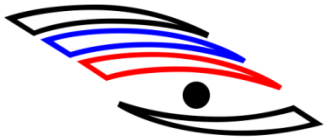
Zuzana Vargová
CSIRT.SK - Jednotka pre riešenie počítačových incidentov

Penetračné testovanie

Úvod do informačnej bezpečnosti
LS 2015/2016
17.5.2016



CSIRT.SK
www.csirt.gov.sk

CSIRT.SK

Computer Security Incident Response Team Slovakia – CSIRT.SK

- zabezpečenie ochrany národnej informačnej a komunikačnej infraštruktúry – NIKI a kritickej informačnej infraštruktúry

- služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov
  - spolupráca s vlastníkmi a prevádzkovateľmi NIKI, telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy, ...),
  - budovanie a rozširovanie poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti,
  - aktívna kooperácia so zahraničnými organizáciami,
  - reprezentácia SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

Penetračný test a.k.a. *pentest*, *ethical hacking*

- *„ ... attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.“ – Wiki*

Ciele:

- Určenie, či je istá skupina vektorov útoku vykonateľná
- Identifikácia zraniteľností vysokého stupňa, ktoré vyplynú z kombinácie menej závažných nedostatkov, zneužitých v určitom poradí
- Identifikácia zraniteľností, ktoré je náročné až nemožné odhaliť automatickou detekciou chýb systému
- Určenie potenciálnych dopadov úspešného útoku
  - Finančná stránka
  - Morálne straty
  - Ohrozenie ľudských životov
- Testovanie schopností vlastníkov (správcov, administrátorov, používateľov, údržbárov, ... ☺) systému pri detekcií a riešení incidentu
- Poskytnutie dôkazov na podporu zvýšenia investícií do bezpečnosti organizácie

Legal disclaimer...

- Prednáška je pripravená pre vzdelávacie účely.
- Postupy, nástroje a príklady nie sú určené na použitie bez písomného súhlasu testovanej strany.
- Testovanie bez predchádzajúceho súhlasu môže byť klasifikované ako trestný čin!

Pentest

- Pri penteste ide o **simuláciu činnosti** vonkajšieho alebo vnútorného útočníka, snažiaceho sa prelomiť bezpečnosť organizácie: exploitovať kritické systémy, získať prístup k citlivým dátam, ...

- V závislosti od okruhu testovania možno použiť aj sociálne inžinierstvo či zamerať sa na fyzickú bezpečnosť– nie štandardné...
- Isté prvky sociálneho inžinierstva sa dajú použiť vždy (odhad nasledujúceho hesla a podobne)

Postup testovania

Čo by robil útočník?

- Reconnaisance
  - Získavanie informácií o cieli: IP adresy, DNS info, typ/verzia systému, dáta o zamestnancoch, ich kontách a prihlasovacích údajoch
- **Scanning and Enumeration**
  - Súhrn znalostí o cieli, identifikácia, ktoré časti môžu byť zraniteľné
- **Penetration**
  - Získanie prístupu zneužitím zraniteľností a obídením bezpečnostných mechanizmov
- Denial of Service
  - Netreba komentár...
- Escalation and Maintaining Access
  - Kroky na vytvorenie a udržanie stabilného a nenápadného prístupu do systému
- Covering Tracs and Hiding
  - Zahladenie stôp

Postup testovania

- Stanovenie okruhu testovania (scope)
- Získavanie informácií o cieli
  - Príklad – www.shodanhq.com: net:85.248.149.56
  - Príklad – nmap, scanovanie siete
- Pokusy o exploitáciu na získanie prístupu do systému a eskaláciu privilégií
  - Scanery, manuálne testovanie a útoky
- Pokus o získanie citlivých dát
- Upratovanie – zahladenie stôp - a reportovanie výsledkov

Typy testov

- 2 základné typy pentestu:
  - „white box“ – určité info sú známe, napríklad výstup vulnerability assesmentu
  - „black box“ – simulácia útoku bez znalosti prostredia (zero-knowledge)
- Podľa predmetu testovania:
  - Interný – LAN
  - Externý – webové aplikácie a služby
- Metóda testovania:
  - automatické – scanovacie softvéry, online nástroje, skripty, ...
  - manuálne – najmä na overenie výsledkov, vylúčenie FP

Čo robíme my?

- Penetračné testy webových aplikácií a interné testy infraštruktúry
  - rozsah podľa dohody a podľa potreby ☺
- Faktory:
  - Požiadavky organizácie
  - Typ aplikácie
    - statický web či portál, prihlasovanie, citlivosť dát...
  - Čas...
- Pri weboch +/- OWASP metodika
- Pri interných testoch postup záleží od prípadu

Pred testom…

- Všetko ošetriť dohodou/zmluvou/súhlasom s podpismi oboch(všetkých zúčastnených) strán

- Naozaj VŠETKO ☺
  - URL s testovanými aplikáciami
  - Cieľové IP adresy
  - IP adresy, z ktorých budeme testovať (výnimky na FW, VPN, ...)
  - Dátumy a časy testovania
  - KONTAKT pre prípad rachnutia aplikácie
  - **(NE)ručenie za prípadné škody**
  - Zákazník má informovať dodávateľov, správcov webu či iné zainteresované subjekty
  - Spôsob reportovania výsledkov
  - Pri internom teste napr. vylúčené aplikácie, časti siete patriace iným subjektom, ošetrenie potenciálneho prístupu k citlivým informáciám, ...
  - **NDA, NDA, NDA...**

Po teste...

- Upratať po sebe
  - **Vytvorené účty, modifikácie ACL, proxychains, port forwardery, inštalované tooly, ...**
- Vytvoriť report
  - **Nájdené zraniteľnosti, ich závažnosť a odporúčanie, ako ich odstrániť**
- Bezpečne odstrániť dáta, získané počas testovania
  - **Formátovanie diskov, ...**

Pentest NIKDY NEVYKONÁVAŤ len tak!

Dobrý úmysel nie je ospravedlnenie...

- Každá krajina má inú legislatívu: aj obyčajný nmap, ak používame invazívne skripty, môže byť považovaný za ilegálny – nedovolené scanovanie portov...
- Riziká – pád aplikácie, manipulácia dát, získanie citlivých informácií...

Čo používame?

- Komerčné scannery a toolkity
  - Acunetix WVS
  - **Burpsuite Pro**
  - Nessus
  - Nexpose

- Open-source
  - Skipfish
  - cURL
  - Nikto
  - **SQLMap**
  - **Nmap/Zenmap**
  - Doplnky prehliadačov – **TamperData**, WebScarab, ...
  - **KALI distro**
  - a iné...

Burpsuite

- Proxy – zachytávanie prevádzky
- Funkcie:
  - Scanner
  - Spider
  - Intruder
  - Repeater
  - Decoder a mnohé iné

TamperData

- Free doplnok Mozilla FF
- zachytenie a manipulácia requestov

OWASP WebGoat

- Zámerne zraniteľná aplikácia
- Free
- Na vzdelávacie účely – možno si vyskúšať rôzne typy útokov na rôzne zraniteľnosti:
  - Cross-site Scripting (XSS)
  - Access Control
  - Thread Safety
  - Hidden Form Field Manipulation
  - Parameter Manipulation
  - Weak Session Cookies
  - Blind SQL Injection
  - Numeric SQL Injection
  - String SQL Injection
  - Web Services
  - Fail Open Authentication
  - Dangers of HTML Comments

  a mnohé iné...

Kioptrix

- Virtuálny PC s mnohými zraniteľnosťami
- Boot-to-root:
  - Cieľom je ovládnuť stroj s čo najvyššími privilégiami
- Staršie, ale na vyskúšanie veľmi dobré

- http://www.kioptrix.com/blog/
- https://blog.g0tmi1k.com/2012/02/kioptrix-level-4-sql-injection/

S čím sa (ešte stále) stretávame

- Chýbajúce flagy cookies
- Clickjacking
- „Ukecaný“server či aplikácia – determinácia použitých technológií, zverejnenie informácií o serveri či o používateľoch
- Neaktuálne verzie softvéru
- Zle implementované SSL či HTTPS
- **Reflexné (až perzistentné) XSS**
- **SQL injection**
- **Command&remote file injection/inclusion**
- Nedostatky v Session managemente

OWASP Top 10 - 2013

- A1-Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- A2-Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

- A3-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

- A4-Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

- A5-Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

OWASP Top 10 - 2013

- A6-Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

- A7-Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

- A8-Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

- A9-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

- A10-Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Flagy Cookies & HTTP Headers

Cookies = identifikátory spojenia:

- prebiehajúca relácia zodpovedá danému klientovi

- Flag *Secure* – cookie nemožno prenášať mimo HTTPS
- Flag *HttpOnly* – cookie nemôže byť manipulovaná z prehliadača, modifikovať ju môže len vydávajúci server
- Header *X-Frame-Options* – ochrana voči clickjackingu
- Header *X-XSS-Protection*

A iné

Determinácia technológie, získanie info o serveri

- Server v odpovediach prezradí aj to, čo nevie...
- Napr. pri chybových hláseniach, no i pri normálnej odpovedi možno získať rôznorodé informácie:
  - Prezradenie bázovej technológie, konkrétnej verzie SW
  - Prezradenie typu databázy
  - Emailové adresy, iné info o používateľoch
  - Neošetrené výnimky – výpis, kde v adresárovom strome vznikli...
- Rôzna príčina a rôzne zdroje úniku

Neaktuálne verzie SW

- Zastarané verzie nepodporované vendorom - nevydávajú sa bezpečnostné záplaty
- Podporované, no neúplné či vôbec neupdatované verzie – ak aj vendori vydajú záplaty, ale správca ich neinštaluje...

- Prečo to nechceme???
  - Vražedné v kombinácií s možnosťou determinovať prítomnosť starého softvéru: **útočník mieri na konkrétne, známe zraniteľnosti, možno na nete nájde aj presne taký exploit, aký potrebuje...**

SSL a HTTPS

- Staré verzie SSL/TLS
- Slabé šifry a hashovacie funkcie – zlá randomizácia RC4, krátke kľúče, kolízie v MD5,...
  - Online test - ssllabs: https://www.ssllabs.com/ssltest/

- Nevynucované použitie HTTPS
- Problematická kombinácia HTTP a HTTPS častí portálov

Session Management

- Pri stránkach s autentifikáciou
- Dodržanie pravidiel na správu identifikátorov spojení (cookies, session tokens)
- 3 scenáre:
  - Paralelné prihlásenie
  - Znovupoužitie cookie
  - Prenos cookie na stroj s inou verejnou IP

- S prihliadnutím na funkciu stránky

Cross-Site Scripting - XSS

- Aplikácia nedostatočne ošetruje používateľské vstupy či iné dáta z nedôveryhodných zdrojov: chýba validácia(zmysluplnosť hodnôt) či escaping (filtrovanie znakov)
- XSS umožňuje útočníkovi spustiť skript v prehliadači obete - dôsledky:
  - Session hijacking
  - Defacement – falšovanie stránky
  - Redirect – presmerovanie používateľa na škodlivé stránky

SQL Injection (a iné injection flaws)

- SQL, OS či LDAP
- Nedôveryhodné dáta sa bez dostatočného spracovania odosielajú interpreteru ako časť príkazu alebo dopytu.
- Zaslané dáta budú interpretované na vykonanie príkazu či získanie prístupu k dátam bez zodpovedajúcej autorizácie... Vylistujeme si databázu, dumpneme zoznam používateľov, spustíme príkaz...
  - Príklad – Kioptrix: získanie root prístupu cez SQLi

Interné testy

- Množstvo možných prístupov
- Podstatné je získať prvého používateľa
  - Ako? Ťažko! ☺

- Štandardná situácia:
  - Organizácia s Windows doménou, sieťovou infraštruktúrou, viac-menej oddelené segmenty; mailové služby, weby, fileservery, VoIP, monitoring (kamery, klimatizácie, ...), Linux servery, ...
  - Máme sieťovú zásuvku v sieti bežných používateľov

Na čo sa zamerať?

- Architektúra siete:
  - oddelenie segmentov používateľov, serverov, sieťových prvkov, ...
- Infraštruktúra
  - ARP Poisoning? Routovacie protokoly?
- Monitoring a manažment
  - SNMP, Telnet, SSH, HTTP prihlasovanie, RDP, IPMI, ...
- Doména
  - Politika hesiel, CIFS NULL, NTLM autentifikácia, cached logon credentials, ...
- Servery a služby
  - Staré verzie, chýbajúce aktualizácie, patche, ...

Na čo sa zamerať?

- SSL/TLS
  - Verzie, platnosť a dôveryhodnosť certifikátov
- Databázy
  - SQL Injection, default credentials, ...
- Sieťové služby
  - FTP, ...
- Weby
- SMB
- Používatelia
  - Social engineering

Príklad

- Doména
  - Server 2008 R2, PC Windows 7 EE
- Kali a Windows 7
  - útočiace zariadenia v sieti

1. Bruteforce doménových hesiel,
2. Eskalácia privilégií na lokálneho administrátora,
3. Získanie administrátorského hesla,
4. Vytvorenie administrátora,
5. Dump hashov z doménového radiča

Referencie

- http://www.csirt.gov.sk/
- https://www.owasp.org/
- https://www.kali.org/
- https://portswigger.net/burp/
- https://blog.g0tmi1k.com/2012/02/kioptrix-level-4-sql-injection/
- https://github.com/foxglovesec/Potato
- http://blog.gentilkiwi.com/mimikatz
- http://www.ampliasecurity.com/research/windows-credentials-editor/
- https://github.com/CoreSecurity/impacket

Sieťová bezpečnosť

O čom to bude

- Sieť z pohľadu útočníka
  - Kam až a k akým dátam sa viem dostať
- Sieť z pohľadu administrátora
  - Ako obrániť sieť voči útokom
- Prezentácia sa nezaoberá:
  - Sociálnym inžinierstvom
  - DoS a DDoS

#Note: [Ľ-S] == ľahké až stredne náročné; {VĽ, Ľ, S, Ť, VŤ}

Pozadie

- Potenciálna obeť má klasickú sieť ako väčšina spoločností:
  - Switched Ethernet network
  - Switche, FWs, APs, servery (rôzne OS), zverejnené služby (web, DNS, VPN, ...), pracovné stanice, možno aj Windows doména
- Útočník chce:
  - Kompromitovať sieť svojho cieľa
  - Mať pod kontrolou jeho zariadenia
  - Získať zaujímavé dáta

Útok

- Reconnaisance
- Sociálne inžinierstvo
- Exploitácia zraniteľností dostupných služieb (otvorené porty, nebezpečná konfigurácia)
- Sniffovanie komunikácie
- Prístup na správcovské rozhrania

Note: k dispozícii je množstvo toolov zásadne
zjednodušujúcich prácu útočníkovi...

Exploitácia zraniteľností dostupných služieb

- Cieľ: získať prístup do siete, alebo ďalej v sieti, ultimátne chcem prístup k OS s admin právami
- Otvorené porty a bežiace služby
  - (nmap) scan, software and OS version detection [Ľ]
  - Známe zraniteľnosti, exploity (nájdem zverejnený exploit [Ľ-S], alebo si urobím vlastný [S-VŤ])
    - Zraniteľný web – eventuálne sa dostanem k OS
    - Windows Server 2003 v doméne == zlatá baňa
    - Enumerácia používateľov, ...
- Nebezpečná konfigurácia
  - Taktiež známe zraniteľnosti a exploity alebo útoky
  - Directory trversal; username disclosure; ICMP redirects enabled; ...

Sniffovanie komunikácie

- Cieľ: odchytiť zujímavé údaje
  - prihlasovacie údaje: switche a routre/FWs, virtualizácia (napr. VMWare servery), SSH/RDP na servery, databázy, weby, SIP auth, IPMI rozhrania...
  - používané služby: kam pristupujú používatelia (najmä admini)? Chcem ďalšie IP:port kam sa pozriem
  - Session hijacking

Sniffovanie komunikácie – ako?

- ARP spoofing/poisoning [VĽ]
- MAC address spoofing [Ľ-S]
- DHCP spoofing [Ľ]
- WPAD MITM (Web Proxy Autodiscovery Protocol) [Ľ]
- DTP mode dynamic auto (Dynamic Trunking Protocol) [S]
- SPAN port [S]
- ďalšie metódy...

Prístup na správcovské rozhrania

- Cieľ: získať prístup do siete, alebo ďalej v sieti, mapovanie siete
- Ako:
  - Pomocou defaultných prihlasovacích údajov
  - Pomocou odsnifovaných prihlasovacích údajov
  - Alebo môžem skúsiť slovník
  - Nejaký exploit?

Sniffovanie komunikácie – ochrana (1)

- Šifrovanie komunikácie
- # šifrovanie len hesla nie je výhra – môže to byť rozbité
- Nepoužívať plaintext protokoly na manažment alebo prístup k chráneným dátam
- Použitie VLAN (iné VLAN pre správcov, používateľov, dodávateľov, ...)
- Ešte lepšie: implementácia PVLAN
- Ideálne: fyzicky oddeliť správcovskú sieť od dátovej
- Rozumná architekúra siete – aby útočník niečo podstatné dosiahol nemalo by stačiť prekonať/ovládnuť jedno zariadenie

Sniffovanie komunikácie - ochrana (2)

- ARP spoofing/poisoning
  - arp inspection (DAI)
  - VLAN, PVLAN a ACL/FW
  - Použitie (vhodne nastaveného) IDS
- MAC address spoofing
  - port security
- DHCP spoofing
  - DHCP snooping

Sniffovanie komunikácie - ochrana (3)

- WPAD MITM (Web Proxy Autodiscovery Protocol)
  - Vypnúť "Automatickú detekciu nastavení" proxy
- DTP mode dynamic auto (Dynamic Trunking Protocol)
  - switchport trunk allowed vlan 42,666
  - switchport mode {access|trunk}
- SPAN port
  - Podrobné logovanie + monitorovanie logov

Exploitácia zraniteľností dostupných služieb - ochrana

- Vypnutie nepotrebných služieb
- Nastaviť lokálny FW/ACL
- Aplikovanie security patchov (pravidelné a včasné)
- Plánované včasné upgrady (nepoužívať zastaralé nepodporované technológie)
- Vynucovanie šifrovania (DB access, proprietárne protokoly, ...)
- Zmena default prihlasovacích účtov
- Používať komplexné heslá
- Pravidelný scan otvorených portov neuškodí:
  - (nmap) otvorené porty na kritických serveroch a routroch
  - (nmap) čo všetko vidím z Internetu?

Prístup na správcovské rozhrania - ochrana

- ACL/FW pravidlá
- správcovská VLAN
- Nepoužívať nešifrované protokoly - Telnet, HTTP, nevynútené SSL/TLS....
- Autentifikácia: použitie klientských certifikátov, RSA kľúče
- Chrániť zálohovacie servery, aj monitorovacie a syslog servery
- Nerecyklovať heslá, používať komplexné heslá

Zabezpečenie aktívnych prvkov

- ACL
  - prístup na manažment rozhranie len zo špecifikovaných IP adries
  - prístup len cez manažment IP.addr z manažment VLAN (nie cez každú existujúcu IP.addr)
- Vypnutie HTTP a Telnet, prípadne aj HTTPS ak ho nepotrebujeme
- Zvážiť vypnutie CDP
- SNMPv3 (ak je vôbec potrebný)
- V konfigu ukladať šifrované heslá (nie plaintext)
  - Aj zálohy konfigurákov obsahujú mená a heslá...
- Aktualizovať firmvéry
- Vypnúť password recovery so zachovaním pôvodného konfigu
- Fyzická ochrana ;)

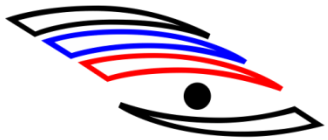
Nastavenie firewallov

- Whitelisting (default DROP + výnimky)
- Vyhnúť sa dieram
  - ~~iptables -s *IP.addr.spravcu* -j ACCEPT~~
- Filtrovanie odchádzajúcej komunikácie
  - Ideálne whitelisting
  - Takmer určite nechceme mať povolené: SMTP všade, DNS všade, SMB von, SYSLOG von, ...
- Zakázať ICMP smerom dovnútra
- Vypnúť posielanie ICMP host unreachable do Internetu
- Centrálny FW nestačí, vždy nasadiť aj lokálny FW
- Nasadenie IPS (Intrusion Prevention System)

Tip: ako je na tom Váš domáci Wifi router?

- Multiple vulnerabilities found in Quanta LTE routers (backdoor, backdoor accounts, RCE, weak WPS ...)
  - https://pierrekim.github.io/blog/2016-04-04-quanta-lte-routers-vulnerabilities.html
- Príklad UPC router (EWW3226)
  - telnet s prihlasovacími údajmi ako na web interface - zmena hesla cez web sa neprejaví na telnet :/
  - UPC WeFree (opt-out?)
  - hm, heslo na telnet admina bolo zmené X týždňov dozadu a zrazu je tam opäť default?
- Je používateľské rozhranie na http://192.168.0.1 ?
  - Prípadne 192.168.1.1 / 172.16.0.1

Otázky



CSIRT.SK
www.csirt.gov.sk

Ďakujeme za pozornosť!

Ing. Zuzana Vargová
zuzana.vargova@csirt.gov.sk

Ing. Valéria Harvanová
valeria.harvanova@csirt.gov.sk

CSIRT.SK
www.csirt.gov.sk