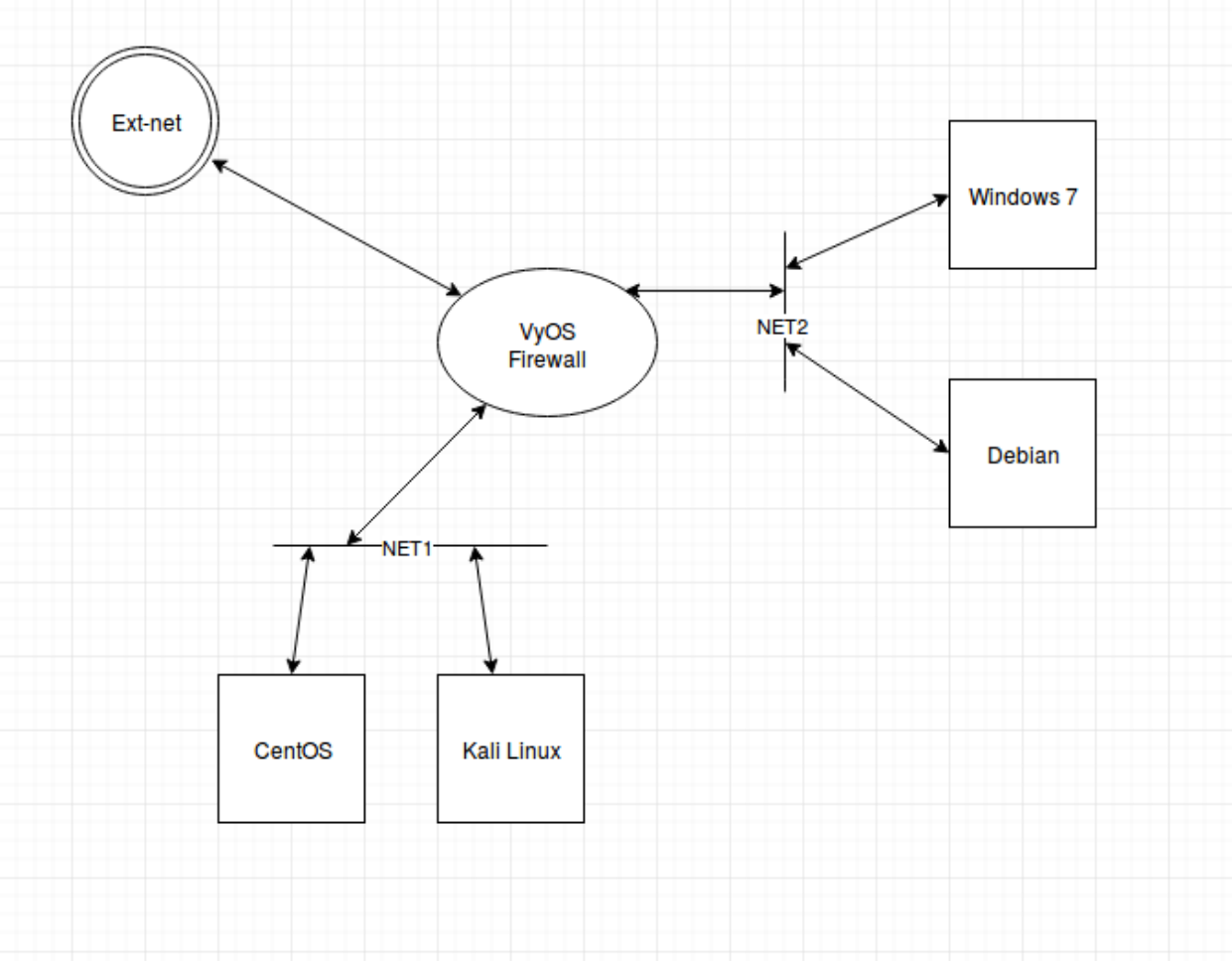
TNP09 - Virtual CCDC Invitational - Part 1



Learning Objectives

1. **Infrastructure provisioning**
2. **Network Security**
3. **Perimeter Security**
4. **Firewall Provisioning**
5. **Logging and Network Scanning**
6. **Service Hardening**

Duration: Oct 20 - Nov 1 (11:59 pm)

Max Possible Points (21/20)

TNP09 - Virtual CCDC Invitational - Part 1

Task 0

1. Create a Lab environment as shown above.
2. Read and familiarize yourself with commands required for VyOS firewall
3. Use your My ASU account to download and create Windows 7 image
4. Download VyOS and Kali Images from location in references below.

Task 1

Using the environment above configure the following services.

Machine	**Services**
Windows 7	ntp client, mysql server
Kali Linux	ntp client
Debian	ssh server, ftp server, dns client, apache, ntp server
CentOS	ssh server, telnet, ntp, smtp, rsyslog server, dns server, ntp client
VyOS	Packet Filtering, Logging

Task 2 - CCDC Invitational 2016

Inject Duration: 60 Minutes

To Infrastructure Team

Subject: Server Hardening

An external consultant has warned us that our servers may not be hardened correctly, and therefore are vulnerable to APT exploits.

Please develop a plan with standard configurations for hardening each of the servers. In the plan, clearly identify how you are going to harden the various Linux and Windows systems.

After developing the plan, implement it, and note in your plan that these tasks have been completed on all machines.

Thank you.

Task 3 - CCDC Invitational 2016

Inject Duration: 90 Minutes

From: CIO Management Team

To: Infrastructure Support Group

Subject: Inventory - Internal Scan

Your predecessors did a poor job keeping documentation updated and we only have a cursory understanding of what services are running on our systems. Lacking a clear picture makes it difficult to make decisions on resource allocation.

Please inventory all of our systems. We need to identify all the accounts they possess and the services they offer. I know you are pressed for time but the more detail you can provide the better.

It would also be helpful if the report was organized and formatted rather than screen dumps and I would prefer a formal report including topology diagrams. That said, I will take whatever you can give me if things are rough.

At minimum, however, the report should clearly identify:

System Name
Platform (Windows, Linux, Solaris etc..)
List of Accounts
List of Services
List of Open Ports

Thank you.

CIO Management Team

Task 4 - CCDC Invitational 2016

From: Sec Ops

To: Network Team

Subject: Implement DoS Protection Policies

The CEO read a report in Network World about how hackers often use DoS Attacks against major businesses.

Be sure your Firewall is configured with a defining Dos Protection Policy together with defining zone protection on the EXTERNAL zone.

Your deliverable is a report to the IT Director on how you accomplished this, with screen shots showing the policy and the zone protection dialogue box.

Thank you.

Task 5 - Firewall Policy

Machine+Service	**VyOS Firewall Policy**
windows-mysql	Allow ALL
debian-apache debian-ftp debian-ntp debian-ssh debian- dns server	Net 2 - ALLOW Net 2 - ALLOW Net 1,2 - ALLOW Net 1,2 – ALLOW Net 2 - ALLOW
centos-ssh centos-telnet centos-smtp centos-rsyslog server	Net 1,2 - ALLOW Net 1 - ALLOW Net 1 - ALLOW Net 1,2 - ALLOW
Firewall	Logging Enabled
Everything Else	DENY

Task 6 - Bonus Point - CCDC Invitational 2016 - 1pt

Inject Duration: 30 Minutes

From: Director - Information Security

To: IT Staff

Subject: Social Networking Policy

I knew I had forgotten something - the Chairman just asked me about a policy for social networking sites. Apparently his son's laptop just got infected thru Facebook and he wants to make sure we're not vulnerable here.

I'm somewhat familiar with Facebook, but I really need your expertise and experience to develop a corporate policy dealing with social media and social networking sites. I want you to make recommendations on whether or not we should allow people to even use social networking sites from our systems; who should be allowed to use them if we do allow it; what types of content can be posted if we allow it, etc. Please submit in the form of a policy document.

I have a meeting with the CIO in 30 minutes - I need this before then. Please remember to cite anything you find and copy from the web.

Thank you.

Director - Information Security

Submission Instructions and Grading

1. Show evidence for successful completion using few screen-shots for each sub task. Submit Report with team name and member names on BB. One file submission per team is required. Any zip file with screenshots will not be accepted. It must be one single report. Penalty of 20% will be applied for not following submission instructions.

Task	Points	Description

Inject Completion (Tasks 1,2,3,4,5)	20 (4x5)	Successful completion of tasks
Bonus Point (Task 6)	1	Successful completion of tasks

.

References

[1] https://www.unixmen.com/configuring-sendmail-smtp-server-on-centos-a-scientific-linux/
[2] CCDC 2016
[3] https://blacksaildivision.com/ntp-centos
[4] http://gitlab.thothlab.org/achaud16/Capstone-Project-2017/tree/master/Capstone2/Resources
[5] https://wiki.vyos.net/wiki/User_Guide
[6] https://wiki.debian.org/NTP