CHIPPY'S CORNER RISK ASSESSMENT

AGENDA

INTRODUCTION

RISK ASSESSMENT SUMMARY

KEY FINDINGS

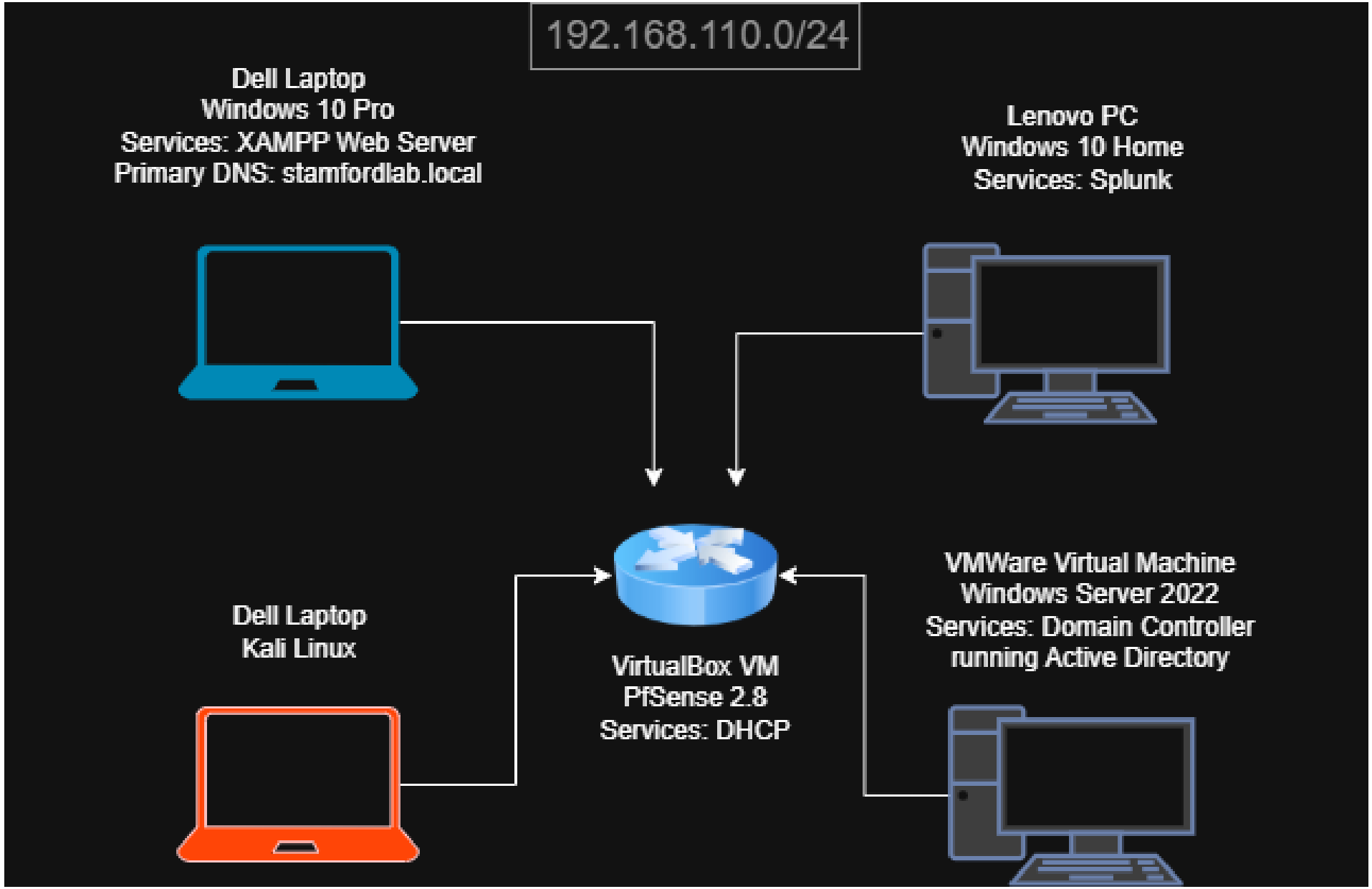
RECOMMENDATIONS

CONCLUSION

INTRODUCTION

PURPOSE & SCOPE

- To ensure the business continuity of Chippy's Corner, the organization has decided to conduct a risk assessment on the subnet used by the staff.
- The scope of the assessment includes an internal web server, a pfSense router, a Domain Controller, and a windows 10 endpoint used by the boss of the staff.
- The staff network range is 192.168.110.0/24


192.168.110.0/24
Dell Laptop
Windows 10 Pro
Services: XAMPP Web Server
Primary DNS: stamfordlab.local
Lenovo PC
Windows 10 Home
Services: Splunk
Dell Laptop
Kali Linux
VirtualBox VM
PfSense 2.8
Services: DHCP
VMWare Virtual Machine
Windows Server 2022
Services: Domain Controller
running Active Directory

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

- The overall risk posture of the organization is **critical**
- There are multiple critical vulnerabilities within the infrastructure that, if exploited, can lead to dire outcomes
- Outcomes include, but are not limited to, remote exploitation, lateral movement, account compromise, domain compromise, and data theft.

KEY FINDINGS

KEY FINDING #1

- The web application used by developers on the network as a ping tool leads to a potential remote code execution of the host OS of the web server.

- Unsanitized input from the text box allows other commands outside of ping to be executed through command chaining.

index.php - Notepad

File Edit Format View Help

```
<!DOCTYPE html>
<html>
<head>

        <title>Ping Tool</title>

</head>

<body>

        <h1>Ping Tool For Developers</h1>

        <form method="GET">
                <input type="text" name="ip" placeholder="Enter IP">
                <input type="submit" value="Ping">
        </form>

        <pre>

        <?php
        if (isset($_GET['ip'])){
                $ip = $_GET['ip'];
                $output = shell_exec("powershell -Command \"ping -n 3 . $ip\"");
                echo $output;
                }

        ?>
        </pre>

</body>


</html>
```

KEY FINDING #2

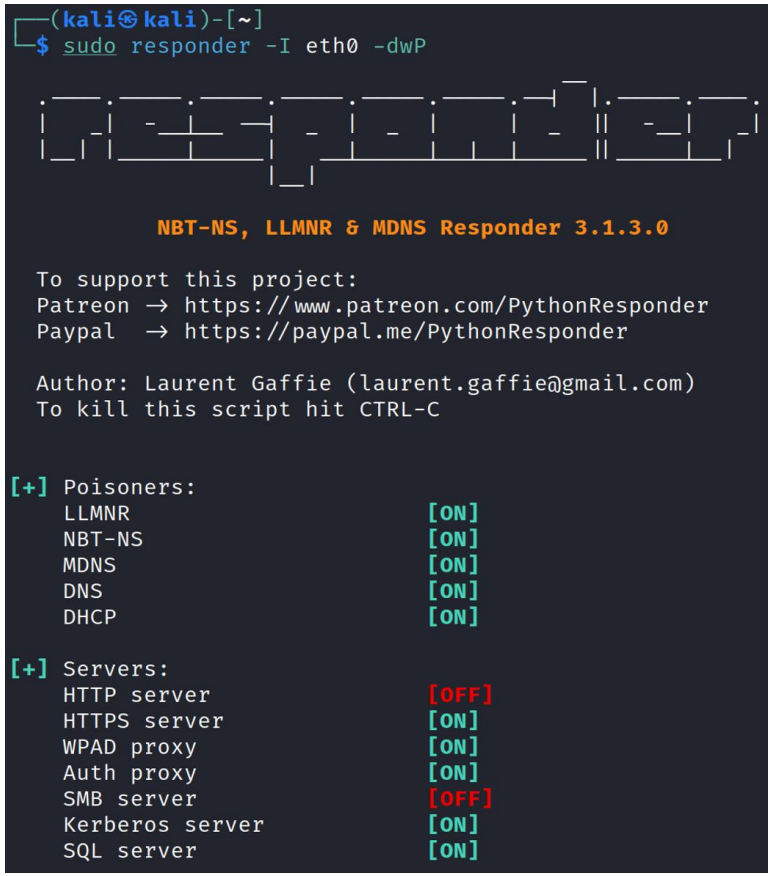
Services such as SysInternals suite, Python and ports such as Server Message Block (SMB) are enabled and installed on the web server host OS.

Attackers can use services such as PsExec (which uses SMB) in order to laterally move into other endpoints on the network after gaining initial foothold on the web server.

KEY FINDING #3

- Lenient outbound traffic rules on each host within the networks allow for each host to connect outwards to any service trying to reach the endpoint

- Mix this with Link-Local Multicast Name Resolution (LLMNR) enabled on the boss's endpoint can allow for attackers to steal hashes.



KEY FINDING #4

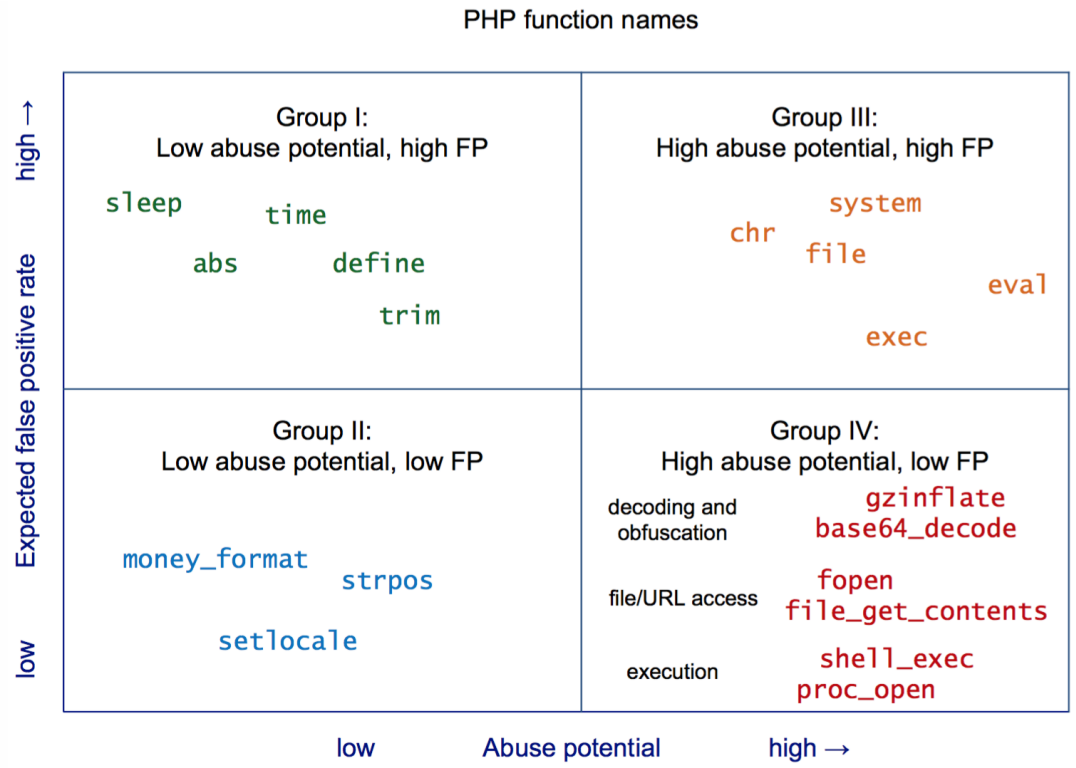
The boss's workstation utilizes a weak password for authentication

The password is a password commonly found in common password lists such as ROCKYOU.TXT

With a password based SSH login enabled on the Boss's machine, attackers can easily brute force the remote login and gain easy access.

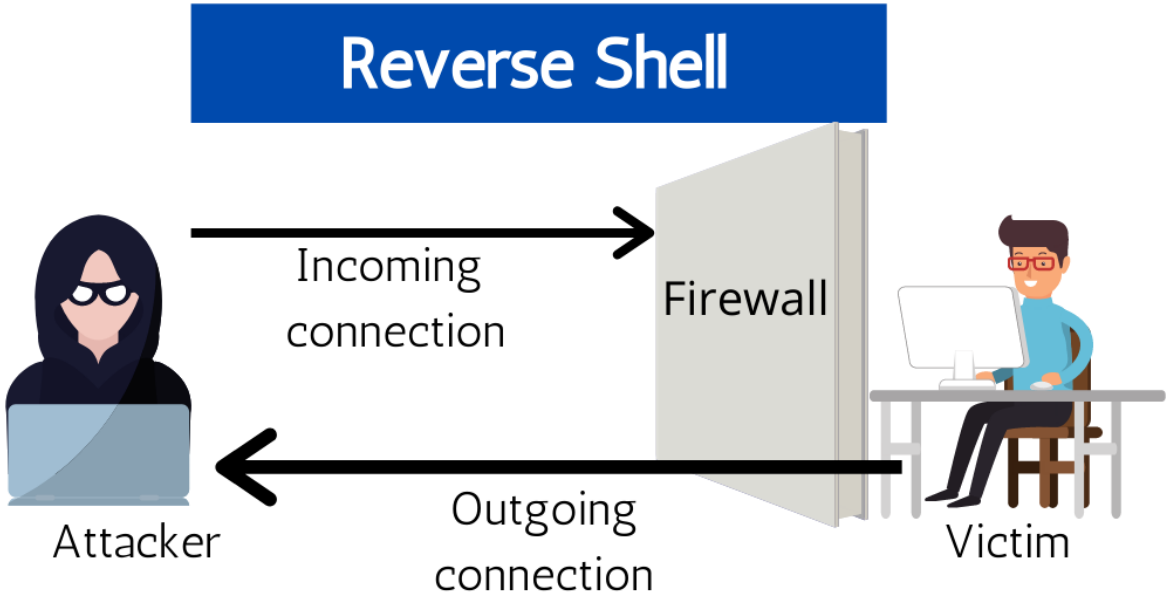
RECOMMENDATIONS

APPLICATION HARDENING



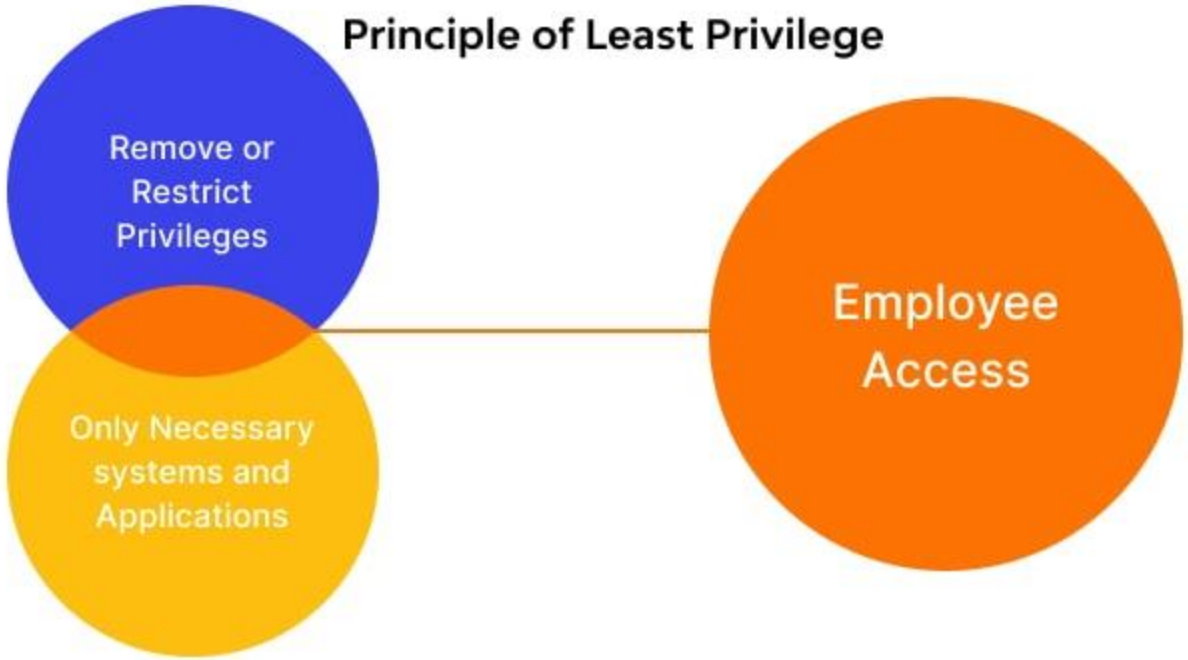
- Sanitize PHP input to prevent code injection.
- Disable dangerous functions in PHP configuration.

ENDPOINT & NETWORK CONTROLS



- Disable LLMNR to prevent credential theft
- Restrict outbound traffic to only business-approved destinations to prevent reverse shells
- Remove unnecessary services and tools from production servers and endpoints

ACCESS CONTROLS & LATERAL MOVEMENT



- Monitor/remove remote admin tools like PsExec and SSH where not required.
- Enforce least privilege access for administrative accounts.

CONCLUSION

FINAL TAKEAWAYS

After the risk assessment, 4 critical risks could allow attackers to compromise the domain easily

Immediate mitigations that can drastically improve the security posture are simple and quick