



Andree Salvo

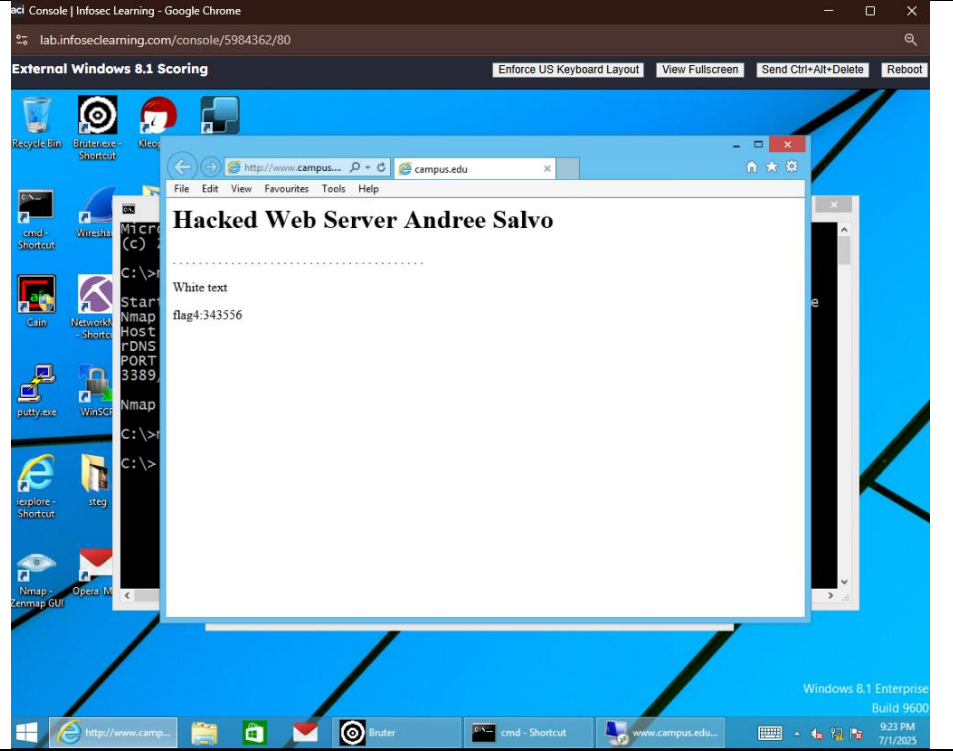
Southern New Hampshire University

CYB 240-13711

2-3 Lab Worksheet

Instructor: Brian Remson

Lab: Attacking Webservers From the WAN

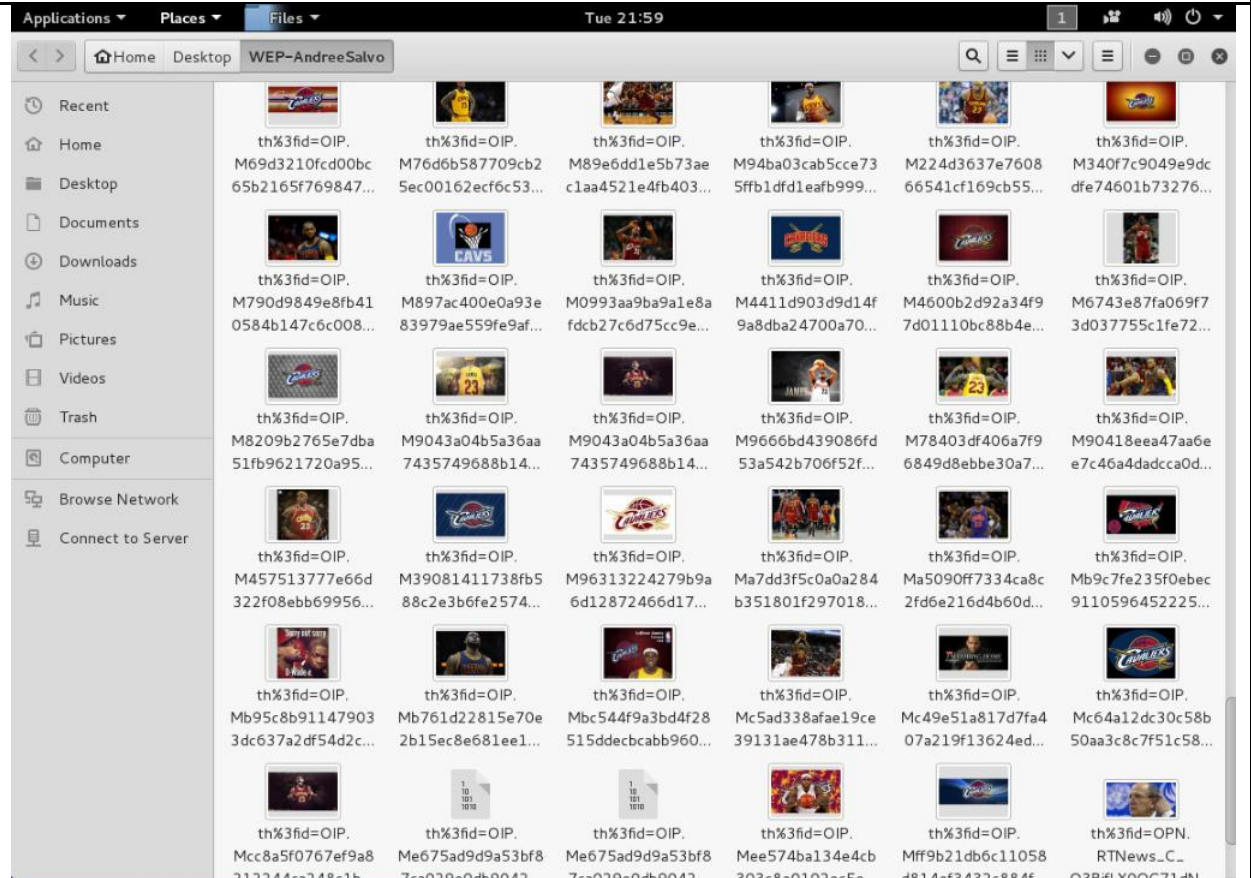
Prompt	Response
<p>In the lab section “Altering the Website,” Step 25, when you type “Hacked Web Server” include your name after the text “Web Server” and provide a screenshot of Step 24.</p>	
<p>In the lab, you covered up the tracking of access to the log files by deleting lines within the Access.log file. What other types of controls could be put in place to identify that these changes occurred? What other types of security measures could be put in place to help secure the web server?</p>	<p>Types of controls:</p> <ul style="list-style-type: none">✓ Audit logging✓ File integrity monitoring✓ Log storage <p>Types of security measures:</p> <ul style="list-style-type: none">✓ HTTPS encryption✓ WAF and Firewall✓ Least privilege

Lab: Breaking WEP and WPA and Decrypting the Traffic

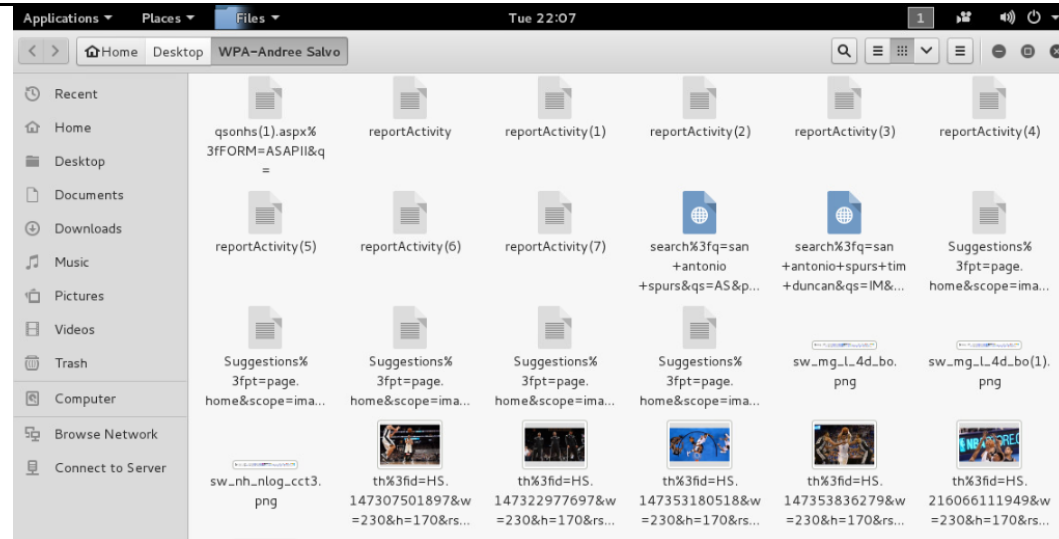
Prompt

In the lab section “Cracking WEP,” **Step 34**, instead of typing WEP, use *WEP-YOURNAME* (for example: WEP-NEOANDERSON) as the name for the file. Provide a screenshot of Step 37 before clicking “next.”

Response



In the lab section “Cracking WPA,” **Step 20**, instead of typing WPA, use *WPA-YOURNAME* (for example: WPA-NEOANDERSON) as the name for the file. Provide a screenshot of Step 24 before clicking “next.”



WEP and WPA are considered weak encryption protocols. What has been done to upgrade and make the protocols more secure?

They improved the protocols by rolling out WPA2 and WPA3 through the Wi-Fi Alliance, which made wireless networks way more secure compared to the older versions.