Ingreslock Vulnerability

Background

Ingres database is a SQL database that is commonly used to support very large commercial and government applications. It is widely used and if older versions are used then it creates very big problems for any organization. SQL databases are used to hold a lot of information that can be accessed both offline and online, most of the websites you use will have a database of some sort and hopefully they are secure. As applications become larger there are additional services are added and in the process of developing the Ingres application it was decided to have port 1524 open. This port links to a service called ingreslock which is meant to lockdown specific areas of the database application. Inadvertently, ingreslock has a backdoor associated with it that automatically binds when a connection is made with this port.

Telnet is an old protocol that allows you to connect over your network to different machines and have a 2-way connection that can exchange information, files, etc. This protocol isn't meant to be used as much any more because there is no encryption applied to the traffic in transit, allowing anyone performing a man-in-the-middle attack to see the information that is being sent in plain-text. More secure protocols have been adopted in place of telnet, including SSH (Secure Shell) which provides encryption to the data in transit, using asymmetric encryption. It is very simple to make a telnet connection, in the terminal you type telnet <target IP> <target port> and it will establish a connection for you.

Walkthrough

Step 1:	Make sure your Kali image is up to date using **apt-get update**, **apt-get upgrade** and if required **apt-get full-upgrade**;
Step 2:	Discover the IP address of the victim machine (use **nmap**, **netdiscover** etc to find this machine);
Step 3:	Open a terminal (Terminal 1 – this will make sense later);
Step 4:	Perform a detailed nmap scan on the victim machine (**nmap -sS -Pn -sC -A <target IP address>**) – This nmap scan can take a while, it's pretty detailed!;
Step 5:	You need to find port **1524** that is the listening port for **ingreslock**;
Step 6:	In the terminal type **telnet <target IP> 1524** and hit **Enter**;
Step 7:	You will automatically have a **root** shell on the target machine;
Step 8:	type **whoami** – the result now should be **root** (YAY!!);
Step 9:	Now you have root you can do **anything** you want on the box;
Step 10:	This is the end of the vulnerability.

Conclusion

In this vulnerability you are using the backdoor capability built into this version of Ingres Database, it is a very common vulnerability, but it can still be found it the system admin doesn't realize that this service needs to be shutdown. There are multiple ways to make a connection with different services that are built into Kali, telnet is only one of the methods of connection. It is important to know a few methods because you might find yourself in a situation where telnet use is restricted, and you will need to use another tool to make a connection. Any backdoor that automatically binds and allows a root shell to be opened is very dangerous because this is not controlled and can allow anyone to connect to your machine. Having root access is the same as having admin rights on a Windows machine. This allows you to change settings, create users, delete users, install applications etc, this is an account that should be highly restricted and controlled. If random users connect with root credentials this is a clear indicator that your system is compromised. The best way to mitigate this vulnerability is to shut down this service, making sure that port 1524 is closed and update the Ingres Database to its most recent version.