Team 5: Team 5 White Team Documentation

Publicly Available Services

Domain Name	IP	Ports
files.team5.isucdc.com	64.5.53.10	22,445
www.team5.isucdc.com	64.5.53.20	22,3000
wc.team5.isucdc.com	64.5.53.30	3389
lc.team5.isucdc.com	64.5.53.40	22
ad.team5.isucdc.com	64.5.53.50	3389

Servers

Overall

All servers have been audited and scanned using 'Nessus', 'nuclei', 'nmap'.

Operating System Information

Our file server is running a Red Hat-based distribution called Alma Linux (v8.9). Our web server is running Ubuntu 22.04. The Windows Client is running Windows 10. The Linux Client is running Ubuntu 22.04. The Active Directory server is running Windows Server 2016.

Firewall Rules:

All Servers: Outbound connections on all devices are only allowed to machines on the 64.5.53.0/24 subnet. **File Server**: Inbound connections are allowed on ports 22 (ssh) and 445 (smb). **Web Server**: Inbound connections are allowed on ports 22 (ssh) and 3000 (http(s)). **WC Server**: Inbound connections are allowed on port 3389 (rdp). **LC Server**: Inbound connections are allowed on port 22 (ssh). **AD Server**: Inbound connections are allowed on port 3389 (rdp).

Applications

File Server: Samba is running to provide students with access to their files and home directories. **Web Server**: A "Next.js" application hosts the school's web page. A regex check has been added to the email handler to validate user input.

Fixes

Web Server: The web server was given it's own service account. The python server for handling emails was fixed to validate emails and prevent injection. Added a timestamp to the python POST server for intrusion reports.