Short presentations

Google Dorks

A Google dork query, is a search string or custom query that uses advanced search operators to find information not readily available on a website. Google dorking, also known as Google hacking, can return information difficult to locate through simple search queries. There are different places to find ready to use Google Dorks. The first place is Google Hacking Database. This is a free public database containing thousands of Google Dorks for finding sensitive publicly available information.

What are Google Dork Operators? Below are Google dork operators: cache: provide the cached version of any website, e.g. cache:google.com. allintext: to get specific text contained within he specific web page, e.g. allintext: hacking tricks

Social Media Security

GDPR: General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live and outside of the European Union (EU). Approved in 2016, the GDPR went into full effect two years later.

How social media is used in crimes?

- Social Engineering
- Phishing attacks
- Fake Profiles
- Sharing every bit of information
- Hacking profiles
- Tracking activity through cookies and sessions and also by malicious script injection

Best practices: Social safe networking

1. Manage your privacy settings. ...
2. Remember: once posted, always posted. ...
3. Build a positive online reputation. ...
4. Keep personal info personal. ...
5. Protect your computer. ...
6. Know what action to take. ...
7. Use strong passwords. ...
8. Be cautious on social networking sites.

Wireless Sniffing

A wireless network is the way that a computer is connected to a router without a physical link.

Sniffing is a process of monitoring and capturing all data packets passing through given network. Attackers use sniffers to capture data which is not encrypted containing sensitive information such as password, account information etc.

Wireless sniffing is the practice of eavesdropping on communications within a wireless network by using special software or hardware tools. Both wired and wireless networks can be monitored or sniffed. Wireless networks generally are easier to sniff because they use radio signals as a method of communication. Computer networks divide information into frames which have data packets inside. Wireless sniffing might target frames, packets or both.

Packet sniffing can be used to monitor e-mail or other data being sent over a wireless network by others. It also can help a network administrator watch for and diagnose network problems.

Tools for Wireless Sniffing

- Iwconfig
- Wireshark
- TCPDump

Precautionary Measures on Sniffing Attacks

- Anti-virus tools
- Data Encryption
- Unencrypted messaging apps

Case studies on data breach

- Medibank
- Adhaar data breach
- Uber
- Plex
- CapticalOne
- Crypto.com

Security Policy

A cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media.

Who should write the cybersecurity policies?

- C-level business executives
- The legal department
- The human resources (HR)

Types of Security Policy

- Organizational
- System-specific
- Issue-specific

Steganography

Types

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Network or Protocol Steganography

Tools

- Stegosuite
- Steghide
- OpenPuff
- Xiao Steganography

Brute force attack

Brute force is a hacking technique used to find out the user credentials by trying out various possible credentials.

Tools

1. Aircrack-ng
2. Hashcat
3. Ncrack

Types

1) Simple brute force attack
2) Reverse brute force attack

How to stop brute force attacks

1) Monitor unsuccessful attempts
2) Strong password
3) 2FAs

Motives behind brute force attack

- Steal sensitive data

- Financial loss
- Attack on systems for malicious purposes
- Make websites unavailable
- Blackmail and extortion
- Reroute website traffic to commissioned ad sites
- Reputational damage

Security Protocols and Security Standards

Security Protocols

A sequence of operations that ensure the protection of data.

Security Standards

techniques generally outlined in published materials that attempt to protect the cyber environment.

PGP.

It stands for Pretty Good Privacy.

- It was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- It is an encryption program that provides cryptographic privacy and authentication for data communication.
- PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

HTTPs

- Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website
- HTTPS is encrypted in order to increase security of data transfer.

Firewalls

a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Intranet and Extranet

types:

Firewalls fall into six broad categories • Packet filters •Circuit level •Application level • Stateful multilayer •Transparent Firewall •Next Generation Firewalls

What is difference between firewall and next-generation firewall?

In plain terms, NGFWs have more layers of security built into them, to protect against more sophisticated threats. Crucially, they go beyond the static inspection that traditional firewalls are limited to, instead having application-level control.

How to hack wifi using wifite

Wifite is **a tool to audit WEP or WPA encrypted wireless networks**. It uses aircrack-ng, pyrit, reaver, tshark tools to perform the audit. This tool is customizable to be automated with only a few arguments and can be trusted to run without supervision.

Malware

Types

1) Virus, worms, spam, trojan horse, phishing, adware, ransomware

Anti-malware software

1) Avast, Malwarebytes

Mobile security

Ways to secure Mobile

- Set a PIN or password and use biometric authentication
- Set up remote wipe
- Backup phone data
- Avoid third-party apps
- Avoid jailbreaking your iPhone or rooting your Android
- Update operating systems often
- Use public wifi carefully

Securing personal devices

Turn on automatic updates

A CTIVATE MULTI-FACTOR AUTHENTICATION (MFA).

What is a passphrase? A passphrase uses four or more random words as your password. For example: ‘crystal onion clay pretzel’ .

HOW DO I RECOGNISE SCAM MESSAGES?

- Authority: is the message claiming to be from someone official, such as your bank?
- Urgency: are you told there is a problem, or that you have a limited time to respond or pay?
- Emotion: does the message make you panic, hopeful or curious?
- Scarcity: is the message offering something in short supply, or promising a good deal?
- Current events: is the message about a current news story or big event?