Report

Interní penetrační test infrastruktury společnosti
UKÁZKOVÝ REPORT

Milan Bartoš <milan@appsec.cz>

appsec

Obsah

1 Úvod

1.1 Disclaimer

Penetrační test je obvykle popisován jako přesná a kompletní simulace útoku na danou službu či aplikaci. Ačkoliv penetrační test a reálný útok mají mnoho společného, například znalosti testera a útočníka, používané nástroje a další, tak zde existuje i několik podstatných rozdílů, které je potřeba brát v úvahu. Jedná se především o omezení penetračního testu penězi či časem.
V případě reálného útoku může útočník plánovat útok i několik měsíců předem. Může si tedy dlouhodobě shromažďovat informace potřebné k útoku. V případě penetračního testu si takovýto luxus dovolit nelze, jelikož takový penetrační test by byl finančně neúnosný a zároveň by nepřinesl požadovaný výsledek v rozumném čase pro případná protiopatření.
Z tohoto důvodu je občas potřeba při penetračním testu určitou součinnost od testovaného subjektu, aby v čase vymezeném pro penetrační test bylo možno otestovat systémy co nejvíce.

1.2 Nástroje použité při testování

- Nessus
- Metasploit Framework
- Nmap
- Burp Suite Pro
- Firefox
- Kali Linux
- Nikto
- APPSEC Toolkit

1.3 Postup testování

Testy probíhaly na základě zkušeností a schopností testerů, podílejících se na penetračním testu, v souladu se standardem PTES.

Jednotlivé fáze penetračního testování byly 1. identifikace cíle, 2. identifikace aktivních služeb, 3. identifikace možných zranitelností, 4. ověření nalezených zranitelností. V průběhu testu byly využívány nástroje, schopnosti a informace tak, aby bylo co nejvěrněji dosaženo simulace útoku takovým způsobem jakým by ho prováděl případný skutečný útočník.

2 Manažerské shrnutí

Předmětem testování bylo provedení komplexního penetračního testu interní sítě společnosti ABC. Testování probíhalo v souladu se znalostmi a zkušenostmi penetračních testerů, kteří se na testování podíleli.

2.1 Cíle testu

Cílem tohoto penetračního testu bylo detekovat bezpečnostní nedostatky v interní síti společnosti ABC.

Předmětem testování bylo provedení komplexního penetračního testu interní infrastruktury na zadavatelem dodaných IP adresách. Tyto IP adresy a rozsahy jsou následující:

- 10.0.0.0/24 - rozsah interní sítě
- 10.0.1.0/24 - rozsah interní sítě
- 192.168.1.1 - router vedoucí do sítě Internet
- 192.168.1.23 - interní autentizační server

2.2 Identifikované zranitelnosti

Během penetračního testu bylo odhaleno několik zranitelností, včetně kritických, které mohou vést ke kompromitaci dat či systémů nacházejících se v interní síti společnosti.

Mezi nejzávažnější nalezené zranitelnosti patří používání starých verzí operačního systému Linux, webového serveru a ftp serveru. V případě webového serveru a ftp serveru dokonce existují veřejně dostupné exploity na bezpečnostní nedostatky, které použité verze těchto systémů obsahují.

Dalšími zranitelnostmi, které byly nalezeny a kterým je vhodné věnovat pozornost jsou nález nezabezpečených dat na SMB discích (sdílené disky) přístupných z celé interní sítě, tedy jakýmkoliv lidem, kteří k dané síti mají přístup (zaměstnanci, útočník, který nějakým způsobem již přístup k interní síti získal) a to bez přihlášení. Během penetračního testu bylo dále nalezeno dalších 5 zranitelností, hodnocené závažností střední a nízkou, kterým je vhodné věnovat pozornost po vyřešení nejzávažnějších nedostatků.

2.3 Závěr

Během penetračního testu byly odhaleny zranitelnosti, které mohou být použity k přímé kompromitaci testované sítě a dat. Z tohoto důvodu doporučujeme věnovat zvýšenou pozornost nejen jejich opravě, ale i důkladnému prozkoumání systému pro zjištění, zda Nálezy jsou řazeny sekvenčně podle jejich závažnosti od nejvyšší (kritická) po nejnižší (nízká). Doporučujeme opravit všechny zranitelnosti se závažností kritickou, vysokou a střední. Doporučujeme opravit také nálezy s nízkou závažností, nicméně ty nepředstavují přímou hrozbu pro aplikaci. Po realizaci náprav identifikovaných nedostatků doporučujeme provést retest interní sítě, aby bylo ověřeno, že nálezy byly skutečně opraveny. Doporučujeme provádět testování aplikace minimálně jednou ročně, aby bylo minimalizováno riziko výskytu případných nových zranitelností, které mohly být objeveny nebo zaneseny do sítě od posledního testování.

3 Klasifikace zranitelností

V této kapitole je popsána klasifikace jednotlivých nalezených zranitelností. Každé zranitelnosti je přiřazena míra závažnosti podle dopadů, které by zneužití dané chyby mělo na testovaný systém.

3.1 Podle míry závažnosti

Závažnost jednotlivých nálezů vychází z jejich dopadů na celkové zabezpečení systému. Během hodnocení závažnosti jednotlivých nálezů je zohledněno případné využití společně s ostatními nalezenými zranitelnostmi.

- Kritická ■

  Závažná zranitelnost, která má přímé dopady na celkovou bezpečnost testovaného systému.

- Vysoká ■

  Zranitelnost, která může mít přímé dopady na bezpečnost testovaného systému v případě schopného či motivovaného útočníka.

- Střední ■

  Zranitelnost, která sama o sobě nemá dopad na celkovou bezpečnost testovaného systému, nicméně společně s dalšími zranitelnostmi může představovat určité riziko.

- Nízká ■

  Nález, který má nízký dopad na celkovou bezpečnost testovaného systému, jedná se většinou spíše o best practices.

- Informativní ■

  Nález, který je čistě informativní povahy a nepředstavuje bezpečnostní problém.

4 Výsledky penetračního testu

V této kapitole uvádíme technické informace k provedenému penetračnímu testu.

4.1 Identifikované servery a služby

Během penetračního testu byla identifikována následující zařízení a služby, které na nich běží.

IP adresa zařízení	Detekované služby
10.0.0.1	• 445/tcp - Apache 2.4.12 • 1823/tcp - Nessus 0.99
10.0.0.3	• 80/tcp - Apache 2.4.24
192.168.1.1	• 21/tcp - vsftpd blíže nezjištěné verze • 80/tcp - Nginx 4.3
192.168.1.23	• 21/tcp - vsftp 2.12 • 80/tcp - Apache 2.6.3 • 94/tcp - SSH 4.2

4.2 Identifikované zranitelnosti

V této kapitole jsou uvedeny jednotlivé zranitelnosti a nálezy seřazené podle závažnosti od nejzávažnějších po nejméně závažné. Jedná se o nálezy, které byly identifikovány během penetračního testování. Jsou zde uvedeny společně s případnými dopady a doporučením na eliminaci rizika. Vzhledem k povaze penetračního testu nemusí být jejich seznam kompletní.

4.2.1 Nepodporovaný operační systém

Závažnost:	Ovlivněné systémy:
	• 10.0.0.1

Nález

Během testu bylo zjištěno, že na serveru běží stará, již nepodporovaná verze operačního systému Linux. Jedná se o následující operační systém v dané verzi: - Linux, Ubuntu 13.10 - server 10.0.0.1

Riziko

Z důvodu již nedostupné podpory pro danou verzi operačního systému nejsou nově nalezené bezpečnostní zranitelnosti opravovány. V případě, že je nalezena nějaká závažná bezpečnostní chyba, její oprava nebude systému dostupná běžnými prostředky (aktualizační mechanismus), což povede ke zranitelnosti daného systému a dříve či později k jeho kompromitaci.

Doporučení

Doporučujeme aktualizaci na nejnovější podporovanou verzi operačního systému. Informace o nejnovějších verzích operačního systému Ubuntu Linux můžete najít na webové stránce www.ubuntu.com.

4.2.2 Zranitelná verze Apache serveru

Závažnost:	Ovlivněné systémy:
	• 192.168.1.23 - 80/tcp

Nález

Během penetračního testu bylo zjištěno, že na daných systémech je provozován webový server Apache ve zranitelné verzi 2.4.XX. Na danou zranitelnost existuje veřejně dostupný a jednoduše použitelný RCE (remote code execution) exploit. Dostupný je na adrese www.example.com, kde je ke stažení zdarma.

Riziko

Zneužitím této zranitelnosti může být útočník schopen docílit spuštění libovolného kódu na zranitelném systému pod právy uživatele se kterými webový server běží. Jedná se o velmi závažnou zranitelnost, protože spuštěním kódu na zranitelném systému může útočník efektivně převzít nad daným systémem kontrolu.

Doporučení

Doporučujeme aktualizovat webový server na nejnovější podporovanou verzi. Informace o nejnovější verzi webového serveru Apache je dostupná na adrese https://httpd.apache.org/.

4.2.3 ProFTPD mod_copy zranitelnost

Závažnost:	Ovlivněné systémy:
	• 192.168.1.23 - 22/tcp

Nález

Během testu bylo zjištěno, že daný server je náchylný na známou zranitelnost ProFTPD ftp serveru, která umožňuje neautentizovanému uživateli manipulovat se soubory na serveru.

```
Trying 192.168.1.23...
Connected to 192.168.1.23.
Escape character is '^]'.
220 ProFTPD 1.3.4a Server (tajne!) [192.168.1.23]
site help
214-The following SITE commands are recognized (* =>'s unimplemented)
214-CPFR <sp> pathname
214-CPTO <sp> pathname
214-UTIME <sp> YYYYMMDDhhmm[ss] <sp> path
214-SYMLINK <sp> source <sp> destination
214-RMDIR <sp> path
214-MKDIR <sp> path
214-The following SITE extensions are recognized:
214-RATIO -- show all ratios in effect
214-QUOTA
214-HELP
214-CHGRP
214-CHMOD
214 Direct comments to root@192.168.1.23
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy
250 Copy successful
```

Riziko

Neautentizovaný útočník může být schopen zkopírovat libovolné soubory ze serveru do míst ke kterým má přístup (webový server) a dané soubory stáhnout a číst. Obdobným způsobem může být útočník schopen soubory na serveru přepsat a tím dosáhnout nějaké změny v konfiguraci daných služeb.

Doporučení

Doporučujeme aktualizovat ProFTPD ftp server na verzi 1.3.5a / 1.3.6rc1 či novější. Nebo v ideálním případě ftp server vůbec nepoužívat a nahradit jej bezpečnější alternativou.

4.2.4 SMB sdílené disky přístupné

Závažnost:	Ovlivněné systémy:
	• 10.0.0.11 - 445/tcp • 10.0.0.12 - 445/tcp

Nález

Během penetračního testu bylo zjištěno, že některé exportované SMB sdílené disky jsou připojitelné a čitelné odkudkoliv bez nějaké další autentizace. Konkrétně se jedná o '\\disk1' (10.0.0.11) a '\\disk2' (10.0.0.12). Na daných discích se nachází velice citlivá data finanční povahy a je tedy velice pravděpodobné, že přístup k nim by neměl být povolen pro jakékoliv zařízení, které se k dané síti připojí.

Riziko

Rizikem je možnost úniku potenciálně citlivých dat, které jsou na daných systémech uložené. Dále také možnost, že případný útočník zneužije dostupné diskové kapacity k ukládání obsahu, i nelegálního.

Doporučení

Doporučujeme vypnutí anonymymního/hostovského přístupu k daným systémům a zavedení autentizace a autorizace tak, aby bylo zabráněno potenciálnímu úniku daných citlivých dat.

4.2.5 Podporováno SSL3, možný útok POODLE

Závažnost:	Ovlivněné systémy:
	• 10.0.0.66 - 443/tcp

Nález

V průběhu penetračního testu byla na daném serveru a dané službě zjištěna zranitelnost POODLE (Padding Oracle On Downgraded Legacy Encryption). Jedná se o man-in-the-middle information disclosure útok umoňující útočníkovi dešifrování vybraného bytu ciphertextu.

Riziko

V případě úspěšného útoku POODLE může být útočník schopen dešifrovat šifrovanou komunikaci. Toto může vést k úniku citlivých informací jako například přihlašovací údaje, session cookies či jakékoliv jiné citlivé informace, které se mohou mezi aplikací a uživatelem přenášet.

Doporučení

Jedná se o zranitelnost, která je principielní pro SSLv3, nikoliv pro konkrétní implementaci. Doporučujeme tedy zakázání SSLv3 na úrovni konfigurace daného serveru a používání pouze TLSv1.1 nebo vyšší verze. V serveru nginx toho lze dosáhnout například použitím direktivy ssl_protocols TLSv1.2 TLSv1.1;, která povolí pouze bezpečné TLS verze 1.1 a 1.2.

4.2.6 Chybí HSTS

Závažnost:	Ovlivněné systémy:
	• 192.168.1.23 - 443/tcp • 10.0.0.7 - 443/tcp

Nález

Během testů bylo zjištěno, že webový server nevynucuje HTTP Strict Transport Security (HSTS). Jedná se o mechanismus chránící komunikaci před downgrade útoky a tedy následného potenciálního úniku citlivých informací, kdy by webový prohlížeč komunikoval se serverem se slabým či žádným šifrováním.

Riziko

V případě chybějící HSTS hlavičky může být útočník schopen provést downgrade útoky na šifrované spojení, SSL stripping útok, man in the middle útoky a další.

Doporučení

Doporučujeme nastavení HSTS hlaviček Strict-Transport-Security na webovém serveru. Toho lze dosáhnout přidáním následující direktivy do konfigurace webového serveru Apache:

```
Header set Strict-Transport-Security "max-age=31536000"
```

4.2.7 Použitý telnet

Závažnost:	Ovlivněné systémy:
	• 10.0.0.5 - 23/tcp

Nález

Na serveru běží telnet, který nepoužívá žádnou formu šifrování. Toto není doporučeno, jelikož přenášená data mohou být útočníkem zachycena při přenosu po síti. Telnet je velmi starý protokol, jehož začátky sahají až do roku 1969, tedy do doby, kdy povědomí o Internetové bezpečnosti a pravidlech zabezpečování dat při přenosu bylo velmi malé až žádné.

Riziko

Rizikem použití telnetu je, že útočník, který se rozhodne na síti odposlouchávat síťové pakety, vidí veškeré přihlašovací údaje a veškerá data, která jsou protokolem telnet přenášena. Těchto znalostí poté může útočník zneužít v dalších fázích útoku na jiné systémy.

Doporučení

Místo protokolu telnet doporučujeme pro veškerou vzdálenou administraci zařízení používat protokol SSH-2, který díky použití kryptografie poskytuje dostatečnou ochranu přenášených dat. Nejvhodnější implementací protokolu SSH-2, kterou doporučujeme, je OpenSSH dostupné na adrese https://www.openssh.com/. Podporuje všechny používané platformy a jeho nasazení je otázkou několika minut.

4.2.8 Podporovány RC4 šifry

Závažnost:	Ovlivněné systémy:
	• 192.168.1.23 - 443/tcp

Nález

Během penetračního testu bylo zjištěno, že webový server na kterém běží testovaná aplikace podporuje cipher suites, které používají RC4 šifry. Jedná se o následující cipher suites:

```
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_SHA
```

Riziko

Algoritmus RC4 nekorektně pracuje se stavovými daty a klíčem během inicializační fáze. Toto může umožnit útočníkovi provést útok, s jehož pomocí se útočníkovi může podařit dešifrovat některá přenášená data a tím pádem k nim získat přístup. Jedná-li se o nějaká citlivá data, dojde k jejich získání útočníkem a může dojít k jejich zneužití.

Doporučení

Doporučujeme v konfiguraci webového serveru vypnout podporu pro dané cipher suites. Toho lze dosáhnout ve webovém serveru Apache pomocí následujícího nastavení, konkrétní relevantní částí nastavení je přidání položky "!RC4" do konfigurace SSLCipherSuite:

```
SSLCipherSuite HIGH:!RC4
```

4.2.9 Únik informací z hlaviček webového serveru

Závažnost:	Ovlivněné systémy:
	• 192.168.1.23 - 80/tcp

Nález

Během penetračního testu bylo zjištěno, že webový server odesílá ve svých hlavičkách informace o použité verzi jazyka PHP.

```
GET / HTTP/1.1
Host: example.com

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 23 Oct 2011 19:19:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2911
Connection: close
X-Powered-By: PHP/5.4.42
Set-Cookie: PHPSESSID=8SF7FGKS87D6FKJDS0S; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
```

Riziko

Rizikem takovéhoto počínání je, že případný útočník má k dispozici informaci o verzi použitého software, který je na serveru nasazen. Tato informace mu může posloužit například ke zjednodušení hledání zranitelností a zpřesnění dalších útoků.

Doporučení

Doporučujeme ve webovém serveru zakázat odesílání těchto potenciálně citlivých informací. Lze toho dosáhnout například přidáním následujících řádků do konfiguračního souboru.

Pro server Apache je to následující nastavení:

```
ServerTokens ProductOnly
ServerSignature Off
```

5 Přílohy

5.1 Citlivá data nalezená na systémech disk1 a disk2

vypis_z_uctu_2_2017.xls
vypis_z_uctu_3_2017.xls
vypis_z_uctu_4_2017.xls
vypis_z_uctu_5_2017.xls
vypis_z_uctu_6_2017.xls
vypis_z_uctu_7_2017.xls
mzdy_zamestnancu_2017.xls
mzdy_zamestnancu_2018.xls