

A decorative border made of teal squares, each containing a white geometric pattern of lines forming triangles.

# Welcome

Cyber Defense Organization



# Collegiate Cyber Defense Competition

We recently went...

1st time ever at regionals

Placed 5th out of 10th teams



# Competition TIME!

Who is interested in being on a competition team?

UBNetDef is on **April 28th, 2018 from 9AM to 5PM**

Hosted at the University at Buffalo.

We are sending TWO teams! They will consist of 6 members each.



# Also upcoming:

1. Eboard meeting Friday at 11am BB121
2. Board applications are coming soon!

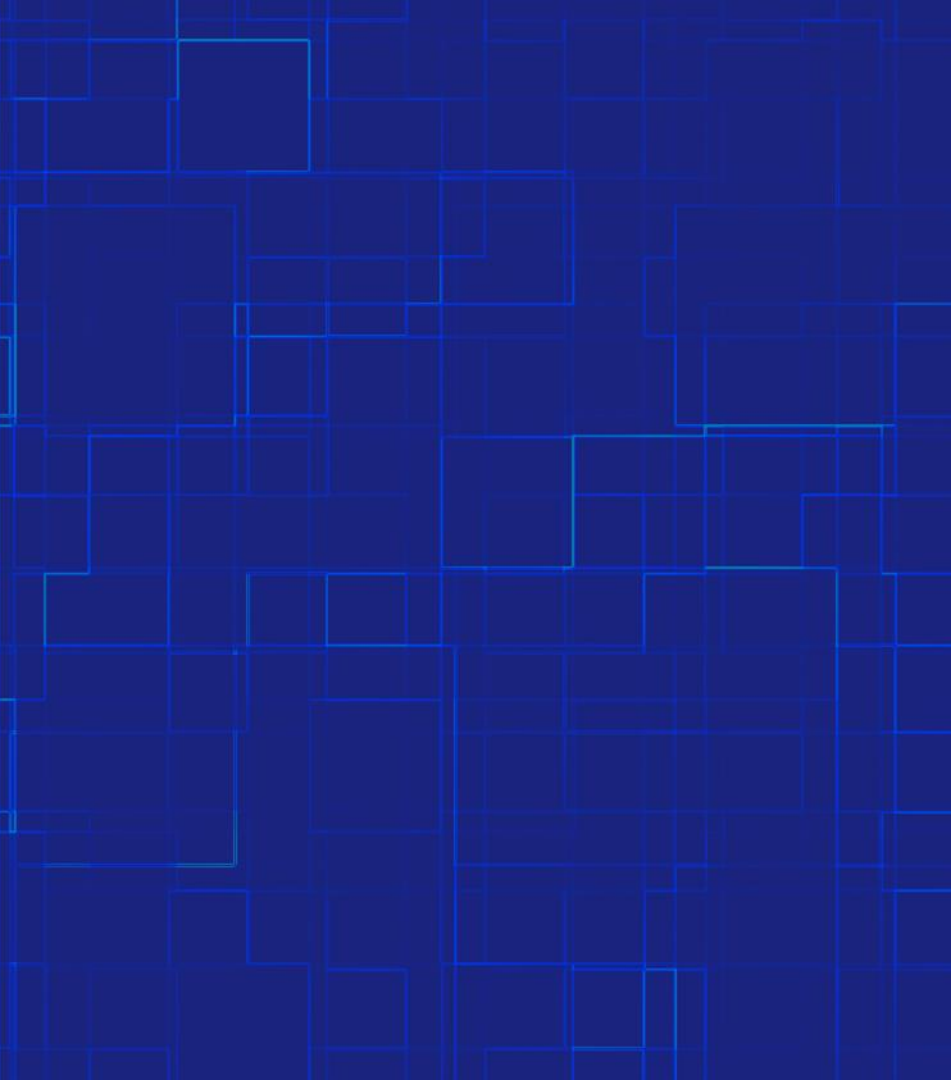


# Student Elections

Guest Dillion Asmus

Business Management Academic Seat -- Student Association

Email: [dasmus@albany.edu](mailto:dasmus@albany.edu)



# **5-Minute Plan Philosophy & Windows Example**

By Liam



**What is a 5-  
minute plan?**



## 5-Minute Plan

This is our plan of attack as soon as you walk on to the scene of an incident.

(In this case the competition).

While it can be longer than 5 minutes, it generally includes context-agnostic steps you want to take.





# What does it actually look like?

A fancy checklist, often separated into modules/chunks.

# Creating a checklist

- Have a factsheet you can fill out
- Be as specific as possible
- Bold the critical parts
- Don't include anything you have never tried
- Don't shorthand anything (funny story in Qualifier)
- Print it a little larger than you need
- Use the full path
- Use a good template that can automatically create a table of contents



# Testing a checklist

Easy way:

1. Don't look at it for a few days
2. Have a friend set up an environment
3. Go through your list step by step

Realistic way:

1. Realize that you have run out of time to build a list
2. Throw together something at the last minute
3. Travel in a car for 5 hours
4. Get to a cold hotel room
5. Barely sleep. (Bonus points if you get an allergic reaction).
6. Wake up at 6:30am
7. Feel too anxious/sick/nervous to eat
8. Listen to a boring person explain the importance of cyber
9. Lose the will to live
10. Run to your room
11. Not even have your coat off before scoring starts
12. Begin your checklist

# My Steps:

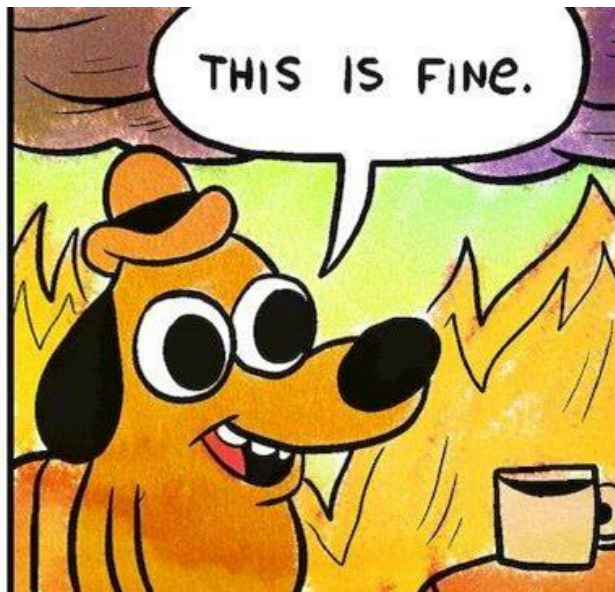
## Phase 1:

1. Initial Access
2. New Admin User
3. Backups
4. **Setting Auditing**
5. **General Hardening steps**
6. Downloading tools

## Phase 2:

1. Service upkeep
2. Firefighting
3. Threat hunting

## Phase 2:



# Setting up Auditing

Why is this so important?

- It lets you get the “heartbeat” of your device
  - Staring at the desktop gives you nothing
- Logs are like a cellar of fine wine
  - It’s hard to have too much
  - And it takes time for them to be valuable



# General Hardening Steps

1. Mitigating Common Vectors
  - a. Preventing connection on certain ports
2. Eliminating unnecessary functionality
  - a. Turning off print spooling, or RDP
3. Setting Up Proactive Measures
  - a. Vulnerability scanners (Microsoft Baseline Security Scanner)
  - b. Antivirus (Windows Defender)



---


# Workshop Plan

Cyberdeforg1


- 
1. Auditing
    - a. Enable logging of Logins, Privilege use, and policy changes
  2. Hardening
    - a. Disable Guest Account
    - b. Set machine lockout threshold
    - c. Enable password complexity requirements
    - d. Disable services: print spooler, Remote Desktop
    - e. Look for weird Firewall rules
    - f. Block port 5968 (Remote execution)


Filters ▾


Best match


 **Local Security Policy**  
Desktop app

Settings >


 View local services


 Connect to work or school

 Edit local users and groups

 Edit group policy

Apps >


 This PC

 Weather

localSecurity Policy

Local Security Policy

File Action View Help

 **Security Settings**

> Account Policies

> Local Policies

> Windows Firewall with Advanced Security

> Network List Manager Policies










> Public Key Policies

> Software Restriction Policies

> Application Control Policies

> IP Security Policies on Local Computer

> Advanced Audit Policy Configuration

Name	Description
 Account Policies	Password and account lockout policies
 Local Policies	Auditing, user rights and security options policies
 Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
 Network List Manager Policies	Network name, icon and location group policies.
 Public Key Policies	
 Software Restriction Policies	
 Application Control Policies	Application Control Policies
 IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration
 Advanced Audit Policy Configuration	Advanced Audit Policy Configuration



Local Security Policy

File Action View Help

← → ↗ ✕ ↶ ? 📄

Security Settings	Policy	Security Setting
Account Policies		
Password Policy	Enforce password history	24 passwords remember...
Account Lockout Policy	Maximum password age	42 days
Local Policies	Minimum password age	1 days
Windows Firewall with Advanced Security	Minimum password length	7 characters
Network List Manager Policies	Password must meet complexity requirements	Enabled
Public Key Policies	Store passwords using reversible encryption	Disabled
Software Restriction Policies		
Application Control Policies		
IP Security Policies on Local Computer		
Advanced Audit Policy Configuration		

# Local Security Policy

File Action View Help



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

## Account lockout threshold Properties

Local Security Setting Explain

### Account lockout threshold

This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE



## Now Try:

1. Auditing
  - a. Enable logging of Logins, Privilege use, and policy changes
2. Hardening
  - a. Disable Guest Account
  - b. Set machine lockout threshold
  - c. Enable password complexity requirements

(Hint, expand all the top level options!)

---

# Enable Firewall logs

---

## Method 1: Windows Firewall GUI

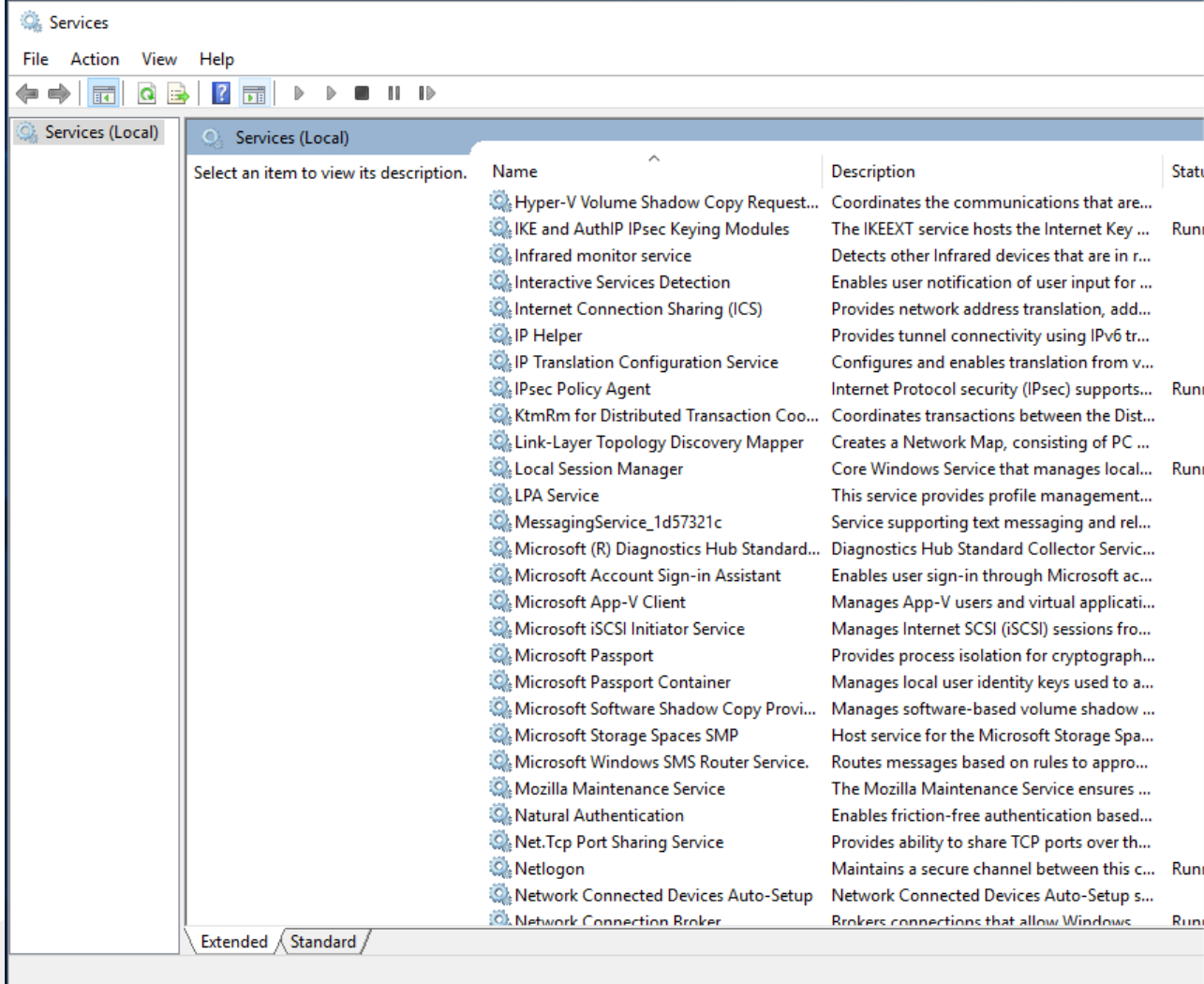
1. Open the **Advanced Firewall Management** Snap-in (WF.msc)
2. Select the **Action | Properties** from the main menu
3. On the **Domain Profile** tab, click **Customize** under the **Logging** section.
4. Increase the file maximum size.
5. Turn on **logging for dropped packets**
6. Turn on **logging for successful connections**

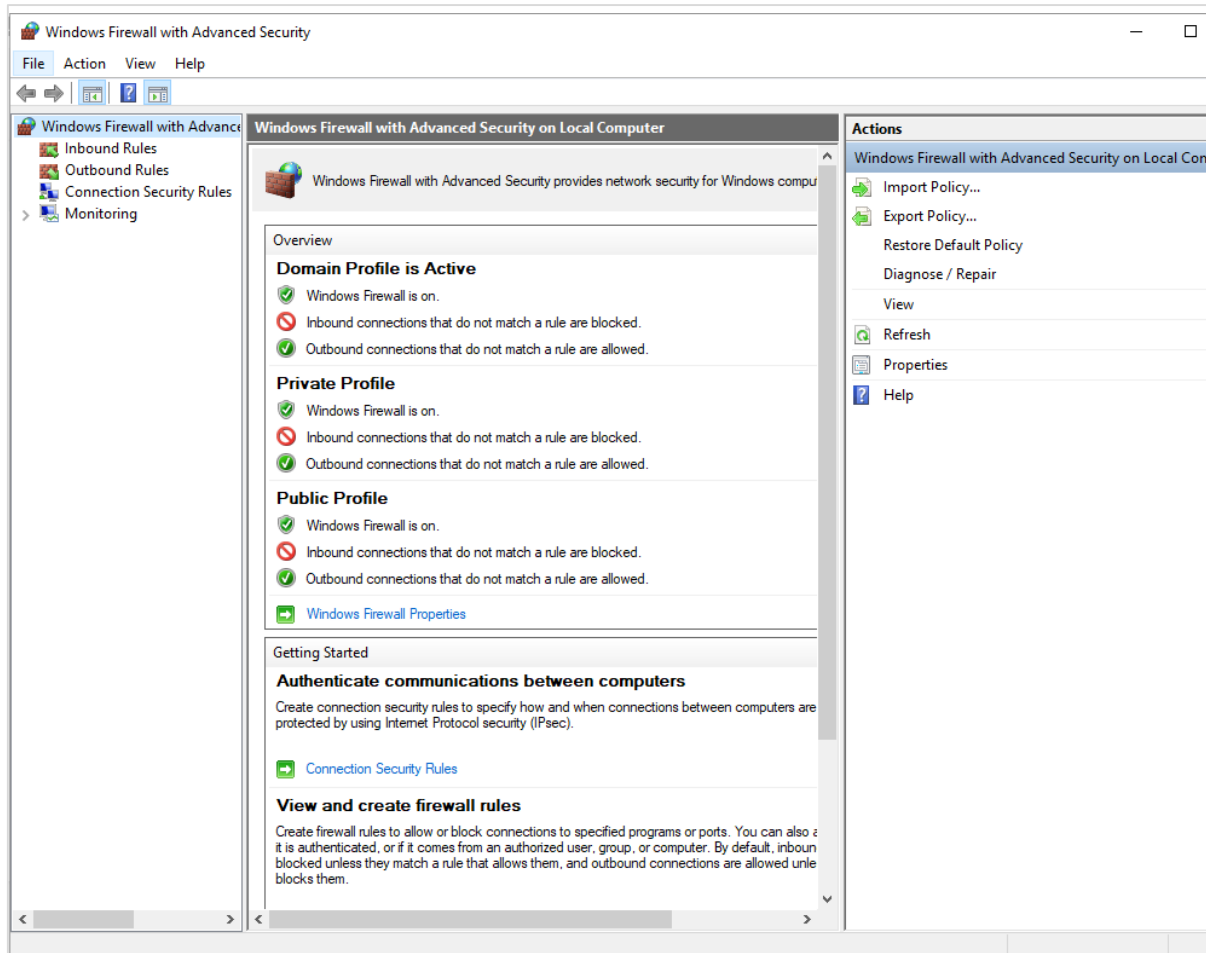
## Method 2 – PowerShell

1. Open a **PowerShell** window as *Administrator* and execute:
2. Set-NetFirewallProfile -name domain -  
LogMaxSizeKilobytes 10240 -LogAllowed true -LogBlocked  
true

By default your firewall will start logging to  
**%systemroot%\system32\LogFiles\Firewall\pfirewall.log**. You  
may like to change this to a central logging server.

# Find and disable: print spooler & remote desktop





Look for weird rules, and remove them.

Create a new inbound rule, block port 5968.

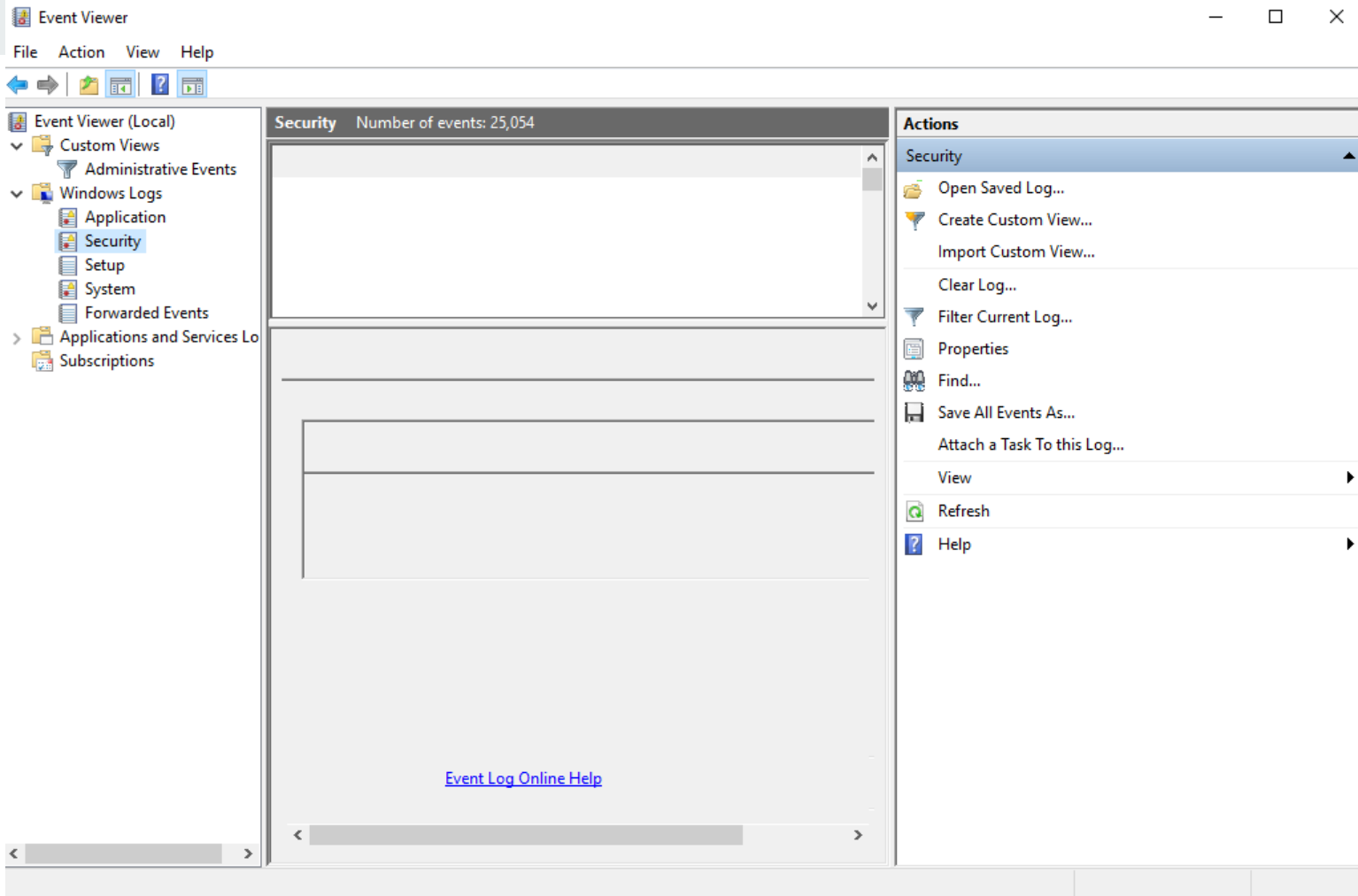


# Finally:

Remember those audit policies?

They *\*should\** have been logging all the actions you have been taking!

They are all in Event Viewer!







# Things we did not cover

- Active Directory User, Group, Computer and OU Management
- Creating a new Administrator
- Creation, implementation, and testing of Group Policy
- Monitoring, Testing, Backing Up, and Managing DNS
- Monitoring, Testing, Backing Up, and Managing DHCP
- Understanding sysinternal tools (procmon, procexplorer, tcpview)
- Running and Understanding a Microsoft Security Baseline Analyzer
- Powershell



# Follow us on Twitter! @ualbanyCDO

New logo -- Ideas? Email them to us at [cyberdefenseorg@albany.edu](mailto:cyberdefenseorg@albany.edu)

Whats coming up again?

1. UBNETDEF
2. Eboard meeting Friday at 11am BB121
3. Board applications are coming soon!

