? Skill Recommendation: Security

Created on: 26.10.2024

ARP

The Adress Resolution Protocol on Networks.

Goals:

I know

- what ARP is
- what address resolution means
- where and how ARP is used

I can

- describe a basic example for using ARP

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

ARP Spoofing

Malicious use of ARP.

Goals:

I know

- what ARP spoofing is
- what ARP Request Poisoning is
- how ARP spoofing works

I can

- describe a basic scenario for ARP spoofing
- describe at least one method of identifying and/or preventing ARP spoofing

Links:

- bettercap Website: https://www.bettercap.org

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Asymmetric Encryption

Encrypting and Decrypting data with the help of a asymmetric keys.

Goals:

I know

- what asymmetric encryption is
- the basic mathematical idea behind asymmetric encryption
- what a private key is
- what a public key is
- how data can be signed in with asymmetric methods
- how data can be en-/decrypted with asymmetric methods

I can

- give an example for asymmetric encryption

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Backup Strategies

Strategies for saving data.

Goals:

I know

- what hot storage is
- what cold storage is
- what on premise means
- what off site means
- what RAID is
- what a NAS is
- what Cloud Storage means

I can

- name different storage media and discuss their advantages and disadvantages
- name examples for cloud storage providers
- describe example setups for backup strategies

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

BeEF for mitm attacks

The penetration testing tool BeEF.

Goals:

I know

- what BeEF is
- the attack vector BeEF is using for assessing security

I can

- setup BeEF for penetration testing
- perform a simple mitm attack on unsecured client communication with the help of BeEF

Links:

- Tutorial using BeEF: https://skanyi.github.io/blog/cyber-security/network-security-man-in-the-middle-attacks/

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Brute Force Hacking Passwords

Unauthorized access via finding a password with trial and error methods.

Goals:

I know

- what bruce force hacking is
- how brute force hacking works

I can

- explain a basic scenario for brute force hacking a password
- express the possible combinations needed for brute force hacking a password based on the available character set
- name defensive measures against brute force hacking a password

Links:

- Brute Force Attack: https://en.wikipedia.org/wiki/Brute-force_attack
- Brute force attack with Hydra: https://gtrekter.medium.com/brute-force-attack-with-hydra-and-kali-linux-3c4ede55d119

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Cookies

Client side storage of data for reuse with the help of cookies.

Goals:

I know

- what cookies in the context of internet browsing are

I can

- explain how cookies are set in a browser
- name examples for using cookies on a website
- check the active cookies for a website via the development tools
- clear specific cookies
- clear all cookies

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Cross-Site Scripting (XSS)

The concept of XSS and options for defense.

Goals:

I know

- what XSS means
- how XSS works
- how defensive measures against XSS can be implemented

I can

- create a simple scenario showcasing XSS
- check for potential XSS threats on my own website
- implement basic defensive measures against XSS on my own website

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Cross-Site-Request-Forgery (CSRF)

Stealing a users session for malicious intent and defending against it.

Goals:

I know

- what CSRF is
- when and how CSRF can occur

I can

- explain a basic scenario for CSRF
- describe methods to prevent CSRF

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Distributed Denial of Service Attack (DDos) concept

How Denial of Services (DoS) attacks are enforced via distribution.

Goals:

I know

- what a DDoS attack is
- which requirements need to be met to perform a DDoS attack
- why it is harder to defend against a DDoS attack than against a DoS attack

I can

- describe defensive measures against DDoS attacks

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Dumpster Diving

Acquiring data of 3rd parties via waste exploration.

Goals:

I know

- what dumpster diving is

I can

- explain a scenario for malicious use of data collected via dumpster diving
- name countermeasures to prevent dumpster diving

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

E-Mail Phishing

The concept of phishing attacks via e-mail and how do defend against them.

Goals:

I know

- what phishing is

I can

- name examples of indicators for identifying a phishing attack
- act in a manner that ensures the security of my own account and that of my company when receiving a phishing e-mail

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Long Term Support (LTS)

Supporting a product for a fixed and publicly disclosed amount of time.

Goals:

I know

- what LTS is
- what End of Life is

I can

- explain how LTS can effect customer choice in projects
- describe possible scenarios for users after End of Life is reached for a product

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Man-in-the-middle attack

An attack where the attacker intercepts and alters communication between two parties.

Goals:

I know

- what a man-in-the-middle attack is

I can

- describe a man-in-the-middle attack scenario
- explain countermeasures against man-in-the-middle attacks

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Metasploit

The penetration testing tool metasploit.

Goals:

I know

- what metasploit is

I can

- name use-cases for penetration testing with metasploit
- setup metasploit for use in my own test network
- simulate a simple attack in my own test network by detecting and abusing a vulnerability

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Pretty Good Privacy (PGP)

Using PGP for en-/decrypting data.

Goals:

I know

- what PGP is

I can

- setup the use of PGP on my computer
- encrypt data with PGP
- decrypt data with PGP
- sign data with PGP

Links:

- Pretty Good Privacy: https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- GnuPG: https://www.gnupg.org/

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

SQL injections and countermeasures in PHP

Risks and countermeasures for malicious code being infiltrated through user input.

Goals:

I know

- what an SQL injection is
- how SQL injections can be made possible in PHP by using passed variable values

I can

- implement basic precautions in my PHP code for increased security against SQL injections

Links:

- SQL Injection in PHP: https://www.php.net/manual/de/security.database.sql-injection.php

Maintainer:

HTL Rennweg (Ferdinand Kasper)

Domain Tag:

- Security

Tags:

Social Engineering

The psychological manipulation of people into performing actions or exposing confidential information in the context of information security.

Goals:

I know

- what social engineering in the context of information security is
- what I can do to lower the risk of becoming the victim of social engineering

I can

- describe a social engineering scenario

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Symmetric Encryption

Encrypting and Decrypting data with the help of a shared secret.

Goals:

I know

- what symmetric encryption is
- what ROT in the context of symmetric encryption stands for

I can

- give an example for symmetric encryption
- perform easy en- / decryption with the help of a key (e.g.: ROT)

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Tracking users with cookies

The method of tracking a users visited sites and actions on the internet with the help of cookies.

Goals:

I know

- how users can be tracked in the internet with the help of cookies
- which requirements need to be met for tracking users with cookies
- the difference between on-site and off-site tracking with cookies

I can

- describe a scenario in which users are tracked with the help of cookies
- name examples on how users can prevent getting tracked with the help of cookies
- name potential privacy issues when users are tracked with cookies

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Trojan horse (computing)

Malware that misleads users on its intent.

Goals:

I know

- what a Trojan horse in the context of IT is
- which security risks a Trojan horse implies on the own computer

I can

- describe measures to prevent the installation or remove a trojan horse

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

USB Drop

The concept and defense against attacks on the local network with the help of USB devices.

Goals:

I know

- what a USB drop attack is

I can

- describe a scenario for a USB drop attack
- describe variants of a USB drop attack
- explain countermeasures agains USB drop attacks

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Virtual Private Network (VPN) Overview

Encrypted connection over the Internet from a device to a network.

Goals:

I know

- what a VPN is
- what is needed to establish a VPN
- which security risks are avoided by using a VPN

I can

- create a VPN connection (hosted on own devices or with the help of 3rd party offers/software)
- describe scenarios where use of a VPN is recommended

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags:

Zero-day vulnerability

A previously unknown computer-software vulnerability,

Goals:

I know

- what a Zero-day exploit is
- ways to find out about a Zero-day exploit
- what window of vulnerability means in the context of a Zero-day exploit

I can

- discuss the concept of Zero-day protection
- describe countermeasures to Zero-day exploits

Links:

Maintainer:

HTL Rennweg (Franz Stimpfl)

Domain Tag:

- Security

Tags: