Penetrační a aplikační testy

Ing. Vladimír Lazecký
vladimir.lazecky@viavis.cz

VIAVIS střežíme podstatné

Cíl a smysl přednášky

- ✓ Pochopení, co je penetrační a aplikační test
  - ✓ Co lze od testu očekávat a co ne
  - ✓ Proč a kdy mají testy smysl
  - ✓ Jak se testuje
  - ✓ Přehled metodik
  - ✓ Jak test zadat

Vědět, kde a jak hledat…

Penetrační testování a testy aplikací

- ✓ Penetrační test:
  - ✓ Prověření úrovně bezpečnosti formou testu
  - ✓ Testování bezpečnostních vlastností
  - ✓ Simulace bezpečnostního incidentu:
    - ✓ Pokus o průnik
    - ✓ Snaha o znefunkčnění
    - ✓ Detekce útoku…

Penetrační test x aplikační test

- ✓ Penetrační test:
  - ✓ Penetrační test – testování bezpečnosti
- ✓ Aplikační test:
  - ✓ Test funkčních vlastností
  - ✓ Test nefunkčních vlastností – zátěžové testy, přístupové testy…
- ✓ Kombinované testy:
  - ✓ Zahrnují bezpečnostní, funkční i výkonové testy
  - ✓ Výhody/nevýhody

Penetrační testy - kategorizace

- ✓ Mnoho různých hledisek a typů testů
- ✓ Podíl lidského faktoru:
  - ✓ **Automatizované testy:**
    - ✓ Algoritmický test
    - ✓ Scan zranitelností – vulnerability scan
    - ✓ Výhody:
      - ✓ Opakovatelnost
      - ✓ Srovnatelnost výsledků
      - ✓ Nižší náklady
    - ✓ Nevýhody:
      - ✓ Omezení algoritmizací

Penetrační testy - kategorizace

- ✓ **„Ručně vedené“ testy:**
  - ✓ Testy dle konkrétní metodiky
  - ✓ Kreativní testy
    - ✓ Výhody:
      - ✓ Opakovatelnost – u testů dle metodik
      - ✓ Kreativita – hloubkové využití zranitelností
      - ✓ Odhalení chyb mimo algoritmus
    - ✓ Nevýhody:
      - ✓ Vyšší náklady
      - ✓ Nižší míra opakovatelnosti a srovnání

Penetrační testy – kategorizace – součinnost testovaného subjektu

- ✓ **Kooperativní testy:**
  - ✓ Testy v součinnosti s testovaným subjektem
  - ✓ Zaměření se na konkrétní slabiny a systémy
  - ✓ Často ve spojení s hardeningem:
    - ✓ Testování konfigurací a zabezpečení
  - ✓ Výhody:
    - ✓ Externí pohled
    - ✓ Test je cílen dle potřeb
  - ✓ Nevýhody:
    - ✓ Test je veden předpokládanou cestou

Penetrační testy – kategorizace – součinnost testovaného subjektu

- ✓ **Nekooperativní testy:**
  - ✓ Testy bez vědomí testovaného subjektu
  - ✓ Součástí jsou obvykle i testy bezpečnostních procesů:
    - ✓ Zda je test zachycen
    - ✓ Jak na test je reagováno
    - ✓ Postup testu se dle reakce upravuje
    - ✓ Růst „brutality“
  - ✓ Výhody:
    - ✓ Procesy jsou součástí testování
    - ✓ Kreativní vedení testu
  - ✓ Nevýhody:
    - ✓ Vyšší náklady
    - ✓ Nižší míra opakovatelnosti a srovnání

Penetrační testy – kategorizace – dle znalostí testujícího

- ✓ **Blind test**
  - ✓ **Žádná vstupní znalost**
  - ✓ Simulace postupu reálného útočníka
  - ✓ Součástí je OSINT
    - ✓ Zjištění informací z veřejných zdrojů
    - ✓ Testovaným publikované zranitelnosti
    - ✓ Výstup pro snižování rizik
  - ✓ Výhody:
    - ✓ Obraz, jak může být úspěšný reálný externí útočník
    - ✓ Odhalení publikovaných slabin
  - ✓ Nevýhody:
    - ✓ Test může být zaměřen zcela mimo záměr
    - ✓ Test nemusí odhalit všechny slabiny

Penetrační testy – kategorizace – dle znalostí testujícího

- ✓ **Test se znalostí**
  - ✓ **Testující má částečnou znalost o subjektu**
  - ✓ Simulace útoku interním zaměstnancem
  - ✓ Součástí může být
    - ✓ Prověření přístupu, konfigurací
    - ✓ Stav interního prostředí
  - ✓ Výhody:
    - ✓ Využití technik útoku s přístupem do interního systému
    - ✓ Odhalení „bílých míst“
  - ✓ Nevýhody:
    - ✓ Obtížně se realizuje jako nekooperativní test
    - ✓ Nákladné testy v případě nekooperativních testů

Penetrační testy – kategorizace – dle předmětu testování

- ✓ **Technické testy**
  - ✓ **Předmětem testování je IT systém**
  - ✓ Cílem:
    - ✓ Odhalení chyb návrhu, architektury
    - ✓ Konfigurační chyby
    - ✓ Integrační chyby
    - ✓ Provozní chyby
  - ✓ Výhody:
    - ✓ Existence metodik a měřitelnost
    - ✓ Testuje se technika
  - ✓ Nevýhody:
    - ✓ Žádný systém není provozován bez lidského faktoru
    - ✓ Limity odhalení interface Hardware/Software/Liveware

Penetrační testy – kategorizace – dle předmětu testování

- ✓ **Sociotechnické testy**
  - ✓ **Předmětem testování je uživatel a jeho chování**
  - ✓ **Etický kodex testování**
  - ✓ Cílem:
    - ✓ Testy uživatelských návyků, dodržování pravidel, jejich znalost, schopnost test odhalit
  - ✓ Metody:
    - ✓ Manipulace, zneužití důvěry, podvrhy
  - ✓ Výhody:
    - ✓ Motivace zaměstnanců k dodržování pravidel
  - ✓ Nevýhody:
    - ✓ Ohrožení důvěry a firemní kultury

Penetrační testy – možnosti provedení

- ✓ **Testy lze vhodně kombinovat**
  - ✓ Technické testy x sociotesty
    - ✓ Phishing, vishing – test průniku do systému
  - ✓ Testy se znalostí x bez znalosti = tzv. GREY test
- ✓ Kreativní testy
  - ✓ Testovací scénář na míru

Penetrační testy – etapy penetračního testu

- ✓ Přípravná etapa:
  - ✓ Cíl testu
  - ✓ Získávání informací – OSINT, konzultace
  - ✓ Plánování testu:
    - ✓ Volba technik testování
    - ✓ tvorba testovacích scénářů
  - ✓ Validace scénářů

- ✓ Detekce zranitelností:
  - ✓ Výstupy OSINT:
    - ✓ Smlouvy, systémy..

Penetrační testy – etapy penetračního testu

- ✓ Testování
  - ✓ Realizace testovacích scénářů
  - ✓ Zvyšování brutality testů

  - ✓ Detekce zranitelností, hodnocení, částečné posouzení rizik
  - ✓ Návrhy protiopatření

Penetrační testy – etapy penetračního testu

- ✓ Zpracování výsledků a předání zprávy
  - ✓ Obsah zprávy:
    - ✓ Metodika
    - ✓ Popis realizace
    - ✓ Zjištěné zranitelnosti s hodnocením
    - ✓ Návrh jejich odstranění - protiopatření

Penetrační testy – metodiky

- ✓ Open Source Security Testing Methodology Manual (OSSTMM)
- ✓ Open Web Application Security Project (OWASP)
- ✓ Web Application Security Consortium Threat Classification (WASC-TC)
- ✓ Penetration Testing Execution Standard (PTES)
- ✓ Information Systems Security Assessment Framework (ISSAF)

Penetrační testy – metodiky

https://www.isecom.org/OSSTMM.3.pdf

Penetrační testy – OSSTMM

- ✓ Často používaná metodika
- ✓ Pokus o přístup k testování systematickým a vědeckým způsobem
- ✓ Lze získat pro testování certifikaci
  - ✓ Do jisté míry univerzální metodika

OSSTM - hodnocení a validace chyb testování

- ✓ Typy chyb testujícího – musí s nimi pracovat:
  - ✓ **False positive** – odhalená pravda je ve skutečnosti lež
  - ✓ **False negative** – odhalená lež je ve skutečnosti pravda
  - ✓ **Gray positive** – na všechny dotazy se jeví odpověď jako pravdivá, ačkoli není
  - ✓ **Gray negative** – na všechny dotazy se jeví odpověď jako lež, ačkoli není
  - ✓ **Specter** – některé odpovědi se jeví jako pravda, některé jako lež, ale realita je neznámá
  - ✓ **Indiscretion** – odpovědi jsou jak pravdivé, tak lži, záleží, kdy se ptáte
  - ✓ **Entropy Error** – odpověď se ztratí v šumu přenosu
  - ✓ **Falsification** – odpověď se mění v závislosti na místě a způsobu dotazu
  - ✓ **Sampling error** – odpověď nezahrnuje celek, ale pouze vzorek
  - ✓ **Constraint** – odpověď je limitována použitím konkrétních nástrojů a jejich omezením
  - ✓ **Propagation** – odpověď je předpokládána bez testu
  - ✓ **Human error** – chyba vyplývající z přístupu a schopností testujícího

Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

https://owasp.org/

Penetrační testy – OWASP

✓ Mnoho použitelných metodik, zdrojů informací a standardů

OWASP Project Inventory (254)

All OWASP tools, document, and code library projects are organized into the following categories:

Flagship Projects: The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole.
Lab Projects: OWASP Labs projects represent projects that have produced an OWASP reviewed deliverable of value.
Incubator Projects: OWASP Incubator projects represent the experimental playground where projects are still being fleshed out, ideas are still being proven, and development is still underway.

List of Projects by Level or Type

Flagship Projects 

- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSRFGuard

https://owasp.org/projects/

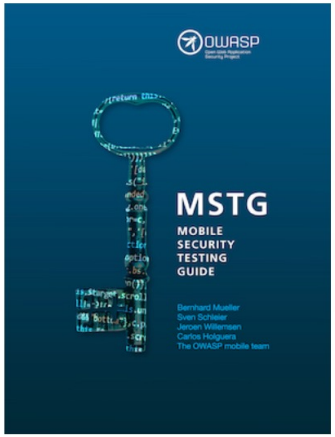
Penetrační testy – OWASP

✓ Testy mobilních aplikací – dobrý zdroj

Mobile Security Testing Guide (MSTG)

The MSTG is a comprehensive manual for mobile app security testing and reverse engineering for iOS and Android mobile security testers with the following content:

- Mobile platform internals
- Security testing in the mobile app development lifecycle
- Basic static and dynamic security testing
- Mobile app reverse engineering and tampering
- Assessing software protections
- Detailed test cases that map to the requirements in the MASVS.



You can contribute and comment in the GitHub Repo. An online book version of the current master branch is available on Gitbook.

https://owasp.org/www-project-mobile-security-testing-guide/

Web Application Security Consortium Threat Classification - WASC-TC

http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

Web Application Security Consortium Threat Classification - WASC-TC

- ✓ Přehled a klasifikace hrozeb aplikací

Attacks	Weaknesses
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross-Site Scripting	Information Leakage
Cross-Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti-automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation
HTTP Request Smuggling	Insufficient Session Expiration
HTTP Request Splitting	Insufficient Transport Layer Protection
Integer Overflows	Server Misconfiguration

Web Application Security Consortium Threat Classification - WASC-TC

✓ Ukázka:

Buffer Overflow

last edited by Robert Auger 11 years, 9 months ago Page history

Project: WASC Threat Classification
Threat Type: ***Attack***
Reference ID: WASC-7

Buffer Overflow

A Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold. Exploiting a buffer overflow allows an attacker to modify portions of the target process' address space. This ability can be used for a number of purposes, including the following:

- Control the process execution
- Crash the process
- Modify internal variables

The attacker's goal is almost always to control the tar… memory that can be modified, directly or indirectly, using the … …n

References

General Reference
"Intel 64 and IA-32 Architectures Software Developer's Manual"
[1] http://download.intel.com/design/processor/manuals/253665.pdf

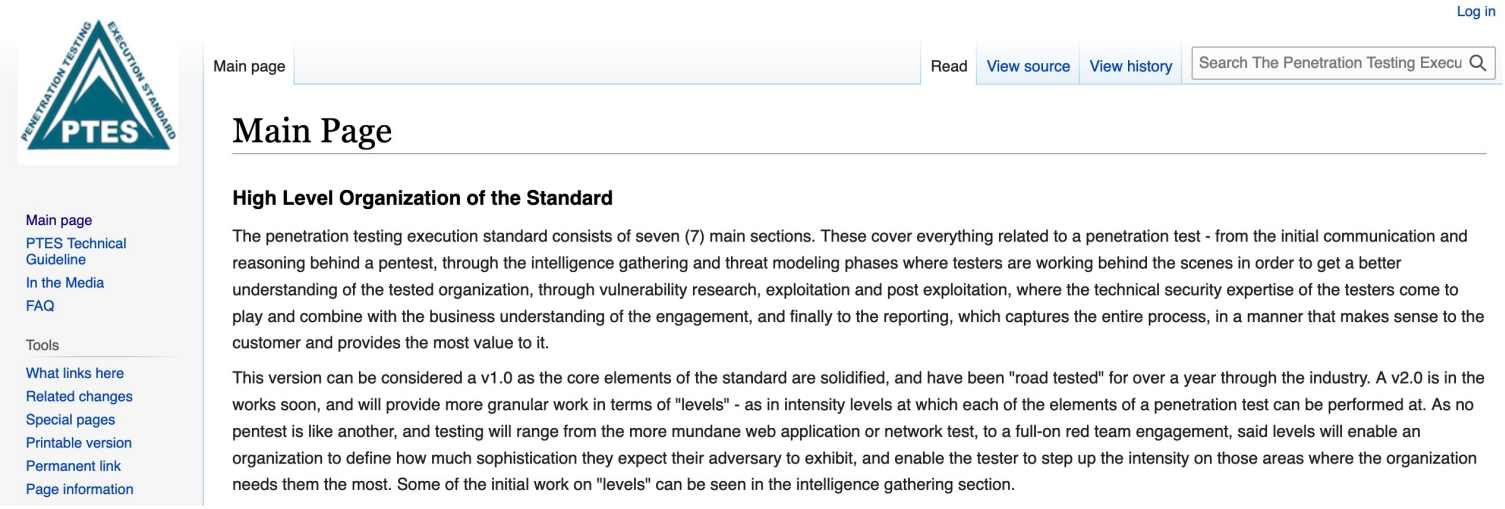
Buffer Overflow
"Smashing the Stack for Fun and Profit", By Aleph One – Phrack 49
[2] http://www.phrack.com/issues.html?issue=49&id=14#article

"w00w00 on Heap Overflows" By Matt Conover and w00w00 Security Team.
[3] http://www.w00w00.org/files/articles/heaptut.txt

"The Shellcoder's Handbook, 2ed." By Anley, C., Heasman, J., Linder, F., & Richarte, G.
[4] Wiley Press

http://projects.webappsec.org/w/page/13246916/Buffer%20Overflow

Penetration Testing Execution Standard (PTES)



http://www.pentest-standard.org/index.php/Main_Page

PTES

- ✓ Obsahuje 7 fází testu
  - ✓ Specifikační fáze:
    - ✓ Rozsah testu
    - ✓ Cíle testu
    - ✓ Časová omezení
    - ✓ Jiné omezující podmínky
  - ✓ Sběr informací:
    - ✓ Metodika OSINT

PTES

OSINT

Open Source Intelligence (OSINT) takes three forms; Passive, Semi-passive, and Active.

- **Passive Information Gathering**: Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. This type of profiling is technically difficult to perform as we are never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet. This means we can only use and gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered from a third party.

- **Semi-passive Information Gathering**: The goal for semi-passive information gathering is to profile the target with methods that would appear like normal Internet traffic and behavior. We query only the published name servers for information, we aren't performing in-depth reverse lookups or brute force DNS requests, we aren't searching for "unpublished" servers or directories. We aren't running network level portscans or crawlers and we are only looking at metadata in published documents and files; not actively seeking hidden content. The key here is not to draw attention to our activities. Post mortem the target may be able to go back and discover the reconnaissance activities but they shouldn't be able to attribute the activity back to anyone.

- **Active Information Gathering**: Active information gathering should be detected by the target and suspicious or malicious behavior. During this stage we are actively mapping network infrastructure (think full port scans nmap –p1-65535), actively enumerating and/or vulnerability scanning the open services, we are actively searching for unpublished directories, files, and servers. Most of this activity falls into your typically "reconnaissance" or "scanning" activities for your standard pentest.

http://www.pentest-standard.org/index.php/Intelligence_Gathering#Mobile_Footprint

PTES

- ✓ Obsahuje 7 fází testu
  - ✓ Modelování hrozeb
    - ✓ Využití výsledků OSINT
    - ✓ Východisko pro tvorbu testovacích scénářů
  - ✓ Analýza zranitelností
  - ✓ Exploitace
  - ✓ Post exploitace
  - ✓ Reporting

- **Sada technických návodů – problém aktuálnosti**

PTES

Page | Read | View source | View history | Search The Penetration Testing Execu

PTES Technical Guidelines

This section is designed to be the PTES technical guidelines that help define certain procedures to follow during a penetration test. Something to be aware of is that these are only baseline methods that have been used in the industry. They will need to be continuously updated and changed upon by the community as well as within your own standard. Guidelines are just that, something to drive you in a direction and help during certain scenarios, but not an all encompassing set of instructions on how to perform a penetration test. Think outside of the box.

Contents [hide]

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

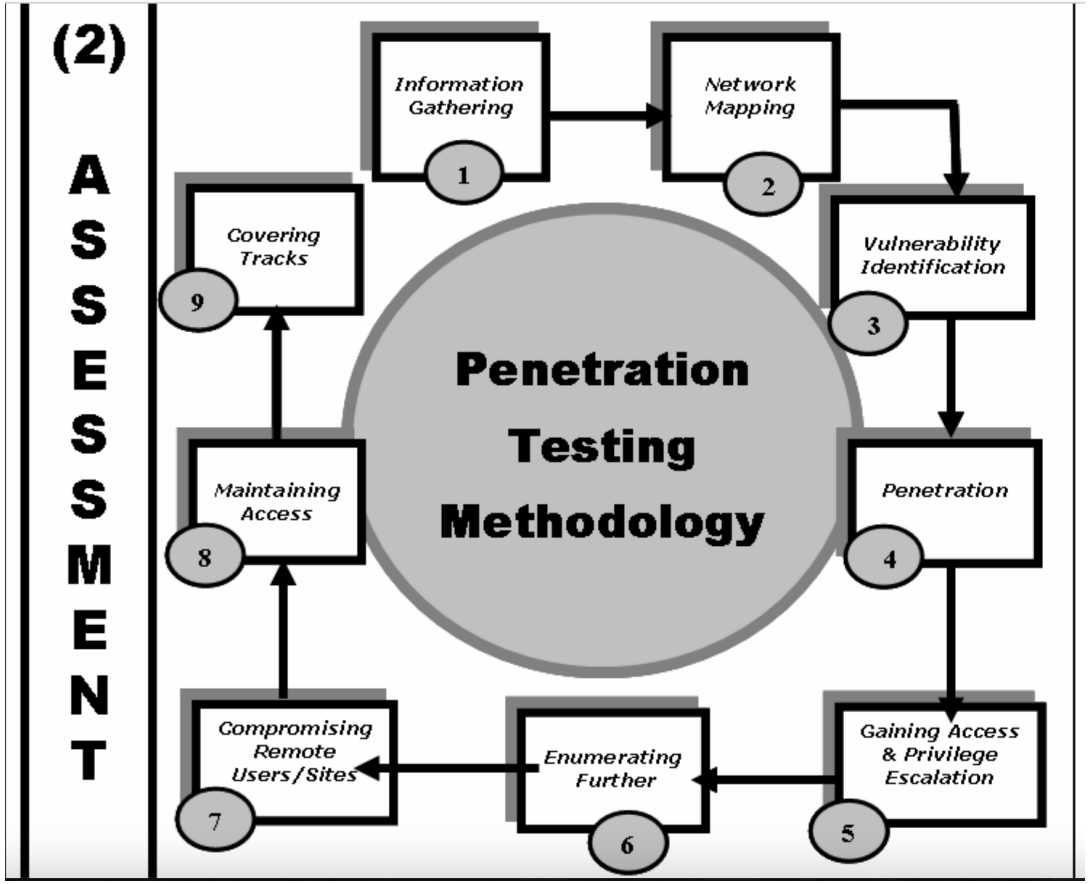
Information Systems Security Assesment Framework – ISSAF

- ✓ Nejde o přímou metodiku penetračního testování
- ✓ Rámec hodnocení bezpečnosti informačních systémů

https://untrustednetwork.net/files/issaf0.2.1.pdf

Information Systems Security Assesment Framework – ISSAF

- ✓ Obdobné fáze, navíc je přidáno ničení stop



https://untrustednetwork.net/files/issaf0.2.1.pdf

NIST – National Institute for Standard and Technology

- ✓ Framework pro Cyber Security, hodnocení a testování

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

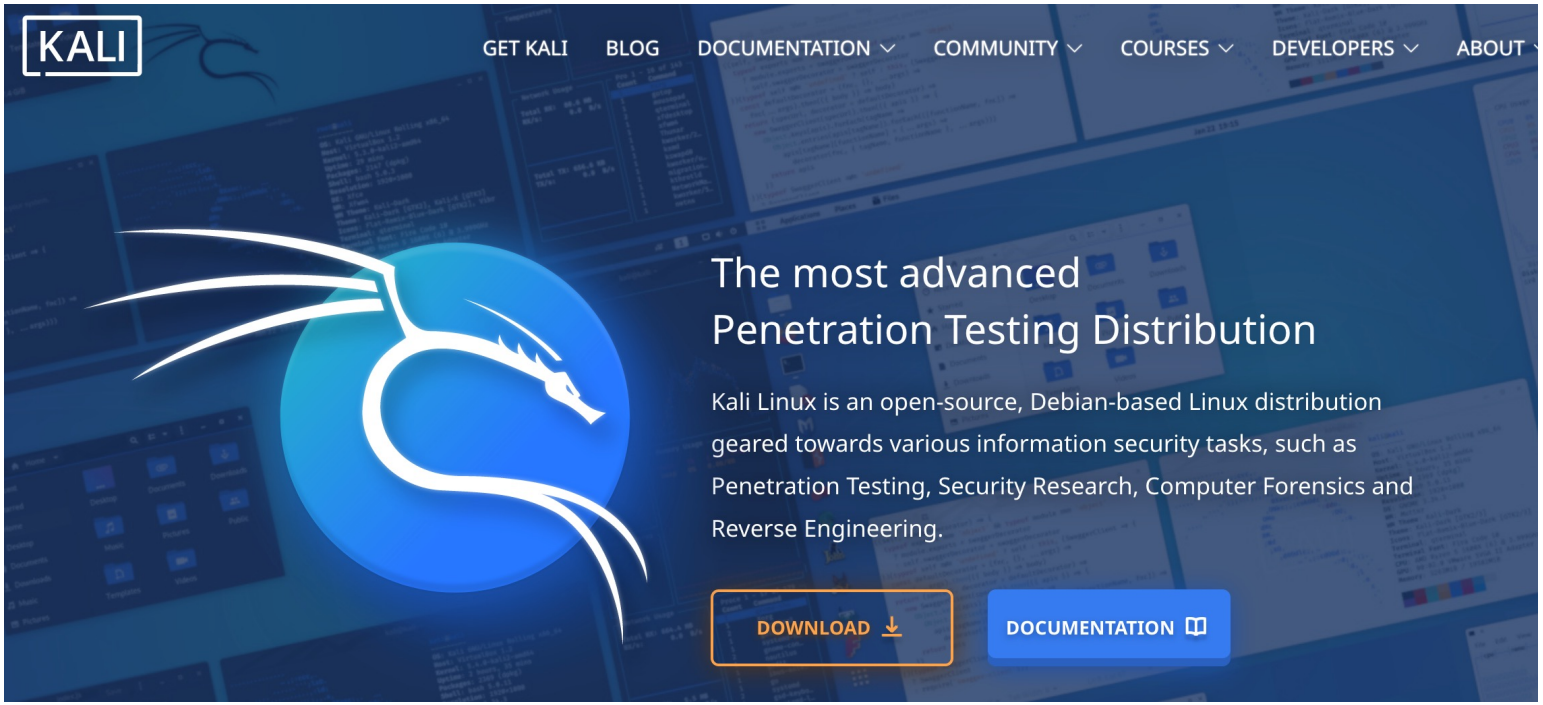
April 16, 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Kde hledat nástroje pro penetrační testy

https://geekflare.com/web-penetration-testing-tools/

Kde hledat nástroje pro penetrační testy



https://www.kali.org/

Penetrační testy – jak je zadat

- ✓ Cíle testování
- ✓ Způsob testování
  - ✓ Metodika
  - ✓ Typ testu…
- ✓ Limitující podmínky

- ✓ Smlouva
- ✓ Závazek na ničení stop

Máte nějaké dotazy?

Děkuji za pozornost

Ing. Vladimír Lazecký