

CONSULT IT FINAL

Sudoerrs

- [Tutorial](#)
- `test ALL=(ALL:ALL) /tmp/scripts/test.sh` This line is potentially dangerous. User test can execute with sudo privileges `test.sh` script which source code can be modified. This means he can execute each command as a root.

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
  
Defaults        env_reset  
Defaults        mail_badpass  
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"  
  
root    ALL=(ALL:ALL) ALL  
%admin   ALL=(ALL) ALL  
%sudo    ALL=(ALL:ALL) ALL  
%support ALL=(ALL:ALL) /bin/bash, /usr/sbin/reboot, /usr/sbin/shutdown  
%usermgmt ALL=(ALL:ALL) /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel  
%grpmgmt ALL=(ALL:ALL) /usr/sbin/groupadd, /usr/sbin/groupdel, /usr/sbin/groupmem, /usr/sbin/  
groupmod  
test    ALL=(ALL:ALL) /tmp/scripts/test.sh
```

NMAP

- There are too many open ports available. Open should remain only:
 1. a
 2. b
 3. c
 4. d
- Having too many open ports expose servers to many potential attack vectors.
- There is an [Exploit](#) available for ftp vsftpd 2.3.4. It should be updated to the newest version.

```
# Nmap 7.80 scan initiated Mon Mar 14 08:52:07 2022 as: nmap -Pn -p- -sT
-sV cybertrans.example
Nmap scan report for cybertrans.example (192.168.12.34)
Host is up (0.0065s latency).
Other addresses for cybertrans.example (not scanned): ::1
Not shown: 65522 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
80/tcp    open  http     Apache httpd 2.4.46 ((Debian))
111/tcp   open  rpcbind  2-4 (RPC #100000)
443/tcp   open  ssl/ssl  Apache httpd (SSL-only mode)
3306/tcp  open  mysql    MySQL 5.5.5-10.1.26-MariaDB-1
4767/tcp  open  unknown
4769/tcp  filtered unknown
5037/tcp  open  unknown
39381/tcp open  unknown
39563/tcp open  webdav
53013/tcp open  soap    gSOAP 2.8
53014/tcp open  ssl/soap gSOAP 2.8
53113/tcp open  soap    gSOAP 2.8
53114/tcp open  ssl/soap gSOAP 2.8

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Mar 14 08:54:55 2022 -- 1 IP address (1 host up)
scanned in 168.03 seconds
```

- Ports for gSOAP are doubled without known reason. To be checked

DataBase

- Passwords should almost always be stored as hashes of hash function (f.e. sha-256) not a plain text. Hashes are irreversible, so even if the attacker will find our database, he has to put in lots of effort to get plain text passwords.
- Security of personal data of customers is extremely important. Any potential leak can cause destructive consequences for whole company. As so database should be well protected

```
LOCK TABLES `eklamot_users` WRITE;
/*!40000 ALTER TABLE `eklamot_users` DISABLE KEYS */;
INSERT INTO `eklamot_users` VALUES (1,"Adam","Wieczorek","adawieczorek68@eklamot.com",
"489193284889","1968-01-19","a12345","2022-02-16 13:28:08","2019-12-01 19:51:38","1"),(2,
"Jagoda","Pawlak","jagpawlak67@eklamot.com","486560820511","1967-10-14","123","2022-02-25
04:18:03","2018-10-21 06:51:16","1"),(3,"Gabriel","Kwiatkowski","gabkwiatkowski86@eklamot.com",
"486304543350","1986-06-16","loveme","2022-02-18 04:21:23","2020-02-02 18:32:12","1"),(4,
"Kajetan","Mazur","kajmazur93@eklamot.com","487690650856","1993-05-17","family","2022-02-17
17:15:03","2020-05-10 20:38:36","1"),(5,"Gabriel","Nowak","gabnowak98@eklamot.com",
"480186921584","1998-06-06","1q2w3e","2022-02-25 07:29:46","2019-06-06 09:46:00","1"),(6,
"Michalina","Pietrzak","micpietrzak86@eklamot.com","487577128915","1986-11-30","999999",
"2022-03-03 04:29:56","2020-08-26 11:25:45","1"),(7,"Kuba","Wieczorek","kubwieczorek75@eklamot.
com","489444280039","1975-09-14","qwerty1","2022-02-22 23:09:41","2018-03-29 00:32:41","1"),(8,
"Aleksandra","Majewska","alemajewska79@eklamot.com","483747663451","1979-12-13","thomas",
"2022-02-18 18:11:11","2018-06-14 00:14:27","1"),(9,"Alan","Wójcik","alawojcik82@eklamot.com",
"484844080318","1982-08-29","aaaaaa","2022-02-22 05:07:22","2021-06-12 03:49:14","1"),(10,
"Fabian","Sikora","fabsikora93@eklamot.com","488002667418","1993-07-23","baseball","2022-02-26
05:39:13","2021-01-23 09:45:53","1"),(11,"Borys","Tomaszewski","bortomaszewski73@eklamot.com",
"485518141222","1973-09-26","a123456","2022-02-25 02:01:33","2019-12-09 01:07:44","1"),(12,
"Jakub","Olszewski","jakolszewski68@eklamot.com","486056993470","1968-02-04","evite","2022-02-15
17:17:50","2020-01-16 15:40:50","1"),(13,"Blanka","Kamińska","blakaminska77@eklamot.com",
"483414658711","1977-05-01","football1","2022-02-19 20:48:53","2019-08-10 14:00:05","1"),(14,
```

Password Policy

- We should force changing temporary password after first login, not only kindly ask for it. It does not work in most cases.
- Adding two-factor authorisation would be a great idea. Authenticator app on smartphone or pendrive authentication to consider.

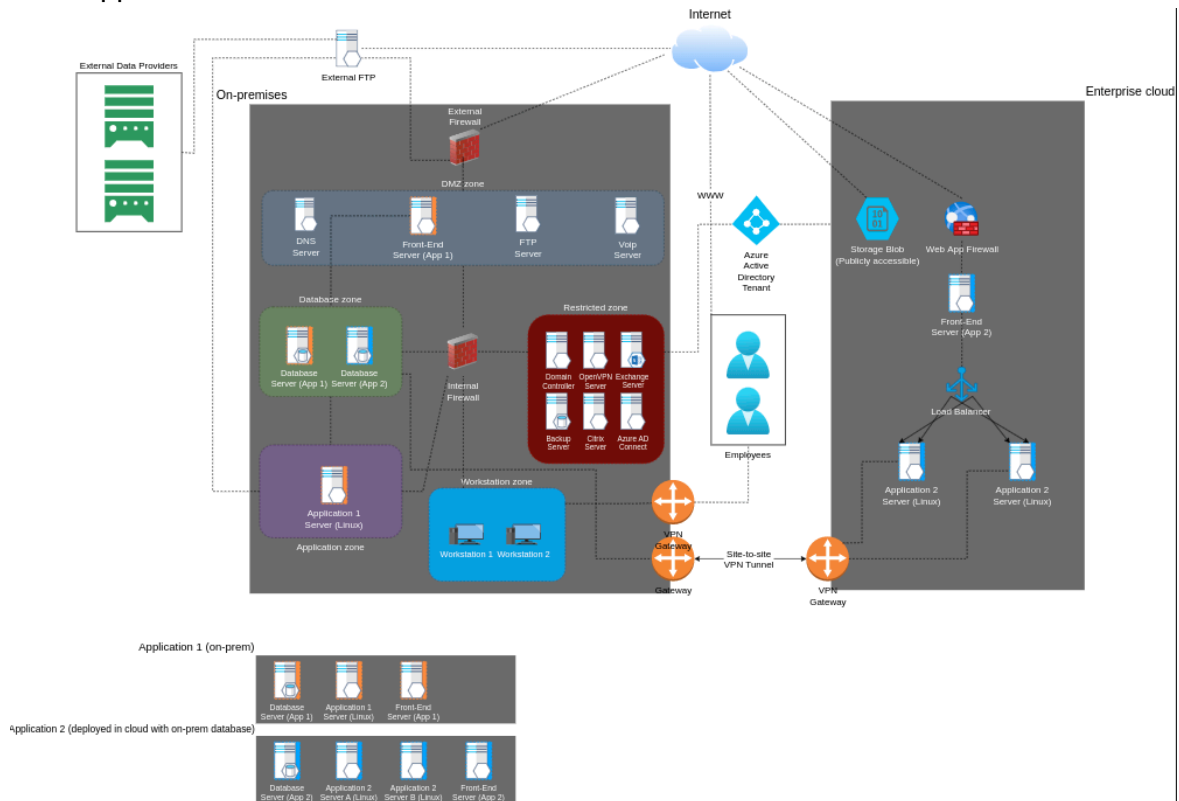
Kroki w przypadku pierwszego logowania:

1. Aby uzyskać dostęp do wirtualnej maszyny wejdź na stronę <https://vm.eklamot.example>
2. Wpisz swoją numer użytkownika i tymczasowe hasło (w celu uzyskania tymczasowego hasła skontaktuj się z pracownikiem działu IT, który prześle je drogą mailową na wskazany przez użytkownika adres email).

5. Pamiętaj o jak najszybszej zmianie tymczasowego hasła na takie, które spełnia politykę haseł w dokumencie „Polityka haseł”

Architecture

- Backup server should be accesible only for admin employess.
- Employess should not have access directry to restreicted zone. They need to connect to workstation zone by VPN or RCP first.
- Maybe a firewall between Front-End server and Database Server.
- Both Application2 should have access to database2.



Phishing

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

- Human is the weak point in phishing attacks. Coaching employess about vectors of phishing attacks and showing examples off those attacks is extreamly important. We can have the best software and hardware security, but without educated employess we won't benefit from that.

Zmiana Procesu Zarządzania Podatnościami w Eklamot

Changes we suggest:

Security scanners are not ideal. We suggest using both famous Nessus and Nexpose for better quality. Moreover even both can miss some dangerous vulnerabilities. As so we insist on sending those reports directly to security team. Security team would then extend research.

Final Process:

1. Prepare a scan request - If there is a need for scanning, the request is made by the System Administrator.
2. Preparation and execution of the scan with Nessus and Nexpose (complementary tools)
3. Provide the results of the scan to the Security Team.
4. The Security Team deepens the vulnerability search.
5. If vulnerabilities are found, they are forwarded to the system administrator with a report describing them.
6. Is a deviation required? A decision point that determines if a deviation is required within the vulnerabilities found. The system administrator reviews and decides whether a derogation request is required.
7. Prepare a deviation request -- If the system administrator decides a deviation is required, the system administrator prepares an appropriate request with justification, which it sends to the Security Team
8. Perform corrective action -- If no deviation request is required, the System Administrator proceeds to implement the planned corrective action.
9. Report completion of corrective action -- Upon completion of the action, the System Administrator reports its completion to the Security Team.
10. Has the variance request been approved? - A decision point that determines whether the deviation request has been accepted by the Security Team. If the request is accepted, the Security Team prepares an appropriate summary. If the request is not accepted, the system administrator must take corrective action.
11. Prepare Summary - The Security Team prepares an appropriate summary depending on whether the process resulted in the implementation of corrective actions to address the vulnerabilities discovered or the acceptance of the deviation request.