Advances in Cyber Security

Mr. Rohit Raosaheb Yadav
TE (Computer Science and Engineering)
KIT's College of Engineering, Kolhapur.

***Abstract*— Computer security is an issue of global concern to those who use the internet just for educational and entertainment purposes. Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk from both physical and cyber threats. Hence, we see the Cyber-Security domain making a way forward in today's global industry. Each day there is an advancement in each domain and technology. This paper will give us an idea about the advances in the Cybersecurity domain. It will try to cover the latest trends in this domain followed by it. It also includes latest attacks carried out by the hackers to the Normal Users who are using the Internet just for Entertainment as well as for Educational Purpose. At last, it will brief idea about how each user can secure himself from these types of Attacks.**

Keywords*— *Cyberspace; Security; Domain; Attack;

INTRODUCTION

In the modern age's growing dependency on the internet, a new threat begins to emerge in the cyberspace. More and more, everyday facts of life are being integrated digitally, more becoming vulnerable. The Internet is being used by students in school to the members of the board of director in the company. But with the advantages of this digital life, there are more disadvantages due to the species in our society known as Hackers. They are using their knowledge and skills to exploit the digital life of the mankind. It includes exploitation of the Web server of the company to the social media account of the individual. Hence there should be some species known as ethical hacker or security researcher present in society to protect against this type of attacks as well as to create awareness about cybersecurity in people mind. Day by day there are lots of advances in this domain with the perspective of hackers and the security researcher to prevent this type of attacks. In this paper, we will learn latest techniques used by the hackers to exploit the digital world and will also see how to prevent them.

This Paper is Divided into two parts, first one is advances in Cyber Security with the perspective of The Hacker and the second one is with the perspective of Security Researchers.

To Prevent the newly developed Cyber Attacks, we should know how they are practically performed.

I. ADVANCES IN CYBERSECURITY ATTACKS (AS HACKER)

A. System Exploitation

This type of attack consists of exploitation of the system after finding certain flaws in them. The system can be operating systems like windows in the personal computers, Android in most of the smartphones. Majority of this attacks will start with creating trojan horses with a compatible extension for the system. Then trojan horse will be sent to the victim by any kind of media like email attachment as well as by sending a link to the malicious software. If the victim clicks on that software or clicks on the malicious link. The session will be created with the victim system to the attacker. Earlier trojans were detected by antiviruses or by an application such as Windows Defender. But now hackers have found ways to bypass them and access the System. Some ways are shown below for Windows Exploitation and Android Exploitation.

Windows Exploitation:

1. Veil-Evasion
2. sAINT

Android Exploitation:

1. Evil-Droid

Veil-Evasion

Veil-Evasion is a tool designed to generate Metasploit payloads that bypass common anti-virus solutions. It uses certain cryptographic techniques to hide the trojan from the Antivirus solutions. The output of the Trojan or of the Payload is same as Windows software Extension as .exe. Till date, updated Windows 10 2018 version is not able to find this Malicious file as Trojan.

https://github.com/Veil-Framework/Veil-Evasion

sAINT

It is a spyware generator for Windows Systems which will generate JAR file as an output. When file enters Windows environment, it looks like normal JAR file but contains malicious code to spy the Systems. sAINT output file is undetectable for Antivirus solutions and for Windows Defender on Fully Updated Machine. After executing file automatically sends keystrokes, webcam snaps after predetermined time duration. All files are sent to the predetermined email address of the Attacker.

Feature of sAINT

1. Keylogger
2. Take Screenshot
3. Webcam Capture
4. Persistence

https://github.com/tiagorlampert/sAINT

Evil-Droid

Evil-Droid is a framework that creates & generate & embed apk payload to penetrate Android platforms. Exploits the Android smartphones. They are undetectable for android security up to latest update of Android. A unique feature of Evil-Droid that, it can be bind with any Android Application file. After successfully exploiting smartphones attacker can get following things:

Features of Evil-Droid

1. Live Webcam Stream
2. Download Files from Device
3. Keylogger
4. Take Screenshot
5. Record Conversation
6. Dump Contacts
7. Dump SMS

https://github.com/M4sc3r4n0/Evil-Droid

B. Phishing

Phishing is used most often by cybercriminals because it's easy to execute and can produce the results with very little effort. Fake Emails, text messages are created to look like they're from an authentic source. Initially, the attacker creates webpage depending on the Victim interest. After sending phishing page to the victim, when victim enters credential to that login box, credential automatically sent to the attacker. Earlier days after creating phishing website, the website was detected by most of the browser as a phishing website. But due to research and advances in this field cybercriminals have got the way to bypass that and create a page that will be HTTPS and will be looked like authentic one.

SocialFish v1.0

It is a framework used to create phishing websites. It is integrated over Internet Attack. It created a webpage with a pre-determined template such as Facebook Login Page or LinkedIn Page etc. Web pages generated with this Framework are undetectable for any browser to detect it as phishing website or as a malicious website.

AVAILABLE PAGES

1. Facebook
2. LinkedIn
3. GitHub
4. StackOverflow
5. WordPress
6. Twitter

https://github.com/UndeadSec/SocialFish

C. Man in the Middle Attack

A man-in-the-middle attack is a type of cyber attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. Basically, it captures traffic and packets between each sender and receiver in the Network. An attacker can inject malicious code to perform phishing or Eavesdropping.

Recently Advance framework created for Performing MITM for penetration testing purpose known as Xerosploit.

It is a big advancement in this Attack that combines multiple operations in Man in the Middle Attack.

Features of Xerosploit

1. Port scanning
2. Network mapping
3. Dos attack
4. Html code injection
5. JavaScript code injection
6. Download interception and replacement
7. Sniffing
8. DNS spoofing
9. Background audio reproduction
10. Images replacement
11. Driftnet
12. Web page defacement

https://github.com/LionSec/xerosploit

D. Denial of Service Attack

When we type a URL into our browser we are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once. If attacker overloads server with requests, it can't process yours. That huge number of requests shut it down forcefully and Denys access to legitimate users.

XERXES

It is the most powerful tool now to test any web server DOS attack flaw.

https://github.com/zanyarjamal/xerxes

E. Wifi Exploitation

In daily we use Wi-Fi with any kind of password that is based on some encryption technique such as WPA2, WPA or WPS. In early days Hackers have exploited wi-fi with Brute force attack or Dictionary attack or by trying some wps pins on WPS enabled Router. But due to Updating wi-fi encryption technique and firmware updating it is very time to consume and risky to exploit wi-fi using such type of attack.

Recently Security Researcher has found some way to Exploit the Wi-Fi and to get WIFI password without trying multiple passwords or by doing any brute force attack.

1. WIFI Phishing

WIFI Phishing

In this type of attack Hacker first sends a number of DE authentication packets to router and deauthenticate all devices in a WIFI network. At the same time, Hacker will create a fake wireless access point with the same name as that of previous connected WIFI name. When the victim tries to connect it, it will be redirected to Fake Firmware Update page of Router where the victim has to enter router password in order to proceed further. After successful submission of Password, Hacker will get that password in Text Format. Without Brute Force Attack.

*Wifiphishe*r is a security tool that performs Wi-Fi automatic association attacks to force wireless clients to unknowingly connect to an attacker-controlled Access Point.

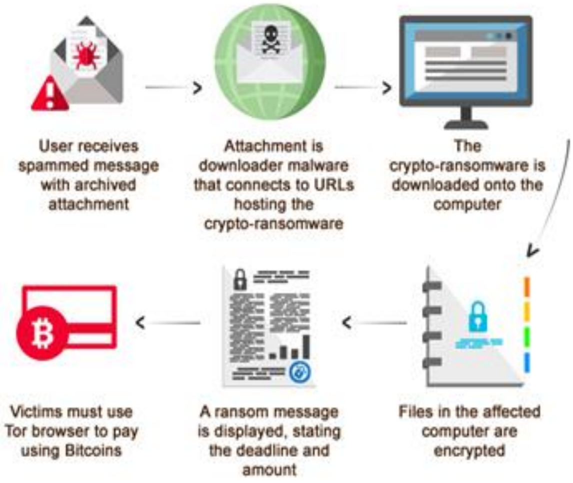
https://github.com/wifiphisher/wifiphisher

F. Ransomware

Ransomware is a type of malware i.e. malicious software which encrypts all the data and information on a computing device thus rendering the data and information inaccessible and the system useless. Cyber-criminals threaten victim for decryption of data and demands payment of ransom in bitcoins. Also, despite paying ransom there is no guarantee that decryption keys will be shared for safe retrieval of information.

WannaCry

"WannaCry has been latest ransomware which caused much disturbance in the digital world and is a different kind of ransomware as compared to the usual traditional ones. This ransomware spreads by using a vulnerability in the implementation of Server Message Block (SMB) in Windows Systems.


User receives spammed message with archived attachment
Attachment is downloader malware that connects to URLs hosting the crypto-ransomware
The crypto-ransomware is downloaded onto the computer
Files in the affected computer are encrypted
A ransom message is displayed, stating the deadline and amount
Victims must use Tor browser to pay using Bitcoins

This is how it works:

WannaCry encrypts the computer's Hard drive on infected Windows Systems.

- There are two key components – a worm and a ransomware package.
- It spreads laterally between computers on the same LAN
- It also spreads through malicious email attachments
- The exploit is named as ETERNAL BLUE.
- Initial ransom amount was $300 USD which was increased to $600 in Bitcoin

G. OWASP TOP 10

In the domain of the Cyber Security OWASP is a key thing to know about latest treats in Cyber Security and in Application Security.

The Open Web Application Security Project (OWASP) is a non-profit organization dedicated to providing unbiased, practical information about application security. The OWASP Top 10 Web Application Security Risks was updated in 2017 to provide guidance to developers and security professionals on the most critical vulnerabilities that are commonly found in web applications, which are also easy to exploit. These 10 application risks are dangerous because they may allow attackers to plant malware, steal data, or completely take over your computers or web servers.

The following identifies each of the OWASP Top 10 Web Application Security Risks and offers solutions and best practices to prevent or remediate them.

1. Injection

Injection flaws, such as SQL injection, LDAP injection, and CRLF injection, occur when an attacker sends untrusted data to an interpreter that is executed as a command without proper authorization.

2. Broken Authentication and Session Management

Incorrectly configured user and session authentication could allow attackers to compromise passwords, keys, or session tokens, or take control of users' accounts to assume their identities.

3. Sensitive Data Exposure

Applications and APIs that don't properly protect sensitive data such as financial data, usernames, and passwords, or health information, could enable attackers to access such information to commit fraud or steal identities.

4. XML External Entity

Poorly configured XML processors evaluate external entity references within XML documents. Attackers can use external entities for attacks including remote code execution, and to disclose internal files and SMB file shares.

5. Broken Access Control

Improperly configured or missing restrictions on authenticated users allow them to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive documents, and modifying data and access rights.

6. Security Misconfiguration

This risk refers to the improper implementation of controls intended to keep application data safe, such as misconfiguration of security headers, error messages. containing sensitive information (information leakage), and not patching or upgrading systems, frameworks, and components.

7. Cross-Site Scripting

Cross-site scripting (XSS) flaws give attackers the capability to inject client-side scripts into the application, for example, to redirect users to malicious websites.

8. Insecure deserialization

Insecure deserialization flaws can enable an attacker to execute code in the application remotely, tamper or delete serialized (written to disk) objects, conduct injection attacks, and elevate privileges.

9. Using Components with Known Vulnerabilities

Developers frequently don't know which open source and third-party components are in their applications, making it difficult to update components when new vulnerabilities are discovered. Attackers can exploit an insecure component to take over the server or steal sensitive data.

10. Insufficient Logging and Monitoring

The time to detect a breach is frequently measured in weeks or months. Insufficient logging and ineffective integration with security incident response systems allow attackers to pivot to other systems and maintain persistent threats.

II. ADVANCES IN CYBERSECURITY ATTACKS PREVENTION (AS SECURITY RESEARCHER)

A. Prevention of System Exploitation

1. Update your OS and other software frequently, if not automatically. This keeps hackers from accessing your computer through vulnerabilities in outdated programs. For extra protection, enable Microsoft product updates so that the Office Suite will be updated at the same time. Consider retiring particularly susceptible software such as Java or Flash
2. Install programs such as Antimalware from Malwarebytes or Hitman Pro to protect the system against undetectable Trojan Files. And scan the system with it once in Week
3. Do not download any kind of software from unknown or from an illegal website. Only download from legitimate download sources
4. Do not download any attachment without scanning, despite sent from known email address.

B. Prevention of Phishing Attacks

1. Keep informed about latest phishing techniques
2. Think before you click
3. Install anti-phishing Toolbar
4. Verify site’s security
5. Use Antivirus Program.

C. Prevention from Man In The Middle Attack

1. never connect to open WIFI routers directly. If you wish to so, you can use a browser plug-in such as HTTPS Everywhere or ForceTLS. These plug-ins will help you establishing a secure connection whenever the option is available.
2. Use VPN in open Wi-Fi network to encrypt your connection.
3. Check connection in your browser, If it is not secure or if it is HTTP do not log in any credential with it.

D. Prevention from DOS

1. Purchase a lot of bandwidth. This may be the easiest solution, but it is also the most expensive. If an enterprise has tons of bandwidth, it makes perpetrating a DOS attack much more difficult, as it's more bandwidth that an attacker has to clog.
2. Use DOS attack identification and detection techniques to help differentiate between legitimate and malicious traffic. The first step in reducing the damage of how to prevent.
3. Prepare for DOS response. The use of throttling and rate-limiting technologies can reduce the effects of a DOS attack. One such response mode stops all new inbound connections in the event of a DOS attack.

E. Prevention from Wi-Fi Exploitation

1. Never connect to same Wi-Fi network which does not have any security associated with it. For example, if your Wi-Fi name is a TEST with WPA2 encryption and there is another Wi-Fi network named as a TEST which does not have any security, don’t connect it. It can be Attack of Wi-Fi Phishing.
2. Change you Router Admin Credentials
3. Set Up Strong Encryption.
4. Keep your Router Firmware Updated
5. Hide Your Wi-Fi Network
6. Enable MAC Filtering.
7. Avoid Open Public Networks.

F. Prevention of RANSOMWARE

1. Backup Your System Data Online or Offline.
2. Strong Security Guard: Antivirus, Antimalware, AntiSpyWare
3. Update OS and all Services/ Software’s
4. Use of SPAM filter on Email Service
5. Running on-time Remote Service and File Sharing
6. Disable Auto Execution of Files
7. Enable ‘Show File Extension’ on Windows PC

III. CONCLUSION

In this 21st Century of the world, there have been lots of advancements in Digital Life. We are using Internet Connection from messaging between one another to post photos and feeds in social media. With this advance, there are many digital threats following it. In violation of privacy compromisation of bank accounts. To prevent this kind of Digital threats first we should know about how they are doing it. That’s why there are lots of advances in this field to prevent them. Also, we must spread awareness about Cyber Security. There are two types of advances in Cyber Security, one with the perspective of Hacker to find out zero exploits in the system and network and another is with Perspective Security Researcher to prevent them against normal people. This Cyber Security Trend will be At Peak Point after some years.

REFERENCE

https://github.com/
https://www.veracode.com/