user's browser.

User opens web browser and connects to http://www.bleepingcomputer.com

Order of Precedence

- The order in which firewalls read rules
- Goes first to last
- Example of firewall without order of precedence: Windows Defender
- If you place a deny any any first this happens:



Requirement	Permission	Protocol	Source	Destination	Port
1	ALLOW	IP	ANY	192.168.1.25	80
2	ALLOW	IP	ANY	192.168.1.25	80
2	ALLOW	IP	ANY	192.168.1.25	443
3	ALLOW	UDP	ANY	192.168.1.10	53
4	DENY	TCP	ANY	ANY	53
5	DENY	IP	ANY	ANY	53
6	DENY		ANY	ANY	

Hands on Time

What we will be using

- Open Source, FreeBSD firewall called pfsense
- Extremely versatile
- Command shell is kind of like linux (a couple of different commands)

Start those VMs

Workshop_pfsense. Webgui login: admin pfsense

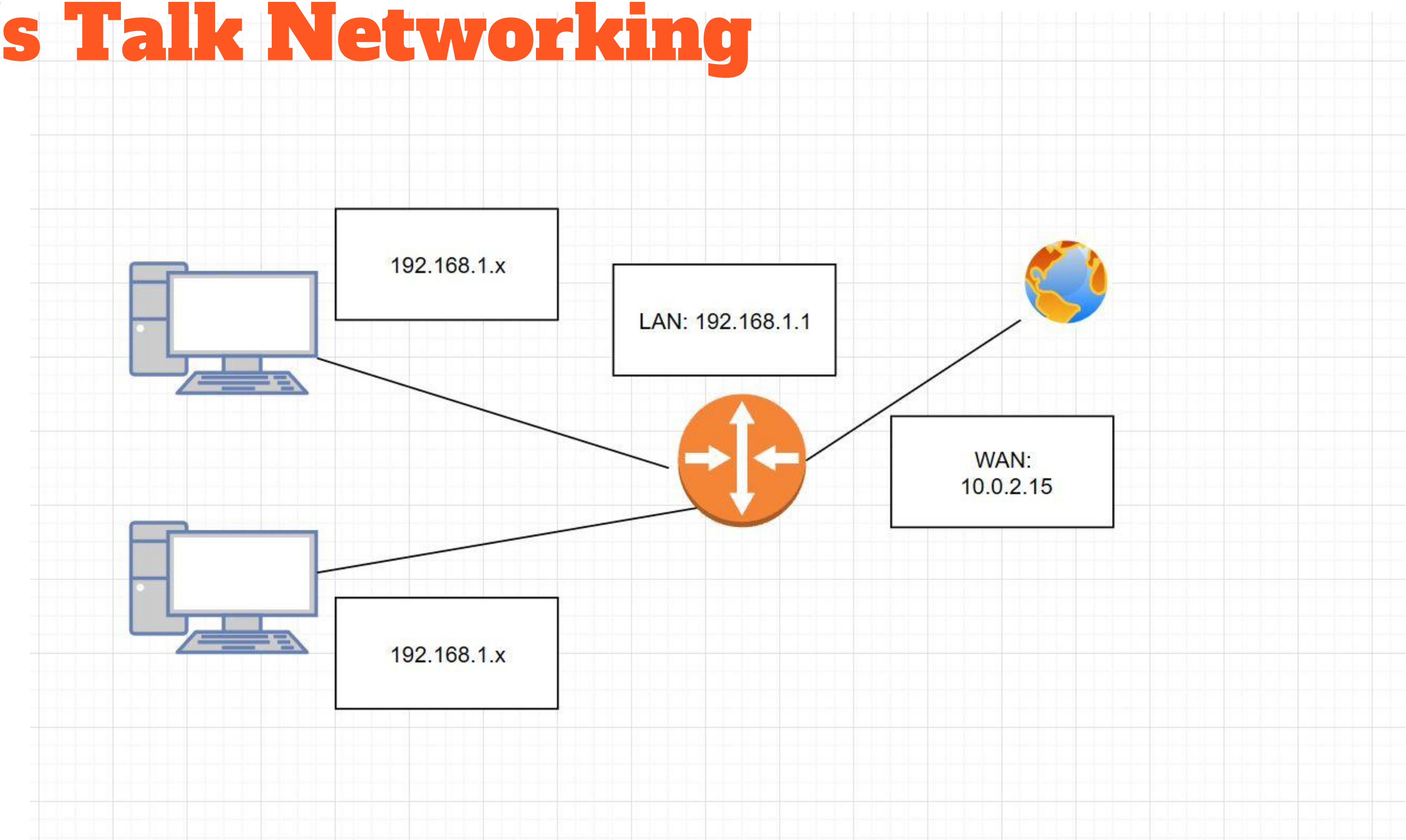
Cdo_ubuntu (password is bb123#123)

Pfsense Guide

- Go here and follow along!

https://tinyurl.com/**CDOFall2019Firewall**

Let's Talk Networking



192.168.1.x

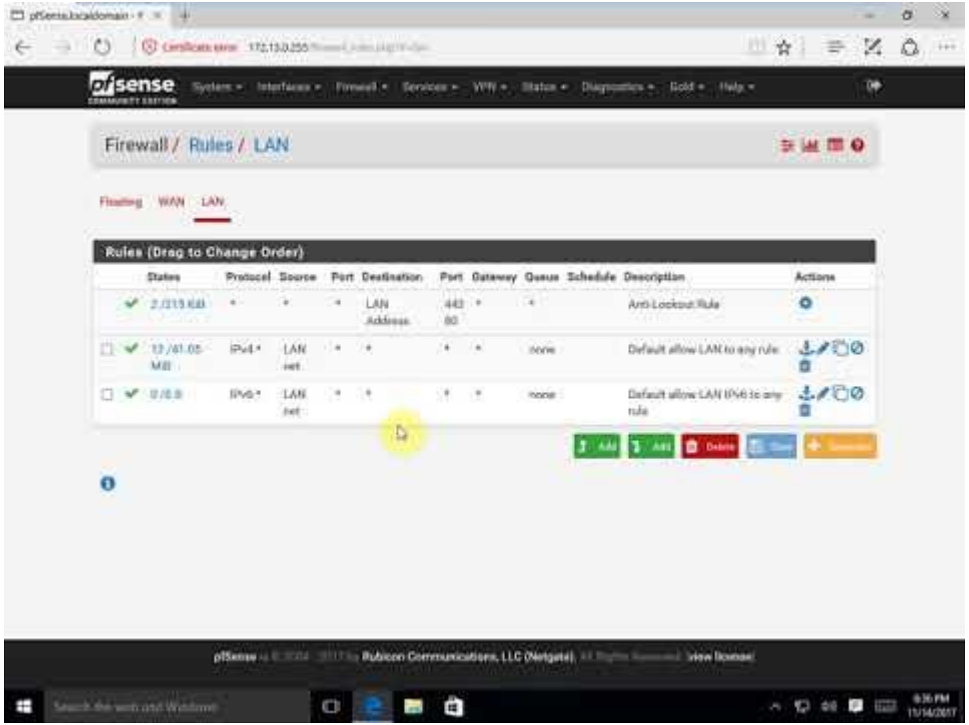
LAN: 192.168.1.1

WAN:
10.0.2.15

192.168.1.x

WebGui

- Everything you can do on the shell you can do here:
  - Rule Creation
  - User management
  - Package installation
  - Log analysis
  - Much More
- Use your LAN IP to access the GUI
- Default gateway: Destination of all traffic that is not on the same network as the sender



Firewall / Rules / LAN

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	2 /215 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
□	✓	12 /41.05 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

The Rule Scenario:

The man, the myth, the legend that is Tyler Blanco, is yelling at me because too many people on the internet are connecting to his private website full of Damien Dane pictures. He even threatened to change the website name to “I hate Jonathan Matza”. The website is located on a web server **http://3.15.234.78/** on the WAN and listens on http (port 80). Create a rule denying all traffic from the LAN to his website.

Second Rule Scenario:

So, you just found out that the man, the myth, the legend Tyler Blanco, tried to SSH into your firewall so that he can change the rule himself. THIS IS UNACCEPTABLE. The firewall is too boring for him to worry about. He needs to worry about other things, like taking pictures of our mascot Damien Dane. Block his ssh access so that he can continue being the man, the myth, the legend.

But First, SSH into Pfsense

- Type in this command on ubuntu: **ssh -p 22 root@192.168.1.1**
- The password: **bb123#123**
- Lets go see the traffic:
  - Go to the Web Gui, under Diagnostics pftop
- Exit out of pfsense and lets block cdo_ubuntu

If we Have time: Aliases

- Allows you to incorporate multiple ports, urls, ips, etc into rules, port forwards, etc
- Great for organization!
- Follow along while I lump the ssh and http ports into one alias and use it to create one rule

NOT MAKING FIREWALL RULES
MAKING FIREWALL RULES ONE PORT AT A TIME WITH NO LOGGING
ADDING LOGGING TO FIREWALL RULES
CREATING ALIASES
imgflip.com

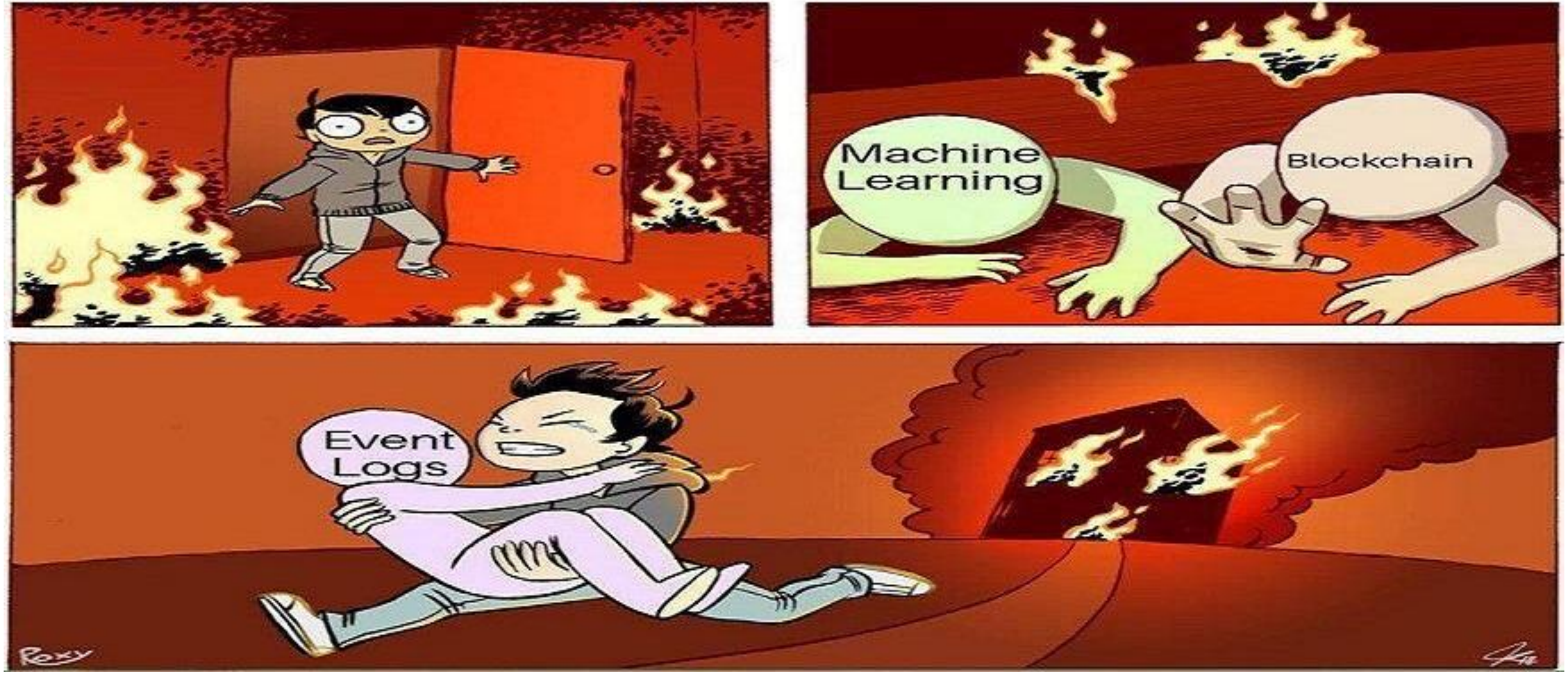
Want more? Try to do these:

Block reddit.com

Try Port Forwarding (remember your minecraft server?)

Create a captive web portal.

Next Time: Forensics! (Log Analysis)



Add us on Social Media! Cya next time!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!