DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DEFAULT ACCOUNTS

The hacker found software with administrator rights on the system which still has the default password.

MITIGATION
Password policies

DETECTION
Monitor whether default accounts have been activated or logged into

LOCAL ACCOUNTS

The hacker found a password that was saved in a text file on an employee's laptop and used it to access the local account.

MITIGATION
Password manager

DETECTION
Regular audits of local system accounts

WINDOWS KERNEL EXPLOITATION

The hacker found a not updated system that allows a Windows kernel exploit.

MITIGATION
Regular updates

DETECTION
Vulnerability scanner

DLL HIJACKING

The hacker discovered a missing DLL that he can replace with a malicious file, the DLLs are executed when Windows starts.

MITIGATION
Disabling DLL loading from remote network shares

DETECTION
Monitor DLL locations

PRINTER NIGHTMARE

The hacker found several devices with the printer nightmare weak point which enabled remote code execution through the Windows spooler service.

MITIGATION
Disable the print spooler

UNQUOTED SERVICE PATHS

The hacker finds an unquoted service path exploit that can be used to execute binaries in the same folder.

MITIGATION
Enclose the path in quotes

DETECTION
Wmic search

STORED CREDENTIALS

The hacker searches the registry for usernames/passwords and found credentials from a putty session.

MITIGATION
Disable cleartext passwords in memory

DETECTION
Implementing audit controls

WEAK FOLDER PERMISSIONS

The hacker has written permission in a folder used by a service, he can replace the binary with a malicious one.

MITIGATION
Folders with service binaries should only be accessible to administrators

DETECTION
Monitor for "write" or "modify" permissions