CWL
CyberWarFare Labs

Uber Hack Simulation

How Lapsus$ Breached a Tech Giant

ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

ABOUT SPEAKER

SUBASHINI K B

Security Consultant

Subashini Balaji is a Security Consultant at **CyberWarFare Labs**, specializing in **Red Teaming and APT simulations** in enterprise environments. She also writes **technical blogs and articles** focused on real-world cyber attack techniques and defenses.

AGENDA

1. Description for the challenge.
2. Attack Scenario.
3. Attack flow
4. Solving lab challenge.

DESCRIPTION

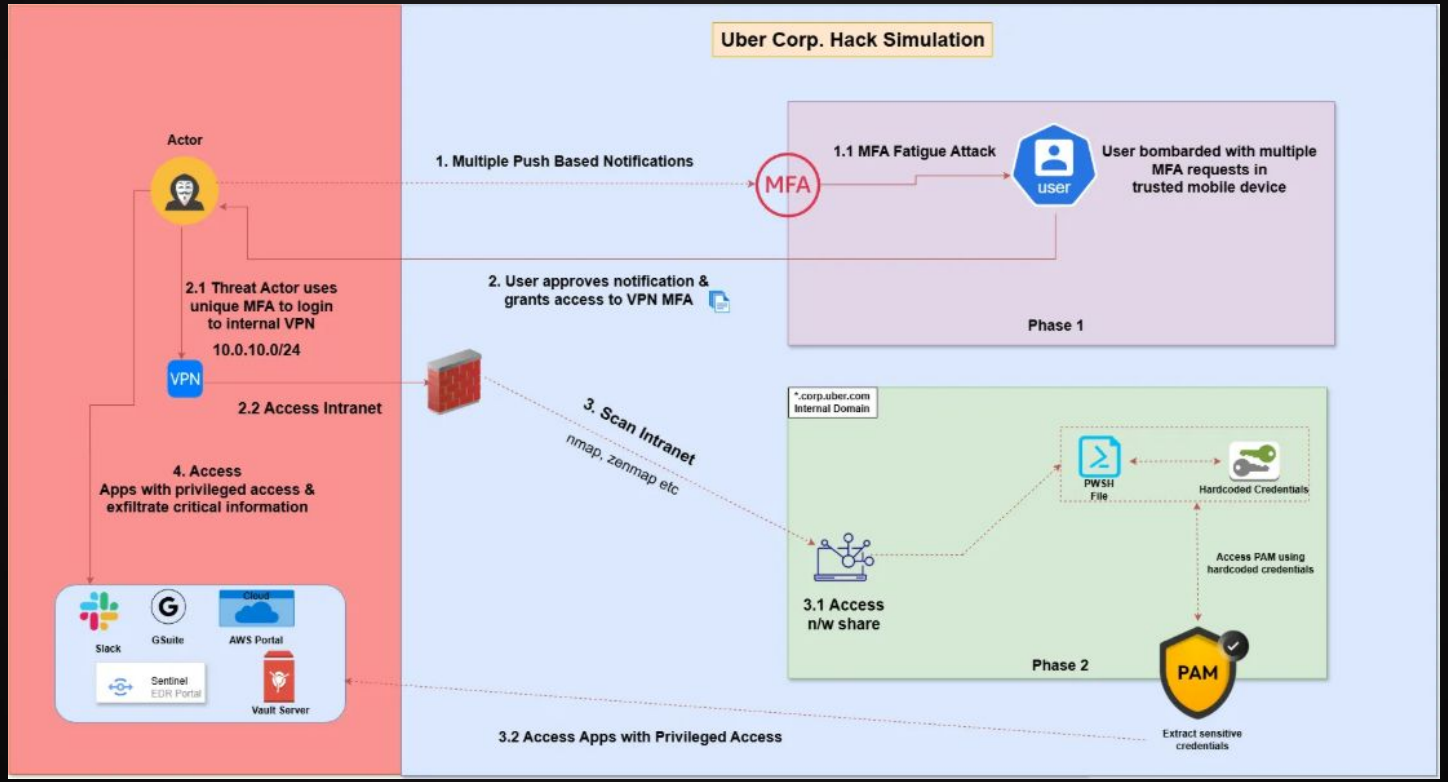
This webinar demonstrates how real-world threat groups like Lapsus$ compromise enterprises using MFA fatigue, social engineering, and credential abuse. Participants will walk through an end-to-end Uber-style breach, from VPN access to privileged system takeover.

SIMULATION GOAL

To replicate how Uber was compromised using:

1. MFA fatigue
2. Credential abuse
3. VPN access
4. Internal reconnaissance
5. Privileged Access Management (PAM) exploitation
6. This lab shows how one small mistake can lead to full enterprise compromise.

ATTACK FLOW



CHALLENGE TIME

Try out the Challenge here

https://infinity.cyberwarfare.live/apt_labs/apt/challenges/69300d6338db4fe55e8993e8

CWL
CyberWarFare Labs

Thank You