

Date: July 3, 2024	Entry # 2
Description	<p><b>Detection &amp; Analysis:</b> Using the Nessus vulnerability scanner tool, it found a few critical areas the computer can be exploited by simply browsing the web.</p> <p><b>Recovery:</b> The company had to fix the SSL signing pof their website to make sure that any data sent back and forth through the TLS protocol is encrypted and can not be altered.</p>
Tools	Nessus Vulnerability Scanner, Virtual Machines,
5 W's	<p><b>Who:</b> A group of unethical hackers</p> <p><b>What:</b> A Backdoor exists within the website Domain</p> <p><b>Where:</b> Amazon</p> <p><b>When:</b> July 3, 2024 at 12:00 PM</p> <p><b>Why:</b> Our current website does not have any signed certificates, which means all customers who use the website to purchase goods can have their information taken by anyone who uses the exploit. Any unethical hacker can go through the website and see the connections of millions of people and checking information such as their banking credentials.</p>
Risk Analysis & Solutions	<p>The company must not risk a data breach otherwise it will face a heavy fine. I recommend the company sign an Extended validation certificate to authenticate every user is who they say they are. This gets rid of the possibility that an imposter is posing as another customer. If the company is using a Cloud provider to expand services, then they must be asked to update the WHOIS records and generate Signin requests.</p>

## Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

## Controls assessment checklist

Control:

Least Privilege (NO)

Disaster recovery plans (Yes)  
Password policies (YES)  
Separation of duties (YES)  
Firewall (YES)  
Intrusion detection system (IDS) (NO)  
Backups (YES)  
Antivirus software (NO)  
Manual monitoring, maintenance, and intervention for legacy (YES)  
Systems (YES)  
Encryption (NO)  
Password management system (YES)  
Locks (offices, storefront, warehouse) (NO)  
Closed-circuit television (CCTV) surveillance (NO)