LIFARS
your digital world, secured

Case Study–
OWA and O365 hacking

LIFARS regularly conducts penetration tests to ensure the effectiveness of the security measures of our clients maintain strong and can uphold to real world scenarios. Our cyber resiliency experts deliver calculated attacks against systems the same way black hat hackers.

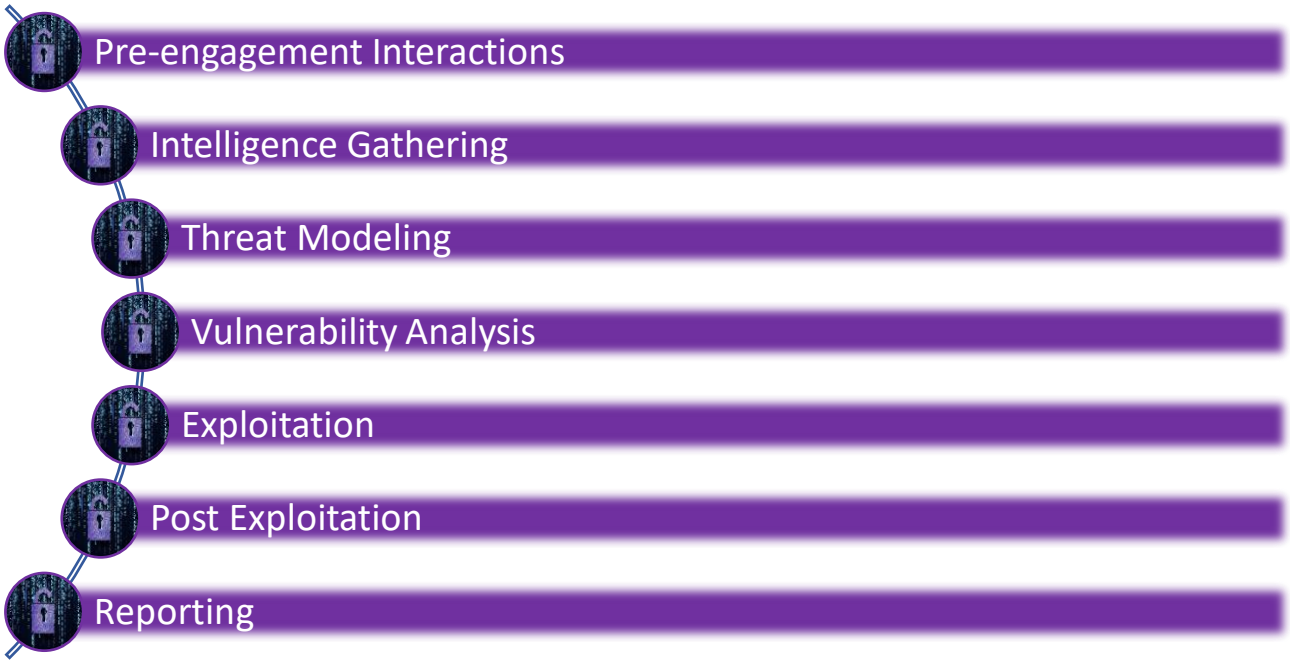
In December, our client requested that LIFARS Pen Testing Team perform an external black box penetration test as part of a due diligence exercise. The client, a medium sized organization with over 1000 employees and 200 IPv4 addresses, understands the risks they face on a daily basis and the importance of meeting compliance standards. Therefore, this client requested an external black box penetration test on their network.

The intent of this assessment was to identify weaknesses in the company internet facing infrastructure and to detail how these vulnerabilities could impact the organization. Therefore, the team used Outlook Web Application (OWA) and Office 365 (O365) as main targets for user enumeration and password spraying. Main emphasis was focused on weak integration of security measures between OWA and O365. The black box testing, as an unauthenticated user for OWA and O365, and its assessment was led in a manner that simulated a malicious actor engaged in a targeted attack against the company's external internet facing network. This security testing effort was conducted with emphasis on the actual state of the systems examined and no documentation to the client was provided.

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

PENETRATION TESTING PHASES

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



KEY FINDINGS

While conducting the pen test, we discovered that the Microsoft Exchange Client Access Server (CAS) was affected by an information disclosure vulnerability. A remote, unauthenticated attacker could exploit this vulnerability to obtain information such as enumerating Outlook Web Access user accounts using password spraying. Therefore, we decided to use OWA to gain access to domain user credentials without getting on the organization's network.

We decided to use a time-delay based enumeration attack on the OWA interface. Essentially, password spraying or a series of password attacks on the portal was administered. Input for this attack includes OSINT data like first and last names of employees. The request time is lowered if existing users are found. If users do not exist, the request time increases significantly. You can see 20 requests, 14 of them have average time 3620ms and other 6 have 200ms. You can tell that probably the one with 200ms is valid because is found (faster) than average request time. As this is time-based enumeration, we are looked for differences between requests in time which we have received response from server.

We were then able to **acquire more than 1,000 company domain user accounts** using time-based enumeration (figure 1)

Request	Payload	Status	Respo...	Error	Timeout	Length
0		302	180	☐	☐	633
15	[redacted]	302	206	☐	☐	633
4	[redacted]	302	207	☐	☐	633
10	[redacted]	302	208	☐	☐	633
5	[redacted]	302	209	☐	☐	633
3	[redacted]	302	229	☐	☐	633
37	[redacted]	302	3621	☐	☐	633
75	[redacted]	302	3621	☐	☐	633
67	[redacted]	302	3622	☐	☐	633
113	[redacted]	302	3622	☐	☐	633
146	[redacted]	302	3623	☐	☐	633
124	[redacted]	302	3624	☐	☐	633
156	[redacted]	302	3624	☐	☐	633
60	[redacted]	302	3625	☐	☐	633
71	[redacted]	302	3625	☐	☐	633
100	[redacted]	302	3625	☐	☐	633
102	[redacted]	302	3625	☐	☐	633
154	[redacted]	302	3625	☐	☐	633
41	[redacted]	302	3626	☐	☐	633
48	[redacted]	302	3626	☐	☐	633

Figure 1 Time based user enumeration

After enumeration we ran brute force and **successfully compromised email accounts** (figure 2).

Request	Payload	Status	Respo...	Error	Timeout	Length	Comment
1	[redacted]	302	3651	☐	☐	633	
15	[redacted]	200	694	☐	☐	23132	
1010	[redacted]	302	298	☐	☐	633	
1012	[redacted]	302	280	☐	☐	633	
1011	[redacted]	302	275	☐	☐	633	
390	[redacted]	302	261	☐	☐	633	
95	[redacted]	302	247	☐	☐	633	
1001	[redacted]	302	244	☐	☐	633	
1035	[redacted]	302	243	☐	☐	633	

Figure 2 Brute forcing accounts after enumeration phase

At this stage, we enumerated accounts to the local domain. After brute forcing the user account, we tried to sign in.

Figure 3 OWA log-in redirect

We were then redirected to MS O365. For a successful login we had to change the format of the login, from domain account to email address.

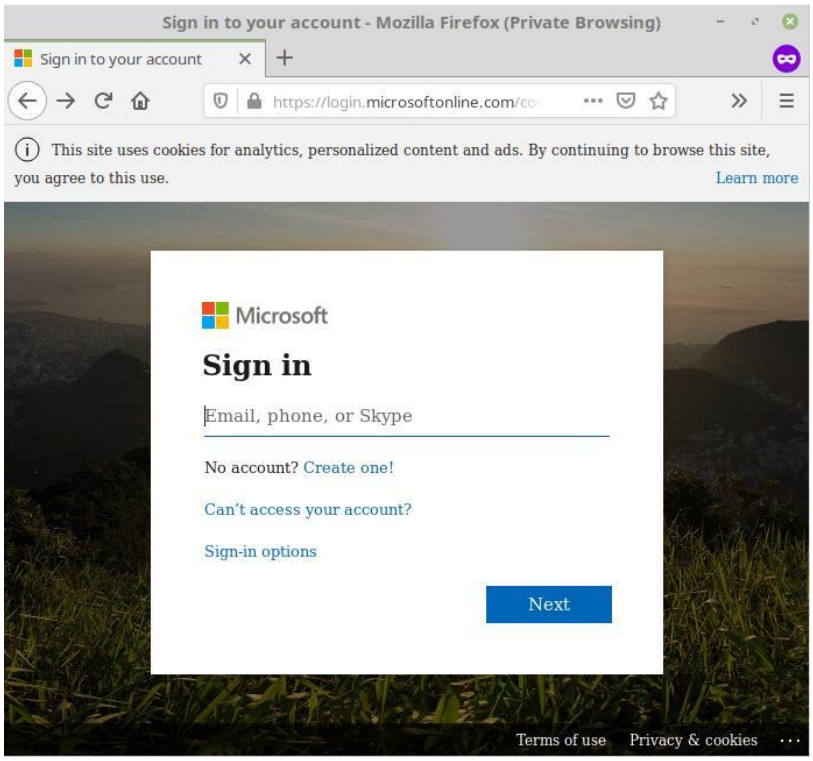


Figure 4 redirection to a new webpage

After logging in, we got access to the mailbox as a company employee.

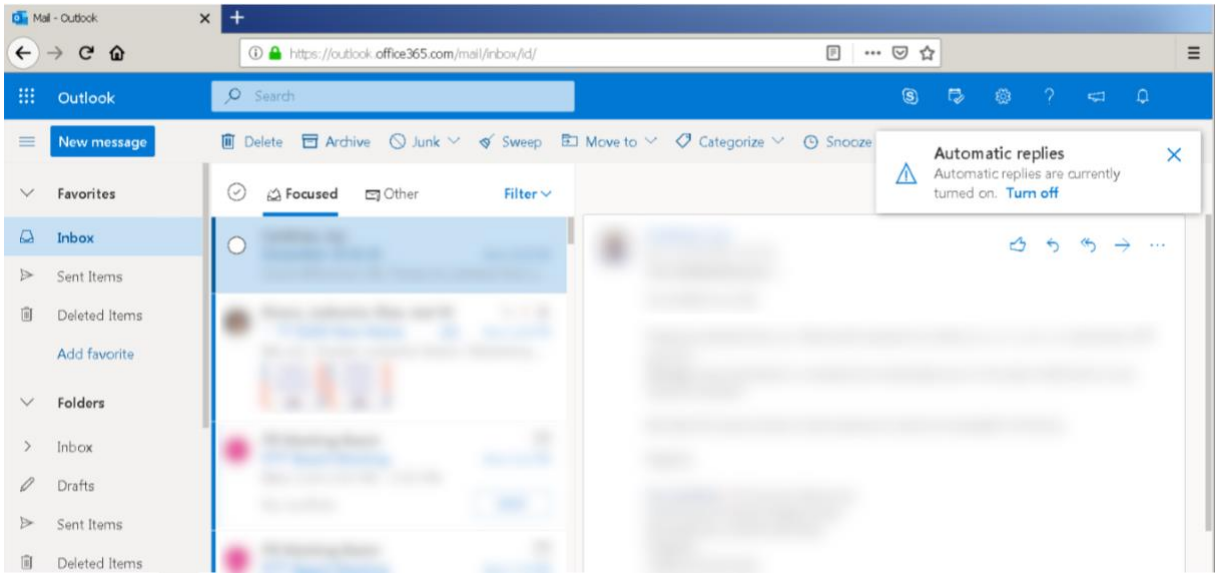


Figure 5 Outlook succesful login

We then managed to dump a list of emails that could help us in targeted attacks, like spear phishing.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extensio
399	https://outlook.office365.com	POST	/search/api/v1/suggestions?&n=47&cv=ucjZY...	✓		200	226619	JSON	
1582	https://outlook.office365.com	POST	/search/api/v1/suggestions?&n=49&cv=jMkX...	✓		200	226617	JSON	
2357	https://outlook.office365.com	POST	/search/api/v1/suggestions?&n=51&cv=m44y...	✓		200	226619	JSON	
2378	https://outlook.office365.com	POST	/owa/service.svc?action=FindPeople&EP=1&...	✓		200	106931	JSON	svc
2669	https://outlook.office365.com	POST	/owa/service.svc?action=FindPeople&EP=1&...	✓		200	106935	JSON	svc

Figure 6 dumping MS O365 email list of all users

CONCLUSION

Our approach to this pen test we proved enumeration to obtain local domain accounts through OWA is possible. However, login to OWA redirected us to the login Office 365 portal, where it was necessary to login by email. After successfully compromising the Office 365 portal, we managed to obtain a complete email list of Office 365 users. This allowed us to launch a phishing campaign to other targeted data abuse attacks.

REPORTING

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