Computer Security Week 9

Khaula Molapo

1.

If I were setting up network security for a cloud platform, I'd start by protecting every part of the system from outside and inside threats. First, I'd install strong firewalls that check all incoming and outgoing traffic, making sure only allowed connections go through. I'd separate users, servers, and databases into different security zones so that one breach doesn't spread everywhere. I'd also set up an intrusion detection and prevention system to monitor suspicious activity in real time. All stored and transferred data would be encrypted, and I'd make two-factor authentication a must for every login. Regular software updates would fix any new vulnerabilities, and backups would be stored safely off-site. I'd also create security logs to track who accesses what and when. The main goal of this setup is to keep the system stable, protect user information, and ensure that even if one defense fails, there's always another layer to keep everything safe.

2.

Next-generation firewalls, or NGFWs, are advanced firewalls that go beyond simple filtering of ports and IP addresses. They can inspect actual data packets deeply, detect malware, and block unsafe websites or suspicious activities. NGFWs can also recognize specific apps, like Facebook or Dropbox, and control how users interact with them. They combine multiple tools like intrusion prevention, antivirus scanning, and web filtering into one single system. This makes them more powerful and easier to manage than using several different tools. They're great for stopping modern cyberattacks that use hidden or encrypted methods. Overall, next-generation firewalls give much better visibility, smarter control, and stronger protection for both business and cloud environments that rely on secure, constant connectivity.

3.

When I configure OpenVPN in VirtualBox, I install it on both the client and the server machines. Then I generate certificates and encryption keys to make sure the connection is secure. I edit the server configuration file to define IP ranges, ports, and authentication methods, then connect the client using its profile. Once it’s up, all the network traffic is safely encrypted and passes through a secure tunnel between the two machines. This setup makes it nearly impossible for hackers to read or steal data. It’s especially helpful when using public Wi-Fi or remote access connections. Working with OpenVPN also helps me understand how virtual private networks keep businesses connected safely across different systems and countries.

4.

If I were creating a network security policy, I’d make sure it’s simple enough for everyone in the company to understand and follow. It would include strong password requirements, access levels for each employee, software update schedules, and data handling rules. The policy would also explain what to do in case of a security breach or suspicious activity. Personal devices would have limited access, and everyone would need to go through basic security training. The main purpose is to make sure everyone knows their responsibility in protecting company data. This reduces mistakes, keeps hackers out, and ensures the system stays safe, private, and reliable for both the users and the organization as a whole.