SCENARIO #3: **PBX Scenario**

Scenario:

On Feb 14, 2015, Aziz Uddin, who is a cyber-criminal and is on the Interpol and the FBI's most wanted list, was arrested [1]. According to FBI, he was involved in an international communication scheme and hacking venture defrauding several companies and individuals, mostly in New Jersey, of over $50 million from November 2008 to April 2012 [2]. He hacked into the phone with remote voicemail access capability and change the permanent forwarding number. Now the next time anyone dials a phone it will place a new call to the pay-per-minute number they owned, thus collecting money. A more rewarding method is to hack VoIP (voice over IP) phones and software-based Private Branch Exchange (PBX) used in many small- and medium-sized companies. The hackers find the IP address of insecure PBXs and try to make a call using that PBX. They use robo-dialers, dialing hundreds of times in the evening or in a weekend.


TECHNOLOGY

The Inside Story Of How Pakistan Took Down The FBI's Most-Wanted Cybercriminal

By Eric Markowitz @EricMarkowitz
03/30/15 AT 10:08 AM EDT

"Just before dawn on Feb. 14, in a quiet residential suburb of Karachi, Pakistan's chief cybersecurity officer, Mir Mazhar Jabbar, stood silently outside the home of Noor Aziz Uddin. He knocked. Standing behind him was a team of local Karachi police officers, waiting to raid Uddin's home and place him under arrest." (IBTimes article)

In this scenario, students will use FreePBX systems [3] inside the virtual machine environment in OCR platform and will try to hack using one of the techniques such as weak password, firewall bypass, and vulnerabilities in FreePBX [4]. Note that FreePBX uses VoIP (voice over IP), and SIP (Session Initiation Protocol) protocol. Students will also study this interesting fraud case, where individual victims experience a relatively small damages and involves attacks originated from outside of the US, which is not unusual in cybersecurity crimes. In this particular case, victims contact the police but they aren't equipped to handle international crimes because calls are almost always going to foreign countries. They contacted the FBI but they did not take any actions because the FBI is usually only interested in threats against the government or crimes that were over one million dollars in damages. Most of this PBX hacking is in the tens of thousands. In 2012 the FBI did receive enough reports about PBX hacking that they began looking at the data [5].

NICE Workforce Framework for Cybersecurity:

Scenario #3 & #4 will cover the following Knowledge areas.

K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
K0005 Knowledge of cyber threats and vulnerabilities.
K0007 Knowledge of authentication, authorization, and access control methods.
K0013 Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0046 Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0104 Knowledge of Virtual Private Network (VPN) security.
K0135 Knowledge of web filtering technologies.
K0202 Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
K0205 Knowledge of basic system, network, and OS hardening techniques.
K0336 Knowledge of access authentication methods.

References:

[1] https://economictimes.indiatimes.com/news/international/world-news/fbis-most-wanted-cyber-criminal-arrested-from-pakistan/articleshow/46246568.cms?from=mdr
[2] A 'Game of Thrones' thief and a dam hacker: These are the FBI's 41 most-wanted cyber criminals, https://www.businessinsider.com/these-are-the-fbis-41-most-wanted-cyber-criminals-2018-6
[3] FreePBX, https://www.freepbx.org/
[4] FreePBX CVE, https://www.cvedetails.com/product/10928/Freepbx-Freepbx.html?vendor_id=6470
[5] The Phreaky world of PBX hacking, Darknet Diaries, https://darknetdiaries.com/episode/1/