1. The IT admins at 04-721 Industries Ltd have deployed a new server on the 10.48.0.10-99 subnet reserved for lab systems. In their wisdom, the admins configured the firewall to block inbound connections from the untrusted VPN subnet (10.48.0.100-255) to this server. Identify this server (by IP and hostname) and at least four of the TCP application versions running on it. You may not install any new programs on any lab system for this assignment.   (8 points)
2. Sometimes a software exploit is not needed at all for attackers to compromise systems and cause serious financial loses. Based on your reading of the [Silent Starling: BEC to VEC—The Emergence of Vendor Email Compromise](https://canvas.cmu.edu/courses/36020/files/9760904)[Links to an external site.](https://www.agari.com/email-security-blog/silent-starling-vendor-email-compromise)article, what defensive measures and detection techniques would you propose to mitigate this new threat?   (6 points)
3. You've successfully exploited the CVE-2012-1823 vulnerability on your Metasploitable machine and gained a reverse shell. However, the remote shell is running as the user www-data and you much rather be root. You notice the Metasploitable machine is running Ubuntu 8.04 with Linux kernel 2.6, which has several local privilege escalation vulnerabilities. How can you escalate your privileges from the www-data to the root user without valid credentials on the system?    (6 points)

Hint #1: You can use the searchsploit "Linux Kernel 2.6 Ubuntu 8 Privilege Escalation" command in Kali to search for compatible local privilege exploits in ExploitDB and their associated CVEs. The ExploitDB exploits are located in the /usr/share/exploitdb/exploits/linux/ directory on your Kali machine.

Hint #2: If you have a Meterpreter shell, you can background it and run another exploit against the same session on the target.

Sometimes a software exploit is not needed at all for attackers to compromise systems and cause serious financial loses. Based on your reading of the Silent Starling: BEC to VEC—The Emergence of Vendor Email Compromise, what defensive measures and detection techniques would you propose to mitigate this new threat?

Based on the reading of the document Silent Starling: BEC to VEC—The Emergence of Vendor Email Compromise, here are some proposed defensive measures and detection techniques to mitigate the threat of Vendor Email Compromise (VEC):

1. **Employee Education and Awareness:** Provide regular training to employees, particularly those in finance and accounts receivable departments, to educate them about the tactics and techniques used in VEC scams. This should include information on how to identify suspicious emails, recognize signs of phishing, and verify email sender identities before taking any action.
2. **Multi-Factor Authentication (MFA):** Implement MFA for email accounts and other critical systems to add an extra layer of security. This can help prevent unauthorized access even if account credentials are compromised.
3. **Robust Email Filtering:** Implement advanced email filtering solutions that can identify and block suspicious emails, including those with malicious attachments or links. These filters should also detect email spoofing or domain spoofing attempts.
4. **Domain Authentication and Protection:** Implement email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the authenticity of incoming emails. This helps detect and block spoofed emails.
5. **Email Banner Warning Systems:** Configure email systems to display warning banners or notifications for emails originating from external sources, especially those considered high-risk or from unknown senders. This helps raise awareness and caution when interacting with such emails.
6. **Suspicious Activity Monitoring:** Deploy monitoring systems that can detect unauthorized access attempts, unusual login activities, or suspicious behavior within email accounts. This can help identify compromised accounts early.
7. **Vendor Verification:** Develop a process for verifying the legitimacy of new vendors or suppliers before engaging in financial transactions. This may involve performing background checks, conducting site visits, or using trusted third-party platforms for verification.
8. **Invoice Verification:** Establish strict procedures for verifying the authenticity of invoices, especially for large payments or changes in payment details. This can include confirming invoice details through known contact information, independently verifying bank account information, or cross-checking with internal records.
9. **Timely Security Updates and Patch Management:** Regularly update and patch all software and systems to protect against known vulnerabilities that could be exploited by attackers.
10. **Incident Response Plan:** Develop and regularly test an incident response plan that outlines the steps to be taken in the event of a VEC attack. This should include procedures for quickly identifying and isolating compromised accounts, notifying relevant parties, and recovering any lost funds.

It is important to note that these measures should be implemented as part of a comprehensive security strategy that includes regular security awareness training, continuous monitoring, and ongoing evaluation and improvement of security controls.