KAMK • University of Applied Sciences

Penetraatiotestaus

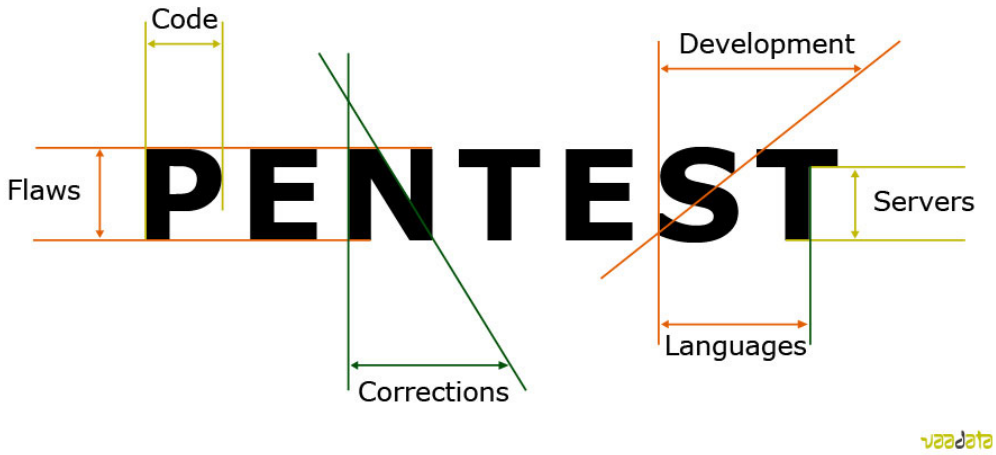
Jussi Ala-Hiiro

KAMK • University of Applied Sciences

Mitä on penetraatiotestaus?

- Penetraatiotestaus on prosessi, jossa simuloidaan tietokonejärjestelmään tai verkkoon kohdistuvaa hyökkäystä

- Turvallisuuden arvioimiseksi ja haavoittuvuuksien tunnistamiseksi, joita hyökkääjät voivat hyödyntää.

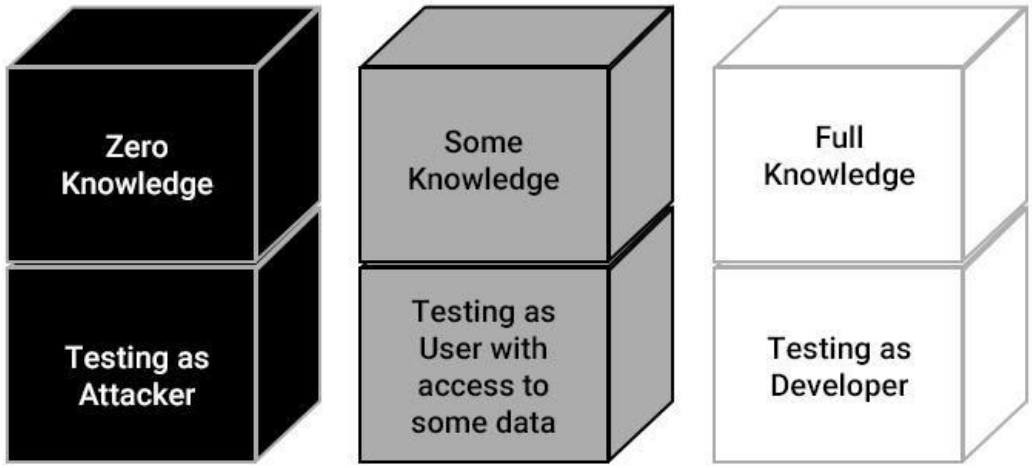


Kuvan lähde: https://www.vaadata.com/blog/7-questions-before-doing-a-penetration-test/

KAMK • University of Applied Sciences

Penetraatiotestauksen tyypit

- Black-box –testaus
- Gray-box –testaus
- White-box –testaus

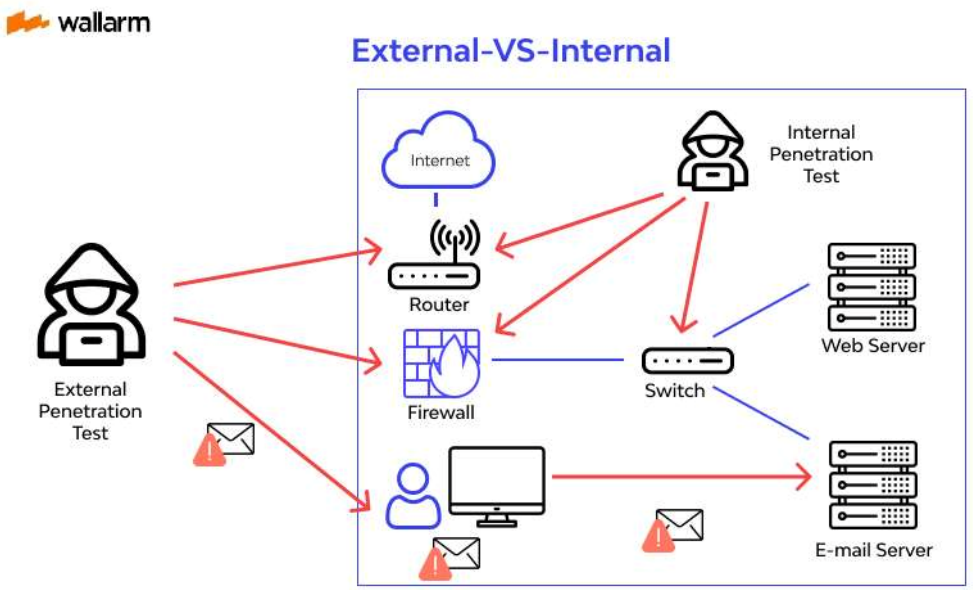


Kuvan lähde: https://www.appsealing.com/penetration-testing/

KAMK • University of Applied Sciences

Penetraatiotestauksen tekniikat

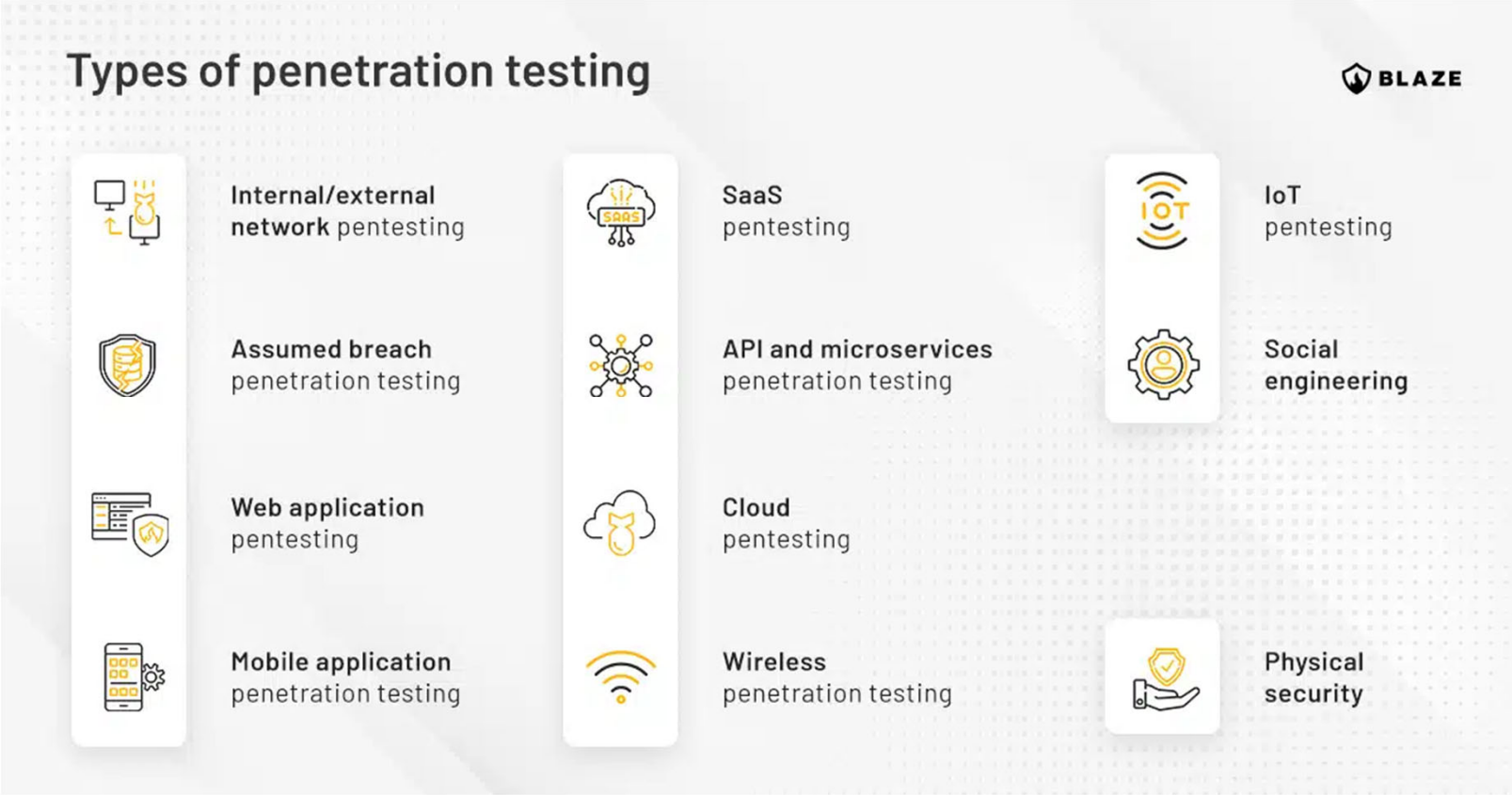
- Ulkoinen (external) testaus
- Sisäinen (internal) testaus
- Blind-testaus
- Double-blind -testaus
- Kohdennettu (targeted) testaus



Kuvan lähde: https://www.wallarm.com/what/what-is-penetration-testing

KAMK • University of Applied Sciences

Penetraatiotestauksen tapaukset

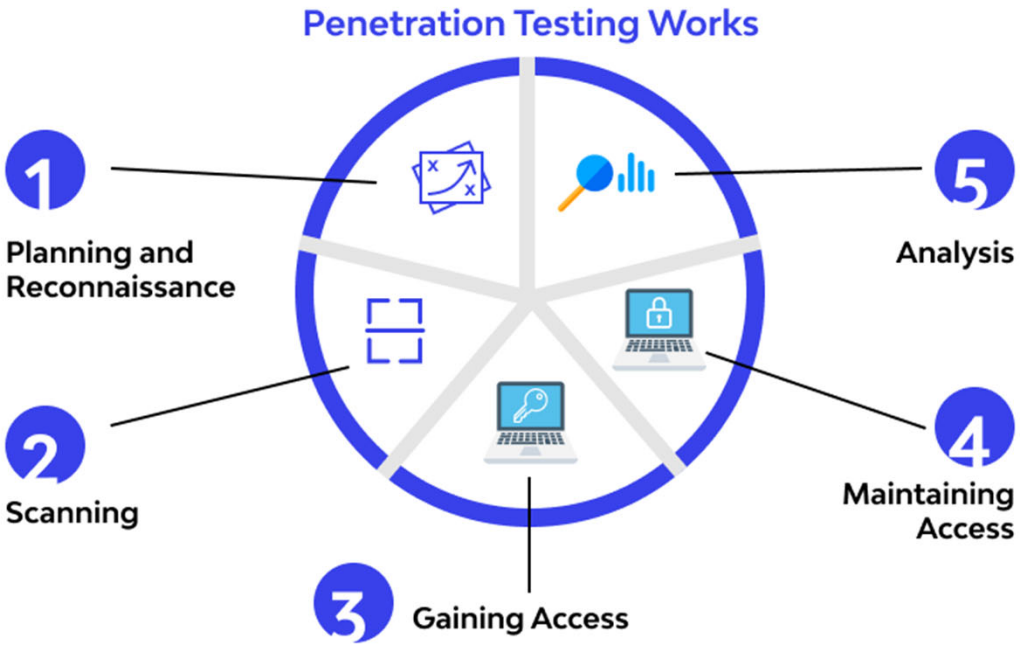


Kuvan lähde: https://www.blazeinfosec.com/post/types-of-penetration-testing/

KAMK • University of Applied Sciences

Penetraatiotestauksen vaiheet

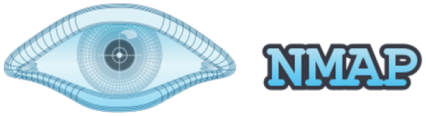
1. Tehtävänanto, sopiminen, suunnittelu, tiedustelu
2. Skannaus
3. Sisäänpääsyn saavuttaminen
4. Sisäänpääsyn ylläpitäminen
5. Analyysi, raportointi, korjaavien toimenpiteiden ohjeistaminen

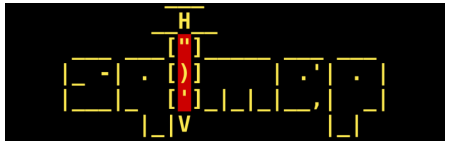


Kuvan lähde: https://www.wallarm.com/what/what-is-penetration-testing

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja





KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Kali Linux** is an open-source pen-testing apparatus that is kept up with and financed by Offensive Security Ltd. It upholds just Linux machines.
- Kali contains in excess of 600 infiltration testing instruments that are equipped towards different data security undertakings, for example, Penetration Testing, Security research, Computer Forensics, and Reverse Engineering.

- **Highlights of Kali Linux**
- A portion of the highlights of Kali Linux include:
- Full customization of Kali ISOs with live-form permitting us to make our own Kali Linux images
- ISO of Doom and Other Kali Recipes
- The Cloud rendition of Kali Linux can be set up effectively in the Amazon Elastic Compute Cloud
- It contains a lot of Meta bundle assortments which are total distinctive toolsets
- Full Disk Encryption (FDE)
- Accessibility highlights for outwardly weakened clients
- Live USB with Multiple Persistence Stores

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Wireshark** is an unquestionable requirement that have network convention analyzer.
- It is broadly used to catch live organization traffic for network investigating including dormancy issues, parcel drops, and pernicious movement on the organization.
- It permits the analyzers to block and investigate information that goes through the organization and converts it into an intelligible arrangement.

- **Highlights of Wireshark**
- Wireshark has incredible highlights that offers profound review of various conventions
- It accompanies a standard three-sheet parcel program and incredible presentation channels.
- Wireshark permits the information to be perused GUI or through TTY-mode TShark utility.
- It can peruse and compose diverse record configurations, for example, tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (packed and uncompressed) and that's just the beginning.
- The instrument offers unscrambling support for various conventions including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2.
- The apparatuses likewise permit review of VOIP traffic.

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **NMap** is an abbreviation of Network Mapper.
- Many frameworks and organization chairmen think that it's helpful for routine undertakings, for example, network stock, check for open ports, overseeing administration overhaul timetables, and observing host or administration uptime. It accompanies both order line and GUI interfaces

- **Highlights of NMap Port Scanning Tool**
- A portion of the highlights of NMap include:
- It finds weaknesses of an organization
- It distinguishes open ports
- It is utilized to decide network stock, network planning, support and resource the executives
- To find and adventure weaknesses in an organization
- It creates traffic to hosts on an organization, reaction investigation and reaction time estimation

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Metasploit** is a PC security project that gives the client significant data about security weaknesses.
- It tends to be utilized on web applications, workers, networks and so on. It has an order line and GUI interactive interface which interacts with Windows, Linux, and Apple Mac OS. It is a business item.
- However it accompanies a free restricted preliminary.

- **Metasploit Features:**
- A portion of the highlights of Metasploit include:
- It has an order line and GUI interface
- It deals with Linux, Windows and Mac OS X
- Network disclosure
- Vulnerability scanner import
- Module program
- Manual exploitation
- Basic exploitation

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Aircrack-ng** is an organization security pen testing instrument that accompanies a progression of utilities to survey Wi-Fi networks for potential weaknesses.
- It gives basic activities of checking, testing, assaulting, and breaking.
- The apparatus likewise assists with checking Wi-Fi cards and driver abilities and can be utilized to break WEP and WPA (1 and 2).

- **Highlights of Aircrack**
- The instrument is most popular for its capacity to break WEP and WPA-PSK with no validated customer, where it utilizes a factual technique for breaking WEP and beast power assault to break WPA-PSK.
- Aircrack-ng is a finished suite that incorporates a finder, parcel sniffer, logical devices, and WEP and WPA/WPA2-PSK wafers.
- Aircrack-ng suite contains devices, for example, airodump-ng, aireplay-ng, aircrack-ng, and airdecap-ng devices
- Airodump-ng is utilized to catch crude 802.11 bundles.
- Airplay-ng is utilized to infuse outlines into remote traffic which is then utilized via Aircrack-ng to break the WEP and WPA-PSK keys once sufficient information parcels have been caught.
- Airdecap-ng is utilized to decode caught documents and can likewise be utilized to strip remote headers.

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Zed Attack Proxy (ZAP)**
- ZAP is an unreservedly accessible open-source web application security scanner instrument. It discovers security weaknesses in web applications during the creating and testing stage.
- It gives mechanized scanners and a bunch of apparatuses that permit us to discover security weaknesses physically.

- **Highlights of ZAP**
- A portion of the highlights of ZAP computerized infiltration include:
- Intercepting intermediary worker
- Traditional and AJAX bugs
- Automated scanner
- Passive scanner
- Forced perusing
- Fuzzer
- Web Socket support

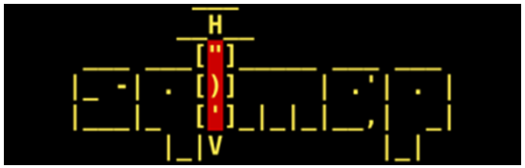
KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **John The Ripper** (otherwise called JTR) is a free and open-source password cracking apparatus that is intended to break even exceptionally lengthy passwords.
- It is quite possibly the most mainstream secret word testings and breaking programs.
- It is most usually used to perform word reference assaults. It assists with distinguishing frail secret word weaknesses in an organization.
- It likewise upholds clients from savage power and rainbow break assaults. It is accessible for UNIX, Windows, DOS, and OpenVMS. It arrives in a master and free structure.

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja



- **SQLmap** is an open-source tool.
- However, it is an exceptionally amazing infiltration testing apparatus that master pen analyzers use to recognize and abuse SQL Injection weaknesses affecting various data sets.
- It is an extraordinary pen-testing apparatus that accompanies a powerful discovery motor that can recover valuable information through a solitary order.

- **Highlights of SQLmap**
- Using a word reference-based assault, SQLmap assists with programmed acknowledgment of secret phrase hash arrangements and backing for breaking them.
- It effectively looks for explicit data set names, tables, or segments across the whole information base, which is helpful in recognizing tables that contain application accreditations containing string like name and pass.
- SQLmap supports to build up an out-of-band TCP association between the data set worker and the assailant machine furnishing client with intuitive order fast or a meterpreter meeting.
- The instrument upholds downloading and transferring any document from/to the information bases it is viable with.

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **W3af** is a Web Application Attack and Audit Framework.
- It gets web applications by finding and exploiting all web application weaknesses. It recognizes in excess of 200 weaknesses and diminishes of your site's general danger openness.
- It distinguishes weaknesses like SQL infusion, Cross-Site Scripting (XSS), Guessable Credentials, Unhandled application blunders, and PHP misconfigurations.

- **W3af highlights:**
- A portion of the highlights of W3af include:
- Integration of web and intermediary workers into the code
- Injecting payloads into pretty much all aspects of the HTTP demand
- Proxy support
- HTTP Basic and Digest validation
- UserAgent faking
- Add custom headers to reports
- Cookie handling
- HTTP reaction store
- DNS store
- File transfer utilizing multipart
- It's a free instrument

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **MobSF** or Mobile Security Framework is an open-source security evaluation instrument that is equipped for performing both dynamic and static examinations.
- This across-the-board device that has functionalities for Android, Windows and iOS stages can likewise perform pen testing and malware investigation.
- MobSF upholds parallels for portable applications like APK, APPX, and IPX and furthermore upholds zipped source code.
- With the assistance of REST APIs, MobSF can be incorporated with DevSecOps or CI/CD pipelines. With this open-source SAST apparatus, engineers can feature weaknesses ahead of schedule during the advancement stage itself.

- **Highlights of MobSF**
- New experiment for Network Security design and dissecting SSL authentications.
- Show LoC.
- Genymotion cloud support.
- Added numerous Frida scripts for root location.

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Burpsuite** is a graphical apparatus for testing Web Application security.
- It is created by PortSwigger Web Security. It was created to give an answer for web application security checks.
- It has three versions, for example, local area release which is a free one, a Professional version, and a Special-feature release. Local area version has altogether diminished usefulness.
- Burp Proxy permits manual analyzers to catch all solicitations and reactions between the programs and the objective application, in any event, when HTTPS is being utilized.

- **Highlights of Burp Suite**
- It has an incredible intermediary segment that performs man-in-the-center assaults to capture the exchange of information and allows the client to change the HTTP(S) correspondence going through the program.
- Burp Suite helps try out-of-band (OOB) weaknesses (those that can't be identified in a customary HTTP demand reaction) during manual testing.
- The apparatus discovers covered up target functionalities through a programmed revelation work.
- The instrument offers quicker threat constraining and fluffing capacities which empower pen testers to send the custom succession of HTTP demands that contain payload sets, which radically diminishes the time spent on various errands.
- Burpsuite Pro offers a component to effortlessly build a Cross-Site Request Forgery (CSRF) Proof of Concept (POC) assault for a given solicitation.
- The apparatus additionally works with more profound manual testing as it can give a view to reflected or put away information sources.
- The application store gives admittance to many local area created modules which are composed and tried by Burp clients.

KAMK • University of Applied Sciences

Penetraatiotestauksen työkaluja

- **Intruder** is an amazing, robotized infiltration testing device that finds security shortcomings across your IT climate.
- Offering industry-driving security checks, persistent observing and a simple to-utilize stage, Intruder guards organizations of all sizes from malicious programmers.

- **Highlights of Intruder**
- Best-in-class danger inclusion with more than 10,000 security checks
- Checks for arrangement shortcomings, missing patches, application shortcomings (like SQL infusion and cross-site prearranging) and the sky is the limit from there
- Automatic investigation and prioritization of sweep results
- Intuitive interface, speedy to set-up and run your first outputs
- Proactive security observing for the most recent weaknesses
- AWS, Azure and Google Cloud connectors
- API combination with your CI/CD pipeline

KAMK • University
of Applied Sciences

www.kamk.fi

KAMK • University of Applied Sciences

Lähteet

- https://securetriad.io/penetration-testing/
- https://securetriad.io/popular-penetration-testing-tools/
- https://www.blazeinfosec.com/post/types-of-penetration-testing/
- https://www.appsealing.com/penetration-testing/
- https://www.wallarm.com/what/what-is-penetration-testing
- https://www.wallarm.com/what/15-must-have-tools-for-penetration-testing
- https://skillsforall.com/course/ethical-hacker

KAMK • University
of Applied Sciences

www.kamk.fi