IT 4983/W01  
Group Members:   
Eric Whang, Mark Schuler, Alex McMath, Daniel McDuffie, Ryan Smith, Samuel Olubummo  
Project 7: Security Solution for a Small Business

Vulnerability Assessment: cyberlei05.kennesaw.edu

**Mapping:**

Using Nslookup (dig for Linux):

* Command: nslookup cyberlei05.kennesaw.edu
  + Result: IP Address - 10.96.60.49
  + Purpose: Gives us the IP address to target the server

Text

Description automatically generated

Testing for ICMP rules on firewall:

* Command: ping 10.96.60.49
  + Result: ICMP not denied – Active ping from target server
  + Purpose: To determine if a DDoS attack would be plausible
  + We were told not to use DDoS because it may affect other services on the KSU network

Text

Description automatically generated

Text

Description automatically generated with low confidenceUsing Nmap:

* Command: nmap -Pn 10.96.60.49
  + Result: SSH, http, https, rpcbind, zeus-admin
  + Assessment: Secure

**Open-Source Intel Gathering:**

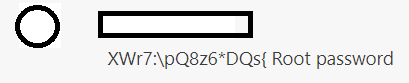
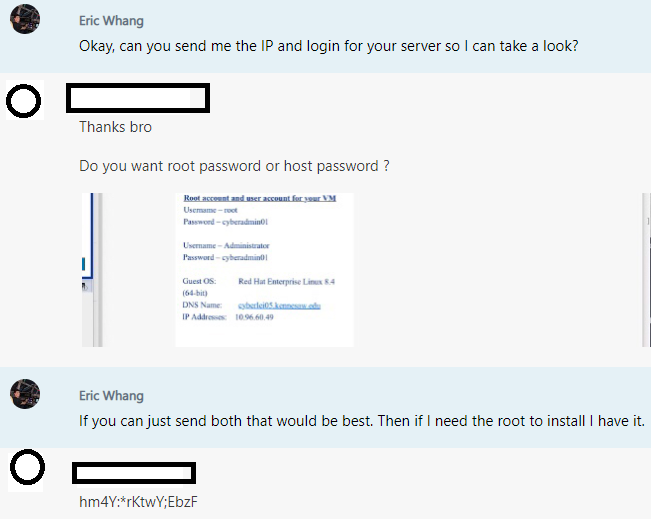
* Facebook, LinkedIn, etc
  + Used to determine who the group members in our target server were

**Target Infiltration**

* Target team changed both root and administrative passwords and according to wpscan and Burp Suite the server was not running a known web platform software like WordPress or OpenCart which we later confirmed through directory mapping
  + Default password was attempted: cyberadmin01
* Password cracking tools were not capable of cracking the root or administrator passwords

**Social Engineering**

* Spear Phishing campaign launched on the group members after password cracking was not successful
  + We reached out to our classmates on the target team to assist with server configurations
  + One member responded and said they needed help configuring Avast Antivirus software



* Once inside, we started mapping directories and installed a back door
  + Commands: adduser Apache3 / passwd \*\*\*\*\*\*\*\* / sudo -l -U Apache3
  + Purpose: To ensure persistent access to the user if the team discovered our presence
  + Added line to visudo: Apache3 ALL=(ALL) ALL

Graphical user interface, text

Description automatically generated



* Unfortunately, the server was not running any SQL database software to infiltrate and the website URLs were not active so no SQL injection or cross-site scripting attacks would work against the website outside of this attack.

Text

Description automatically generated

* Finally, we ransomed the index.html file of the user’s website, changed the motd file to give a made up email address to team for them to “pay the ransom” by sending an email saying that they are paying
  + Command: gpg -c index.html
  + Purpose: To deny access to the webpage and test to see if they have a backup of their web page files

A picture containing graphical user interface

Description automatically generated