Penetration Test Report

Internal IT

of Dubius Payment Ltd.

EXAMPLE

June 6, 2024

v1.1

Contents

i List of changes

Version	Description	Author	Date
1.0	Report generation	Dominik Sauer	June 5, 2024
1.1	Quality Assurance	QA-Team	June 6, 2024

1 Contact persons

1.1 Contact person Dubius Payment Ltd.

Damian Westcott
CEO

🖂 d.westcott@dubius-payment.com

Dubius Payment Ltd.
71 Peachfield Road
SO53 4NE CHANDLER
United States

1.2 Contact person binsec GmbH

Dominik Sauer
Head of Penetration Testing

☎ +49 69247560713
🖂 ds@binsec.com

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

1.3 About the pentester

Since 2013, Mr. Dominik Sauer has been responsible for the management and implementation of penetration tests at binsec GmbH. He started his career while studying computer science at the Darmstadt University of Applied Sciences and ended his academic career with a very good master's degree in computer science with a specialization in IT security. He also holds the leading certifications in the field of penetration testing and has been an Offensive Security Certified Professional (OSCP) since 2013 and an Offensive Security Certified Expert (OSCE) since 2015.

In addition, he has been a lecturer for teaching at the Darmstadt University of Applied Sciences (HDA) and the TH Mittelhessen University of Applied Sciences (THM) since 2017. For example, he holds courses on penetration testing or digital forensics and supervises theses.

2 Project overview

2.1 Introduction

Dubius Payment Ltd. is operating a payment application that stores, processes and forwards credit card information. The company is thus subject to the security standard of the credit card industry, the PCI DSS (Payment Card Industry Data Security Standard). In requirement category 11, the PCI DSS requires the implementation of application-level and network-level penetration tests. In this context, the network level penetration test comprises both an external and internal test inside the network. These tests must be performed annually or following significant changes.

2.2 Basic conditions

The penetration test was conducted between June 5, 2024 and June 7, 2024 performed as an internal grey box test, without using aggressive attacking techniques such as DDoS attacks. The complete classification is illustrated in chapter 5.1. The general pentest approach is described in chapter 5.2.

2.3 Scope

In detail, the IT systems of the domain 'dubius-payment.com' were checked for vulnerabilities, which were located in the following private IPv4 network areas:

- 10.250.53.0/24 (DMZ)
- 10.247.97.0/24 (Management)
- 10.250.229.0/24 (Client)

2.4 Performed tests

The following pentest tasks were performed on the systems and applications described previously. This list was automatically generated by binsec GmbH's documentation tool.

Target → Active Directory: Dubius

Result	Task: Configuration management	Findings
✘	Verification whether SMB signing has been activated	Page 12

Result	Task: Vulnerability identification	Findings
✔	Is the domain controller vulnerable to already published vulnerabilities?	-

Result	Task: Vulnerability identification (without credentials)	Findings
✔	Manual and automated AD enumeration	-
✔	NTLM-Relay to LDAP(S) (LDAP Signing and Channel Binding)	-
✔	Check for use of leaked credentials	-
✔	Extract AD credentials from network printers	-
✔	Capturing usernames and hashes via network poisoning	-
✔	Checking whether the creation of computer objects can be forced to gain initial access	-
✔	Checking whether a computer object can be created and access delegated	-
✘	Checking whether valid login data can be guessed via password spraying or bruteforce	Page 14
✔	Checking if it's possible to spoof WSUS	-
✔	Capturing credentials from unencrypted network traffic	-

Result	Task: Vulnerability identification (with credentials)	Findings
✔	Checking for misconfigured ADCS templates	-
✔	Checking wether passwords can be found in description fields of AD users	-
✘	Search file shares for credentials	Page 15
✔	Checking whether sensitive data is exposed in group policy preferences (gpp)	-
✔	Password hash extraction (Kerberoasting)	-

Result	Task: Privilege Escalation	Findings
✘	Dumping local hashes and cached passwords	Page 14

Target → Network: Internal IT · DNS: DNS (tcp/53)

Result	Task: Information gathering	Findings
✔	Identification of the stored DNS entries	-

Result	Task: Configuration management	Findings
✔	Check whether a zone transfer can be performed	-

Result	Task: Vulnerability identification	Findings
✔	Check whether vulnerabilities are known for the software version of the DNS server	-

Target → Network: Internal IT · FTP: FTP (tcp/21)

Result	Task: Configuration management	Findings
✔	Does the FTP server support anonymous login?	-

Result	Task: Secure data transmission	Findings
✔	Check whether sensitive data is transmitted in plain text	-

Result	Task: Vulnerability identification	Findings
✔	Check whether vulnerabilities are known for the software version	-

Target → Network: Internal IT · HTTP: HTTP (tcp/80)

Result	Task: HTTP Check	Findings
✔	Information gathering (active, test objects)	-
✘	Secure data transmission	Page 17

Target → Network: Internal IT · HTTPS: HTTPS (tcp/443)

Result	Task: HTTPS Check	Findings
✔	Information gathering (active, test objects)	-
✔	Authentication testing of access controls	-
✔	Input validation (e.g. Injection, XSS)	-

Target → Network: Internal IT · IPMI: IPMI (udp/623)

Result	Task: Configuration management	Findings
✔	Checking whether the server can be accessed via the IPMI interface without user authentication	-

Result	Task: Vulnerability identification	Findings

✔	Checking whether the authentication can be bypassed via Cipher Suite Zero	-
✔	Checking whether password hashes for system users can be queried externally	-

Target → Network: Internal IT · LDAP: LDAP, LDAPS (tcp/389, tcp/636)

Result	Task: Information gathering	Findings
✔	Information gathering without access data	-
Result	Task: Secure data transmission	Findings
✔	Check whether sensitive data is transmitted in plain text	-

Target → Network: Internal IT · MySQL / MariaDB: MYSQL (tcp/3306)

Result	Task: Configuration management	Findings
✔	Checking whether a database connection can be established without user authentication	-
Result	Task: Vulnerability identification	Findings
✔	Check whether vulnerabilities are known for the software version	-

Target → Network: Internal IT · NTP: NTP (udp/123)

Result	Task: Information gathering	Findings
✔	Checking whether NTP commands for information retrieval have been disabled.	-
Result	Task: Configuration management	Findings
✔	Checking whether the NTP server can be abused as part of a DDoS attack	-
Result	Task: Vulnerability identification	Findings
✔	Check whether vulnerabilities are known for the software version	-

Target → Network: Internal IT · RDP: RDP (tcp/3389)

Result	Task: Information gathering	Findings
✔	Identification of the operating system via an RDP connection	-
Result	Task: Vulnerability identification	Findings
✔	Verification that the RDP server has been patched against known vulnerabilities	-

Target → Network: Internal IT · RPC: RPC (tcp/139)

Result	Task: Information gathering	Findings
✔	Can remote procedure calls be executed without user authentication?	-

Target → Network: Internal IT · SMB: SMB (tcp/445)

Result	Task: Information gathering	Findings
✘	Identification of accessible SMB network shares without user authentication	Page 15

Result	Task: Vulnerability identification	Findings
✔	Verification that the SMB server has been patched against known vulnerabilities	-

Target → Network: Internal IT · SMTP: SMTP (tcp/25)

Result	Task: Information gathering	Findings
✔	Check whether SMTP commands for information retrieval have been disabled	-

Result	Task: Configuration management	Findings
✔	Check whether mails can be sent via the SMTP server to external people with a company-internal e-mail address (Open-Relay)	-
✔	Check whether fake e-mails with a company-internal sender address can be sent to employees?	-

Result	Task: Vulnerability identification	Findings
✔	Check whether vulnerabilities are known for the software version	-

Target → Network: Internal IT · SNMP: SNMP (udp/161)

Result	Task: Configuration management	Findings
✘	Can system information be extracted due to the use of outdated SNMP protocols?	Page 18

Target → Network: Internal IT · SSH: SSH (tcp/22)

Result	Task: Configuration management	Findings
✔	Check whether an outdated SSH protocol version is supported	-

Result	Task: Vulnerability identification	Findings
✔	Check whether vulnerabilities are known for the software version	-

Target → Network: Internal IT · Telnet: TELNET (tcp/23)

Result	Task: Configuration management	Findings
✔	Can the IT system be accessed via Telnet?	-

Result	Task: Vulnerability identification	Findings
✔	Checking whether the user authentication can be bypassed	-

3 Management overview

3.1 Summary

The penetration test was conducted between June 5, 2024 and June 7, 2024. During it 14 vulnerabilities were identified which were combined into 5 findings and subjected to an initial risk assessment. As result there are 3 findings that require immediate action and one finding that requires action. The finding of category note is to be understood as a suggestion to increase the security level.

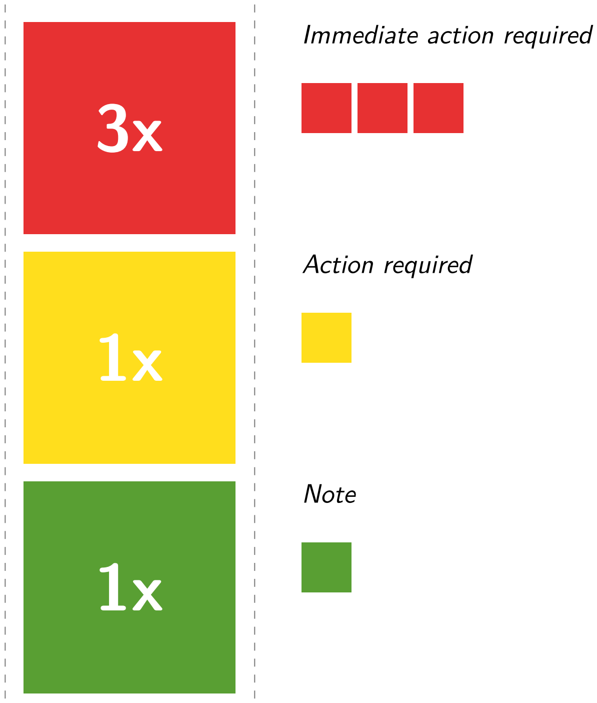


Fig. Risk Overview of Findings

During the penetration test, several critical vulnerabilities were identified, which could be used to compromise all internal IT systems in the 'Dubius' domain. For example, administrative access can be gained through weak user passwords or due to a lack of Active Directory security. All critical vulnerabilities should be fixed immediately.

3.2 List of findings

# 1	🟥 ⬜ ⬜	Not fixed: *Misconfiguration* All IT systems in the internal domain can be compromised due to a missing security feature on the SMB server. See page 12. System: SMB
# 2	🟥 ⬜ ⬜	Not fixed: *Access Control* IT systems can be accessed due to the use of weak user passwords. See page 14. System: Domain Controller
# 3	🟥 ⬜ ⬜	Not fixed: *Access Control* Due to an incorrect authorization, files of other domain users can be accessed via the network shares. See page 15. System: 10.247.97.204, 10.247.97.210, 10.247.97.212
# 4	⬜ 🟨 ⬜	Not fixed: *Data Transmission* The access data of several services and applications are transmitted in clear text. See page 17. System: e.g. 10.247.97.56, 10.247.97.57, 10.247.97.58 (total of 5)
# 5	⬜ ⬜ 🟩	Not fixed: *Misconfiguration* System information such as network configuration can be extracted due to a missing user authentication. See page 18. System: e.g. 10.247.97.174, 10.247.97.190, 10.247.97.201 (total of 4)

4 Technical report

4.1 Missing SMB signing

🟥 immediate action required
⬜ Damage: critical
⬜ Occurrence: medium

Finding #1 Not fixed

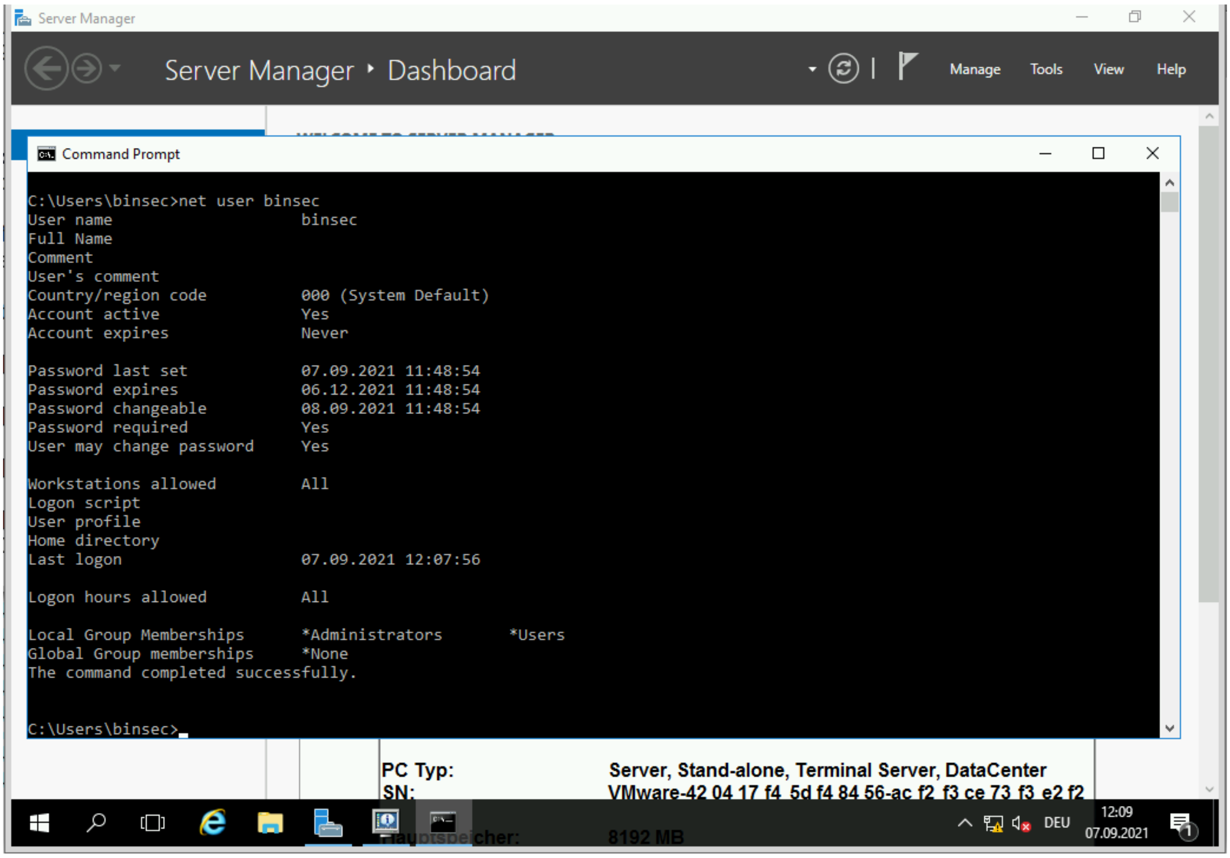
Dubius Payment Ltd. uses SMB to exchange data between heterogeneous systems, as can be seen in the following port scan:

```
Nmap scan report for 10.247.97.142
Host is up (0.0013s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

Windows has implemented a single sign-on for user authentication on the network shares, whereby clients send an NTLM hash over the network as proof of identity. Since the NTLM hashes are not digitally signed by their owners, the NTLM hashes can be intercepted by an attacker in a local network and forwarded to the target system:

```
[HTTP] NTLMv2 Username : Dubius\dpadmin
[HTTP] NTLMv2 Hash     : dpadmin::Dubius:41414141414141414141414141414141:4
    e51fb6e7ae458c248879791706e1023:0101000000000000a79bd1ebad701815cd4bb325b[...]
```

As a result, an attacker could successfully log on to a target system and execute system commands. During the penetration test it was possible to execute commands as an administrative user of the internal domain 'Dubius'. For example, the following screenshot shows the newly created domain admin 'binsec':



Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Command Prompt
PC Typ:
Server, Stand-alone, Terminal Server, DataCenter
SN:
VMware-42 04 17 f4 5d f4 84 56-ac f2 f3 ce 73 f3 e2 f2
8192 MB
DEU
12:09
07.09.2021

```
C:\Users\binsec>net user binsec
User name                    binsec
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            07.09.2021 11:48:54
Password expires             06.12.2021 11:48:54
Password changeable          08.09.2021 11:48:54
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   07.09.2021 12:07:56

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\binsec>_
```

Recommendation

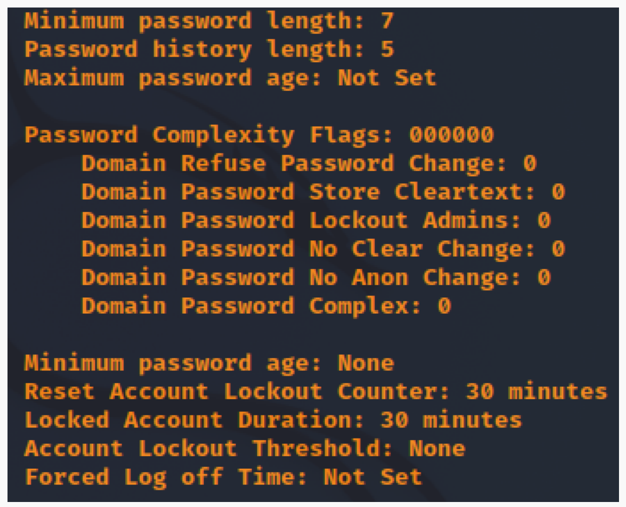
SMB signing should be activated for all IT systems in the domain using a group policy. In addition, the domain admin 'binsec' should be deleted.

4.2 Weak user passwords

🟥 immediate action required
⬜ Damage: critical
⬜ Occurrence: low

Finding #2 **Not fixed**

As can be seen from the following screenshot, a weak password policy is in place for the domain 'Dubius', which requires user passwords to contain only 7 characters:



```
Minimum password length: 7
Password history length: 5
Maximum password age: Not Set

Password Complexity Flags: 000000
    Domain Refuse Password Change: 0
    Domain Password Store Cleartext: 0
    Domain Password Lockout Admins: 0
    Domain Password No Clear Change: 0
    Domain Password No Anon Change: 0
    Domain Password Complex: 0

Minimum password age: None
Reset Account Lockout Counter: 30 minutes
Locked Account Duration: 30 minutes
Account Lockout Threshold: None
Forced Log off Time: Not Set
```

To identify weak passwords, the password hashes of all domain accounts were extracted on the domain controller '10.247.97.31'. The following list contains all user passwords that could be cracked within the time frame of the penetration test:

Username	Password	Note
Dubius\csimmons	Dubius2021!	domain admin
Dubius\pbaker	Chandler#1982	domain user
Dubius\rhobbes	Rylan_1234	domain user

Recommendation

All user passwords should be changed immediately after a strong password policy is enforced for all IT systems. In general, a password should be at least 12 characters long and contain a combination of lowercase and uppercase letters, numbers and special characters.

In addition to the password policy, a password policy enforcement solution could be used to check for dictionary entries, names and the presence of past password leaks when assigning passwords. In principle, words such as the company name in the password reduce the entropy of a password.

4.3 Insufficient authorization management for network shares

🟥 immediate action required

⬜ Damage: high

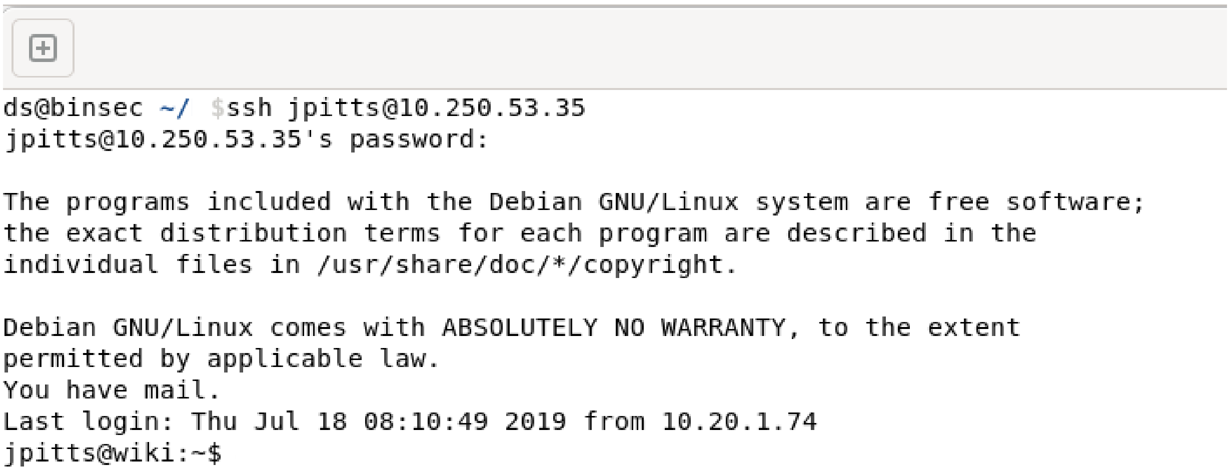
⬜ Occurrence: medium

Finding #3 **Not fixed**

The user accounts of the domain 'Dubius' with the group memberships 'Domain Users' and 'dubius-payment' have read and write access to the following network shares:

```
[+] IP: 10.247.97.204:445      Name: ad.dubius-payment.com
        Disk                                 Permissions     Comment
        ----                                 -----------     -------
        c$                                   READ ONLY
        home                                 READ, WRITE

 [+] IP: 10.247.97.210:445      Name: unknown
        Disk                                 Permissions     Comment
        ----                                 -----------     -------
        Backup                               READ ONLY

[+] IP: 10.247.97.212:445      Name: srv01.dubius-payment.com
        Disk                                 Permissions     Comment
        ----                                 -----------     -------
        McAfee                               READ ONLY
        NETLOGON                             READ ONLY
        SYSVOL                               READ ONLY
```

For example, credentials for the domain account 'Dubius\jpitts' could be extracted from cached Firefox profiles on the network share //10.247.97.204/home/. As a result, unprivileged domain users can change their user role:



```
ds@binsec ~/ $ssh jpitts@10.250.53.35
jpitts@10.250.53.35's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Thu Jul 18 08:10:49 2019 from 10.20.1.74
jpitts@wiki:~$
```

Recommendation

In consultation with Dubius Payment Ltd. unprivileged domain users should only be allowed to access the network share '//10.247.97.204/home'. As a result, the authorization management should be reviewed internally.

In addition, the IT system 10.247.97.204 is used as a file server but also as a domain controller. According to security best practices, only one function per server should be implemented. As a result, the file server should be operated on a dedicated IT system to reduce the attack surface on the domain controller.

4.4 Cleartext transmission of access data

■ action required
🟨 Damage: medium
■ Occurrence: medium

Finding #4 **Not fixed**

The credentials of the following services are transmitted in cleartext. Therefore, attackers can gain unauthorized data access if they intercept the network traffic:

Telnet (23/tcp)

- 10.247.97.56
- 10.247.97.57
- 10.247.97.58

HTTP (80/tcp)

- http://10.247.97.80
- http://10.247.97.81

Recommendation

The web applications should only be accessible via HTTPS and SSH should be used exclusively instead of Telnet.

4.5 Information gathering via outdated SNMP versions

⬜ note
⬜ Damage: warning
🟩 Occurrence: high

Finding #5 **Not fixed**

Network elements can be monitored and controlled from a central station using the Simple Network Management Protocol (SNMP). However, neither the SNMP version 'SNMPv1' nor 'SNMPv2' provides data encryption. In addition, system information can be extracted from the following IT systems using the community string public via 'SNMPv1' and 'SNMPv2':

- 10.247.97.174
- 10.247.97.190
- 10.247.97.201
- 10.247.97.235

The following listing shows the routing table of 10.247.97.174 as an example:

```
[+] Try to connect to 10.247.97.174 using SNMPv1 and community 'public'


[*] Routing information:

  Destination           Next hop            Mask                  Metric
  0.0.0.0               10.247.97.1        0.0.0.0               1

[...]
```

Recommendation

The SNMP versions 'SNMPv1' and 'SNMPv2c' should be deactivated and SNMPv3 should be used instead, which supports both data encryption and user authentication

5 Appendix A

5.1 Classification details

In cooperation with Dubius Payment Ltd., the following classification variant was agreed as the approach: The penetration test was performed as an internal grey box test, without using aggressive attacking techniques such as DDoS attacks.

Pursuant to the study “Implementation Concept for Penetration Tests“ by the German Federal Office for Information Security (BSI), binsec GmbH used the following classification for this penetration test:

Test Type	Black-Box	[✓ Grey-Box]	White-Box	
Aggressiveness	passive	cautious	[✓ calculated]	aggressive
Scope	full	[✓ limited]	focused	
Aproach	covert	[✓ overt]		
Technique	Internet	[✓ physical access]	Social engineering	
Starting Point	external	[✓ internal]		

5.2 Procedure for IT infrastructures

The exact course of a penetration test depends heavily on the specific services in an IT infrastructure. Nevertheless, the approach of a real attacker can be generalized. For example, the BSI (german Federal Office for Information Security) lists modules describing various intrusion attempts in its implementation concept for penetration tests. Based on the information from the BSI, the test method used by binsec GmbH is roughly divided into the 3 following test phases:

Identification of attack surface

- Evaluation of publicly available data
- Identification of services based on open ports via TCP and UDP
- Verification that access controls such as firewalls or network segmentation are in place

Checking for vulnerabilities

- Checking the patch statuses and the software versions used to ensure that they are up-to-date
- Checking the access restrictions of services
- Checking whether services have been set up according to security best practices

Exploitation

- Development of proof of concepts to exploit identified vulnerabilities
- Privilege escalation through the chaining of vulnerabilities

5.3 Procedure for Active Directoy

The test method used by binsec GmbH for an Active Directory (AD) is based on the fundamentals of 'IT-Grundschutz' from the German Federal Office for Information Security (BSI) and the CIS benchmarks (Center for Internet Security Benchmarks) for protecting IT systems and data from cyber attacks. The penetration test is usually carried out on the client's premises, which provides a physical access to the local network. In addition, the attacker perspective for the penetration test against an AD can vary:

- The attacker has gained physical access to the network and must gain initial access to the domain in the first step. For example, attack vectors such as man-in-the-middle attacks, password spraying or the identification of information leaks can be used to take over accounts of domain users.
- The attacker was able to compromise an AD user and gain initial access to the Active Directory (assumed breach). This scenario is comparable to unprivileged domain users who wants to extend their authorizations. Vulnerabilities such as the exploitation of misconfigurations and authorization flaws in AD and its services, as well as data analysis of network shares, are used for this purpose.
- The attacker has access to an administrator account of the domain and has internal knowledge of the local IT infrastructure (e.g. former IT employee). For example, the password hashes of all users can be extracted as a domain admin in order to identify weak passwords and check the effectiveness of the password policy.

The methodical test approach of binsec GmbH is roughly divided into the following 3 test phases:

1. Identification of vulnerabilities (without access data)
    - OSINT analysis (Open Source Intelligence) such as the query of access data in data leaks
    - Manual and automatic AD enumeration
    - Check for the use of outdated operating systems and software
    - Check whether hardening measures are in place to protect against man-in-the-middle attacks
    - Extraction of access data and password hashes in services
    - Compromising user accounts via password spraying
2. Identification of vulnerabilities (with credentials)
    - Manual and automatic AD enumeration
    - Extraction of access data and password hashes in services
    - Checking authorization management (e.g. network shares)
    - Checking the hardening measures of the AD
3. Privilege escalation
    - Dependency check to other domains
    - Extraction of local password hashes and cached passwords

5.4 Risk assessment

Binsec GmbH considers the term “risk“ to mean a combination of the probability of occurrence of a vulnerability (or the likelihood of its exploitation) and the possible extent of damage. The probability of occurrence or the probability of exploitation of a security gap in IT systems essentially depends on these factors:

- How easily can the vulnerability be identified? (Visibility)
- Are there any exploits for this vulnerability available, or is the attacker required to have a certain level of knowledge to exploit them? (Exploitability)
- Does the exploitation require special rights? (Privilege Escalation)
- Is a combination with other security holes required? (Vulnerability Chaining)
- Is human interaction necessary for the vulnerability? (Social Engineering)

The following classifications are decisive for the possible extent of damage:

1. Financial damage
2. Complete compromising of the system
3. Violation of security objectives related to data or user accounts:
    a) Confidentiality
    b) Availability
    c) Integrity
4. Bypassing of security measures
5. Information disclosure

Taking into account both the probability of occurrence and the potential extent of damage, the penetration tester makes a subjective assessment of the risk for each vulnerability found. We recommend taking an own assessment of the vulnerabilities.

The assessment is subject to the following classification:

occurrence probability	
high	The vulnerability is obvious or exploits are freely available.
medium	The vulnerability can be identified in a reasonable amount of time; exploits may need to be adapted.
low	The vulnerability is difficult to find and may require permissions or the exploitation of other vulnerabilities.

extent of damage	
critical	Complete compromising of the system.
high	Violation of security objectives concerning information or IT systems.
medium	Bypassing of security measures.
low	Preparation for exploitation of other vulnerabilities as part of a sustained attack.
warning	Information disclosure.

The risk classification entails a priority for action.

extent of damage

occurrence probability	warning	low	medium	high	critical
high	🟩	🟨	🟥	🟥	🟥
medium	🟩	🟨	🟨	🟥	🟥
low	🟩	🟩	🟨	🟨	🟥

🟩 note 🟨 action required 🟥 immediate action required

5.5 About the binsec GmbH

We are a company that specializes in IT penetration testing, located at Frankfurt am Main, Germany. Since 2013, carrying out technical security analyses of IT infrastructures, web applications, APIs, mobile apps (Android / iOS), etc. has been the core of our daily work. As an owner-managed company, the long-term satisfaction of our customers is of great importance. The certifications of our employees, the teaching activities at universities and our pentesting experience speak for themselves.

BETTER PENTESTING

NO NONSENSE

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

✉ info@binsec.com
☎ +49 69 2475607-0

Managing Director:	Patrick Sauer
Authorised Officers:	Dominik Sauer, Florian Zavatzki
Commercial Register:	Frankfurt a.M. HRB 97277
VAT ID no.:	DE290966808