Day-6

Security Misconfiguration

[Task 20] [Day 6] Security Misconfiguration

Security Misconfiguration

Security Misconfigurations are distinct from the other Top 10 vulnerabilities, because they occur when security could have been configured properly but was not.

Security misconfigurations include:
• Poorly configured permissions on cloud services, like S3 buckets
• Having unnecessary features enabled, like services, pages, accounts or privileges
• Default accounts with unchanged passwords
• Error messages that are overly detailed and allow an attacker to find out more about the system
• Not using HTTP security headers, or revealing too much detail in the Server: HTTP header
This vulnerability can often lead to more vulnerabilities, such as default credentials giving you access to sensitive data, XXE or command injection on admin pages.
For more info, I recommend having a look at the OWASP top 10 entry for Security Misconfiguration

Default Passwords

Specifically, this VM focusses on default passwords. These are a specific example of a security misconfiguration. You could, and should, change any default passwords but people often don't.
It's particularly common in embedded and Internet of Things devices, and much of the time the owners don't change these passwords.
It's easy to imagine the risk of default credentials from an attacker's point of view. Being able to gain access to admin dashboards, services designed for system administrators or manufacturers, or even network infrastructure could be incredibly useful in attacking a business. From data exposure to easy RCE, the effects of default credentials can be severe.
In October 2016, Dyn (a DNS provider) was taken offline by one of the most memorable DDoS attacks of the past 10 years. The flood of traffic came mostly from Internet of Things and networking devices like routers and modems, infected by the Mirai malware.
How did the malware take over the systems? Default passwords. The malware had a list of 63 username/password pairs, and attempted to log in to exposed telnet services.
The DDoS attack was notable because it took many large websites and services offline. Amazon, Twitter, Netflix, GitHub, Xbox Live, PlayStation Network, and many more services went offline for several hours in 3 waves of DDoS attacks on Dyn.

Practical example

This VM showcases a `Security Misconfiguration`, as part of the OWASP Top 10 Vulnerabilities list.
Deploy the VM, and hack in by exploiting the Security Misconfiguration!

#1
Deploy the VM

No answer needed

#2
Hack into the webapp, and find the flag!

found source code on GitHub https://github.com/NinjaJc01/PensiveNotes
creds shown in README.md
`pensive:PensiveNotes`

thm{4b9513968fd564a87b28aa1f9d672e17}