Introduction

- Everyone need top-class cybersecurity to make sure that their data remains private and is not hacked or leaked for all the world.
- And with the increasing popularity of Artificial Intelligence and Machine Learning, these technologies are even becoming key players in the field of cybersecurity.
- Machine Learning has many applications in Cyber Security including identifying cyber threats, improving available antivirus software, fighting cyber-crime that also uses AI capabilities.
- With machine learning, cybersecurity systems can analyze patterns and learn from them to help prevent similar attacks and respond to changing behavior.
- It can help cyber security teams be more proactive in preventing threats and responding to active attacks in real time.
- It can reduce the amount of time spent on routine tasks and enable organizations to use their resources more strategically.

Role of ML in Cyber Security

- Machine learning can make cybersecurity simpler, more proactive, less expensive and far more effective.
- AI is necessary for cybersecurity because hackers are already using it for cyberattacks.
- 75% of the surveyed executives also believe that AI allows for a faster response to security breaches.
- Therefore, Machine Learning based cybersecurity software is fast becoming a necessity and not only a luxury.
- Machine learning preemptively stamps out cyber threats and security infrastructure through pattern detection, real-time cyber crime mapping and thorough penetration testing.
- This can be done by using predictive analytics to detect threats and malicious activity, using natural language processing for security, enhancing biometric-based login techniques, etc.

Role of ML in Cyber Security

- Machine learning uses algorithms born of previous datasets and statistical analysis to make assumptions about a computer's behavior.
- The computer can then adjust its actions — and even perform functions for which it hasn’t been explicitly programmed.
- With its ability to sort through millions of files and identify potentially hazardous ones, machine learning is increasingly being used to uncover threats and automatically squash them before they can wreak havoc.

Penetration Testing using ML

- Proactively testing our environment or applications to detect vulnerabilities before a hacker can find them
- You are trying to look for deficiencies in processes and controls by conducting simulations or false attacks
- AI and ML can help the pen tester to not only gather all the information automatically but also analyze it and determine different courses of action.
- There are several well- known methodologies and standards that can be used to perform penetration tests such as
  - OSSTMM (Open Source Security Testing Methodology Manual),
  - OWASP (Open Web Application Security Project),
  - NIST (National Institute of Standards and Technology),
  - PTES (Penetration Testing Methodologies and Standards),
  - ISSAF (Information System Security Assessment Framework).

Phases of Penetration Testing using ML

- Information Gathering
  - Gather as much information as possible about our targets by collecting information from publicly accessible sources to discover the ports and services that are open.
- Vulnerability Assessment / Scanning
  - Perform more in-depth vulnerability scans trying to determine all the potential vulnerabilities that the targets could have.
  - The results of the scans by analyzing them and removing everything that is not applicable or generates noise, taking into consideration information gathered from the previous phase
- Exploitation
  - To gain access to the systems, perform lateral movements, escalate privileges, gather more information, and maintain persistent access
- Reporting
  - A report with detailed information about the issues found, the risk implications, and recommendations is prepared and delivered
  - AI and ML can enhance the reporting process by analyzing the data obtained during the assessment and combining it with threat intelligence and the knowledge acquired in previous engagements to generate actionable insights specific for the organization

Social Engineering

- Social engineering is a type of hacking that is carried out through human interactions.
- An attacker uses psychological manipulation to make the person do mistakes and reveal information.
- There is no particular way to carry out a social engineering attack, an attacker may try different techniques depending on the victim’s nature.
- Social engineers are equipping themselves with the futuristic tools of AI in order to further exploit human psychology and gain access to systems and data.
- Social engineering is completely about human error and that is what makes it a dangerous attack.

Social Engineering

- Here are the five social engineering attacks to watch out for:
  - **Phishing**: It uses email or malicious websites to solicit personal information by posing as a trustworthy organization.
  - **Pretexting**: It is a made-up scenario developed by threat actors for the purpose of stealing a victim's personal data.
  - **Baiting**: The trap could be in the form of a malicious attachment with an enticing name.
  - **Quid Pro Quo**: It exploits human weaknesses like negligence or unawareness to steal their private information
  - **Tailgating**: It involves closely following an authorized person into a restricted access area.

Social Engineering

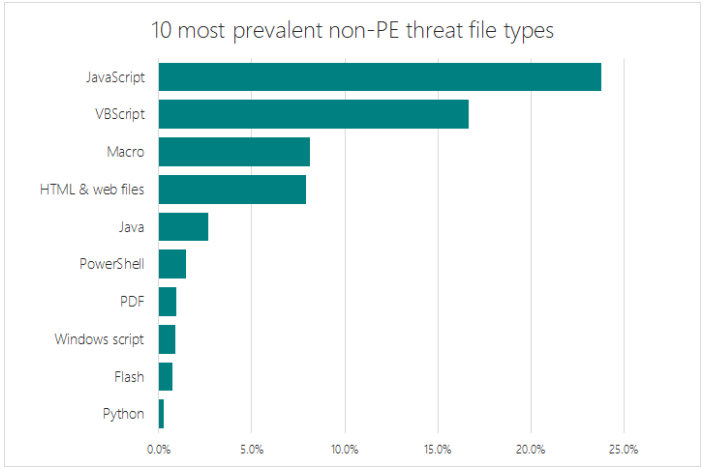
- Social engineering is one of the hardest attacks to identify. So, it is always advised to:
  - Not open any emails that don’t seem to be from a legitimate id
  - Not revealing any kind of information over phone calls
  - Not trusting lottery bait web links — ignore web links that say you have won a million dollar
- There are numerous AI-powered chatbots available on the web that work towards sorting out customer issues.
- However, if a malicious AI-powered is taught to interact with humans in a friendly helpful way, it can be used to seek out customer complaints online, and they can be used to pose as customer service bot trying to remedy the situation.
- And if anyone falls to this trap, they may end up handing over sensitive data such as security question answers or passwords or personal identifying information.

AI for Social Engineering

- AI can be a great option to tackle future threats — it can make the work of security researchers and analysts more effective.
- Therefore, technology firms across the world have started working day in and out to leverage every possible tech to deal with cyber-attacks.
- Virtual Risk Score alerts users or groups when they are vulnerable to social engineering attacks.
- The risk scores help organisations identify the person or the group that is most likely to click on a phishing link and fall into a trap.

AI for Social Engineering

- Modern social engineering attacks use non-portable executable (PE) files like malicious scripts and macro-laced documents



AI for Social Engineering

- Non-PE threats are typically used as intermediary downloaders designed to deliver more dangerous executable malware payloads.
- Due to their flexibility, non-PE files are also used in various stages of the attack chain
- Beyond targeted credential phishing attacks, we commonly see large-scale malware campaigns that use emails with archive attachments containing malicious VBScript or JavaScript files.
- These emails typically masquerade as an outstanding invoice, package delivery, or parking ticket, and instruct targets of the attack to refer to the attachment for more details.

AI for Social Engineering

- The target opens the archive and runs the script, the malware typically downloads and runs further threats like ransomware or coin miners.
- The power of machine learning is that it is scalable and can be powerful enough to detect noisy, massive campaigns, but also specific enough to detect targeted attacks with very few signals.
- This flexibility means that we can stop a wide range of modern attacks automatically at the onset.
- In addition to these ML-learned features, the models leverage expert researcher-created features and other useful file metadata to describe content.

AI for social engineering

- Deep Fakes
- Voice Impersonation
- Fake review generator