Provedení penetračních testů pen-cypherfix2016

Případová studie FLAB

Popis situace

Vedení organizace Cypherfix, a. s. chápe důležitost své IT infrastruktury pro zajištění chodu svých služeb a v rámci preventivních úkonů by chtělo realizovat penetrační testy, aby byl zjištěn aktuální stav bezpečnosti klíčových systémů a následně mohla být případně provedena náprava detekovaných bezpečnostních problémů.

Pověření pracovníci IT oddělení při hledání vhodného dodavatele zjišťují, že službu penetračního testování nabízí také Forenzní laboratoř CESNET, s jejímiž pracovníky má organizace Cypherfix, a. s. dobré zkušenosti už z předchozí spolupráce při analýze bezpečnostních incidentů. Forenzní laboratoř je tedy kontaktována s žádostí o provedení penetračních testů.

Forenzní laboratoř FLAB

Při prvním konzultačním telefonátu je zákazníkovi popsán standardního postup při realizaci penetračních testů, tj. jakými kroky bude potřeba postupně projít. V rámci telefonátu jsou rovnou zahájeny některé z těchto kroků.

Nejprve jsou zjištěny informace o infrastruktuře zákazníka a identifikována cílová oblast pro testování. Výsledkem je seznam rozsahů nebo jednotlivých IP adres, doménových jmen nebo služeb, které mají být testovány. Všechny zjištěné informace jsou sepsány do technického zadání (viz příloha A), ze kterého pak také vychází časová náročnost penetračních testů. Tvorba technického zadání je iterativní záležitost a řada informací je několikrát upřesňována a měněna. Pracovníci Forenzní laboratoře CESNET zde vystupují v roli konzultanta, který pomáhá zákazníkovi zadání vytvořit.

Následuje nacenění prací ze strany sdružení CESNET a zaslání cenové nabídky, návrhu smlouvy a termínu realizace zákazníkovi. Po schválení právníky a vedením organizace Cypherfix, a. s. je smlouva podepsána a je možné přejít k předmětu plnění, tj. zahájení penetračních testů.

Rozbor cílů

Během komunikace mezi IT pracovníky organizace Cypherfix, a. s. bylo vypracováno technické zadání penetračních testů (viz Příloha A), které popisuje jaké systémy, kdy a jakým způsobem budou testovány. Konkrétně se jedná o tři klíčové servery – webový server, aplikační server a AAA server. Testování bude probíhat jak z vnější sítě (Internetu), tak i ze sítě zákazníka, do které bude dočasně připojen server Forenzní laboratoře CESNET. Při testech webového portálu bude také využita testovací identita s právy běžného

zaměstnance organizace Cypherfix, a. s., aby mohly být vyhledány zranitelnosti zneužitelné pouze autentizovanými uživateli. Formální aspekty zakázky jsou pokryty smlouvou, jejíž součástí je také dohoda o mlčenlivosti (NDA – non-disclosure agreement).

Cílem penetračních testů je:

- **Zjistit aktuální stav bezpečnosti** – u specifikovaných systémů a služeb jsou prováděny testy za účelem zjištění existujících zranitelností návrhu systému, jejich implementace a používání.
- **Vyhodnotit nalezené zranitelnosti** – ohodnotit závažnost jednotlivých zranitelností a možné dopady jejich zneužití na organizaci zákazníka.
- **Navrhnout nápravná opatření** – pro jednotlivé nalezené zranitelnosti jsou navrženy postupy a opatření, která povedou k odstranění zranitelností, minimalizaci jejich výskytu nebo alespoň minimalizaci dopadů zneužití.
- **Předat zjištěné skutečnosti** – vhodným a srozumitelným způsobem, aby mohla být realizována náprava nalezených zranitelnosti pracovníky zákazníka.

Penetrační testy také musí probíhat nedestruktivní formou, tj. běžný chod ogranizace Cypherfix, a. s. nebude nijak ohrožen.

Řešení

Vlastní technické realizaci penetračních testů ještě předchází výměna kontaktních údajů a šifrovacích klíčů mezi pracovníky Forenzní laboratoře CESNET a pracovníky organizace Cypherfix, a. s. V případě výskytu nečekaných problémů je pak možné snadno kontaktovat druhou stranu a ověřit si, zda jde o následek testování a pokud ano, přerušit danou činnost. Zároveň lze zajistit bezpečnou výměnu informací, například předání přihlašovacích údajů testovacích identit nebo nahlášení velmi závažných zranitelností, které je potřeba odstranit ihned a nečekat až na závěrečnou zprávu.

Zjišťování přítomných zranitelností je prováděno nejprve automatickými nástroji (scannery) a na základě vyhodnocení jejich výsledků jsou pak vybrané nálezy prověřeny a dále testovány s osobním přístupem. V souladu se zadáním je AAA server testován pouze v pracovní době zaměstnanců organizace Cypherfix, a. s., zatímco zbylé dva servery mohou být testovány kdykoliv během dohodnuté doby.

Výsledky všech testů jsou následně vyhodnoceny a shrnuty v závěrečné zprávě (viz Příloha B). Nalezené zranitelnosti jsou popsány, a to včetně klasifikace závažnosti a návrhu příslušných nápravných opatření. K závěrečné zprávě zákazník obdrží ještě samostatný soubor, který obsahuje další podrobnější informace o nalezených zranitelnostech, zejména způsob jak konkrétně byly nalezeny. Administrátor dané služby nebo zařízení si tak může sám snadno ověřit, zda nápravné opatření realizoval správně nebo je zranitelnost stále přítomna.

Kromě závěrečné zprávy jsou výsledky předávány také formou workshopu v sídle organizace Cypherfix, a. s. Pracovníci Forenzní laboratoře CESNET zde lehce stravitelnou formou prezentují výsledky obsažené

v závěrečné zprávě, postup, kterým dané zranitelnosti našli, a jakým způsobem pronikli do testovaných systémů. Administrátoři i další zaměstnanci zákazníka mají možnost dané nálezy prodiskutovat, nechat si vysvětlit podrobnosti a také konzultovat vlastní navržená opatření.

Výsledky

Pro organizaci Cypherfix, a. s. je IT infrastruktura důležitá a v rámci prevence potřebovala prověřit aktuální stav zabezpečení vybrané části své infrastruktury, aby mohly být případné nalezené bezpečnostní problémy opraveny. Na základě předchozích pozitivních zkušeností se spoluprací byla tímto úkolem pověřena Forenzní laboratoř CESNET, která je schopna požadované cíle splnit v rámci služby „Penetrační a zátěžové testy“.

Na základě konzultace s pracovníky sdružení CESNET bylo vypracováno technické zadání (viz příloha A), podle kterého byly penetrační testy následně realizovány. Všechny nalezené zranitelnosti byly vyhodnoceny z hlediska jejich závažnosti a pro každou byly navrženy příslušná nápravná opatření. Veškeré informace byly shrnuty v závěrečné zprávě, která byla předána pracovníkům organizace Cypherfix, a. s. V rámci předávání výsledků penetračních testů v sídle zákazníka proběhl také workshop, kde pracovníci Forenzní laboratoře CESNET prezentovali obsah závěrečné zprávy doplněný o popis průniku do testovaných systémů a o možnost prodiskutovat předložené nálezy a konzultovat vlastní návrhy nápravných opatření.

Výsledkem proběhlých penetračních testů je splnění požadavku organizace Cypherfix, a. s. na prověření aktuálního stavu zabezpečení specifikované části infrastruktury. Aplikací doporučených nápravných opatření byly eliminovány nalezené zranitelnosti dříve než mohly být zneužity reálným útočníkem.

Příloha A: Zadání penetračních testů

Zadání penetračních testů – pen-cypherfix2016

1. Specifikace zadání

Na základě objednávky provedou pracovníci forenzní laboratoře (FLAB) sdružení CESNET, z.s.p.o. penetrační testy níže specifikovaného rozsahu. Výstupem penetračních testů bude závěrečná zpráva obsahující seznam nalezených bezpečnostních zranitelností a doporučení k jejich odstranění.

1.1.Cíle

Cílem penetračních testů je ověřit, zda

- lze získat neoprávněný přístup k službám/datům/systémům,
- lze neoprávněně modifikovat/zničit data,
- lze narušit dostupnost služeb/systémů,
- lze získat autentizační údaje,
- lze zneužít infrastrukturu k útokům na sítě a služby třetích stran a
- existují zranitelnosti, které mohou vést k předchozím bodům.

1.2. Realizace

Testy budou prováděny nedestruktivní formou a budou zaměřeny na zranitelnosti programového vybavení a OS, ponechání výchozích hesel, provozování nadbytečných služeb, a také na detekci zařízení a služeb, které je možné zneužít pro odrážení záplavových útoků na síťové vrstvě.

1.3. Výstupy

Výstupem penetračních testů bude závěrečná zpráva obsahující kompletní seznam nálezů, tj. nalezených bezpečnostních zranitelností, jejich klasifikace dle závažnosti a doporučení k jejich odstranění.

1.4. Personální zajištění

Sdružení CESNET, z. s. p. o. a/nebo zúčastnění pracovníci sdružení budou vázáni Smlouvou o mlčenlivosti a ochraně důvěrných informací (NDA), která bude uzavřena mezi sdružením CESNET a zákazníkem před zahájením penetračních testů. Po zahájení realizace mohou být informace týkající se penetračních testů poskytovány pouze níže uvedeným pracovníkům.

Kontaktní osoby na straně CESNET, z. s. p. o.

Pracovník	Kontaktní e-mail	Kontaktní telefon

Ing. Aleš Padrta, Ph.D.	flab@cesnet.cz	+420 234 680 280

Řešitelský tým na straně CESNET, z. s. p. o.

Pracovníci		
Ing. Radoslav Bodó	Ing. Michal Kostěnec	Ing. Radomír Orkáč

Kontaktní osoby na straně zákazníka

Pracovník	**Kontaktní e-mail**	**Kontaktní telefon**
Ing. Jan Bezpečný, Cypherfix, a. s.	jan.bezpecny@cypherfix.cz	---

Poskytování informací o průběhu penetračních testů dalším osobám ze strany sdružení CESNET je možné pouze na základě jejich uvedení ve Smlouvě o mlčenlivosti a ochraně důvěrných informací a Smlouvě o dílo.

2. Technické specifikace

Penetračnímu testování budou podrobena zařízení specifikovaná v sekci 2.3, přičemž mohou být testována pouze z IP adres uvedených v sekci 2.1. Pro testování z lokální sítě bude provedeno prostřednictvím VPN zřízené objednatelem, nebo testovacím serverem dodavatele včetně vzdáleného KVM, kterým objednatel přidělí potřebný počet IP adres.

2.1. Zdroje testování

Všechny testy budou prováděny výhradně z následujícího výčtu IP adres.

Externí zdroje testování (mimo síť zákazníka)

- 195.113.144.0/24
- 2001:718:1:1f::/64

Interní zdroje pro testování (v síti zákazníka)

- 192.168.33.32/29 (testovací server umístěný v síti zákazníka)
- 192.168.33.31 (VPN)

2.2. Kategorie zařízení

Na přání zákazníka lze během penetračních testů k testovaným zařízením přistupovat různě, zejména pokud je u některých systémů vyžadována garantovaná dostupnost. Každé zařízení může být zařazeno do jedné z kategorií dle následující tabulky.

Kategorie	Způsob testování zařízení
I.	Může být testováno kdykoliv
II.	Může být testováno pouze v pracovní době (7:00 – 17:00)
III.	Může být testováno pouze ve specifikovaném čase
IV.	Nesmí být testováno

Implicitně je předpokládáno zařazení všech zařízení do kategorie I. Množství vyžadovaných omezení, zejména kategorie III., ovlivní dobu a tedy i cenu testování.

2.3. Seznam testovaných sítí a zařízení

V rámci penetračních testů budou prověřeny následující služby sítě a zařízení:

IP adresa / rozsah	Popis	Kategorie	Poznámka
203.0.113.10 portal.cypherfix.cz	WWW server	I.	---
203.0.113.11	APP server	I.	---
203.0.113.22	AAA server	II.	---

2.4. Seznam poskytnutých identit

V rámci penetračních testů vybraných zařízení a služeb mohou být používány následující identity:

Systém	Služba	Identita	Poznámka
portal.cypherfix.cz	Webová aplikace	pen-testuser1	Práva běžného zaměstnance

Hesla, certifikáty apod. budou předány bezpečným způsobem před zahájením penetračních testů.

3. Časový harmonogram

Plánovaný postup prací:

Popis úkonu	Zahájení	Dokončení
Realizace testů v síti zákazníka	12.12.2016	16.12.2016

Sepsání závěrečné zprávy	19.12.2016	20.12.2016
Validace závěrečné zprávy	21.12.2016	
Prezentace výsledků	22.12.2016	

Plánovaná přerušení prací: ---

Příloha B: Závěrečná zpráva

Pen-cypherfix 2016

Klasifikace dokumentu: Veřejný

Závěrečná zpráva – Penetrační testy *pen-ukazka2016*

1. Obsah

2. Zadání

Na základě Smlouvy o zajištění penetračních testů provedou pracovníci forenzní laboratoře (FLAB) sdružení CESNET, z. s. p. o. penetrační testy níže specifikovaného rozsahu. Výstupem penetračních testů bude závěrečná zpráva obsahující seznam nalezených bezpečnostních zranitelností a doporučení k jejich odstranění.

2.1 Cíle

Cílem testů jsou následující zjištění:

- Lze získat neoprávněný přístup k službám/datům/systémům?
- Lze neoprávněně modifikovat/zničit data?
- Lze narušit dostupnost služeb/systémů?
- Lze získat autentizační údaje?
- Lze zneužít infrastrukturu k útokům na sítě a služby třetích stran?
- Potenciální zranitelnosti, které mohou vést k předchozím bodům.

2.2 Realizace

Testy budou prováděny nedestruktivní formou a budou zaměřeny na zranitelnosti programového vybavení a OS, ponechání výchozích hesel, provozování nadbytečných služeb, a také na detekci zařízení a služeb, které je možné zneužít pro odrážení záplavových útoků na síťové vrstvě.

2.3 Výstupy

Výstupem penetračních testů bude závěrečná zpráva obsahující kompletní seznam nálezů, tj. nalezených bezpečnostních zranitelností, jejich klasifikace dle závažnosti a doporučení k jejich odstranění.

2.4 Technické specifikace

Penetračnímu testování budou podrobeny zařízení specifikované v sekci 2.4.2, přičemž mohou být testovány pouze z IP adres uvedených v sekci 2.4.1. Pro testování z lokální sítě bude provedeno prostřednictvím VPN zřízené objednatelem, nebo testovacím serverem dodavatele včetně vzdáleného KVM, kterým objednatel přidělí potřebný počet IP adres.

2.4.1 Zdroje testování

Všechny testy budou prováděny výhradně z následujícího výčtu IP adres.

Externí zdroje testování (mimo síť zákazníka)

- 195.113.144.0/24
- 2001:718:1:1f::/64

Interní zdroje pro testování (v síti zákazníka)

- 192.168.33.32/29 (testovací server umístěný v síti zákazníka)
- 192.168.33.31 (VPN)

2.4.2 Seznam testovaných sítí a zařízení

IP adresa / rozsah	Popis	Kategorie	Poznámka
203.0.113.10 portal.cypherfix.cz	WWW server	I.	---
203.0.113.11	APP server	I.	---
203.0.113.22	AAA server	II.	---

3 Manažerské shrnutí

Provedené penetrační testy odhalily 7 zranitelností v různých kategoriích závažnosti. Mezi nejzávažnější nalezené nedostatky patří: nevhodné zacházení s údaji kritickými pro provoz infrastruktury a zpracování webových aplikací. V přiděleném čase byly provedeny všechny plánované testy.

Penetrační testy by měly být opakovány v horizontu 24 měsíců a bylo by vhodné jejich záběr rozšířit i na širší infrastrukturu spojenou s testovaným prostředím (např. pracovní stanice administrátorů).

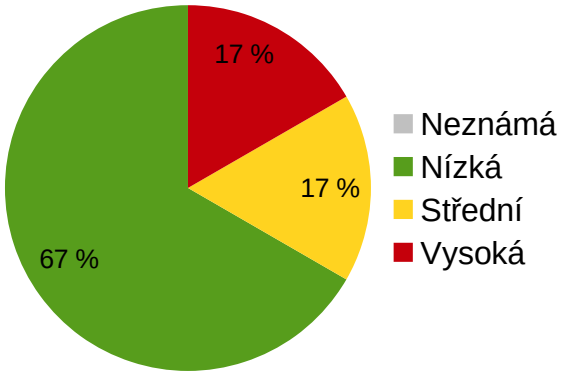
4 Metody sběru dat, provedené testy

Ke sběru dat byl použit distribuovaný skener SNER, nástroj Nessus provozovaný CESNET-CERTS, OSS Nikto a Metasploit. Vybrané zranitelnosti a služby byly testovány ručně, případně specializovanými nástroji. Vybrané služby byly podrobeny záplavovým testům a v součinnosti s pracovníky zadavatele byl vyhodnocen dopad výpadků citlivých služeb na zbytek výpočetního prostředí.

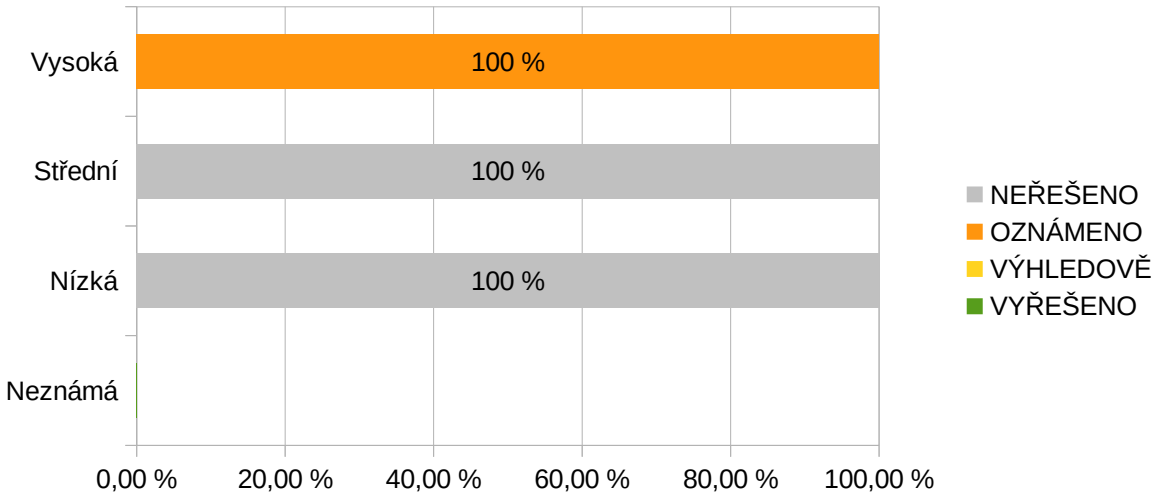
5 Vyhodnocení

V cílové IP síti byla sběrem dat nalezena celkem tři zařízení, zjištěno cca 12 TCP/UDP portů (služeb) a vytipováno cca 16 zranitelností, které byly dále podrobněji testovány. Nedostatky byly zpracovány do formy jednotlivých nálezů, byla zhodnocena jejich individuální závažnost v kontextu testovaného prostředí a navrženo odpovídající doporučení k odstranění zranitelnosti. Technické detaily jsou uvedeny v příloze A1.

Rozložení nalezených zranitelností do kategorií dle závažnosti:



Stav řešení nálezů vzhledem k jejich závažnosti (ke dni 16.12.2016):



5.1 Nevhodné zacházení s údaji kritickými pro provoz infrastruktury

V průběhu testování byla nalezena důležitá data (centrální repozitář konfiguračního managementu puppet) uložená v nešifrované podobě na serveru *owncloud.cypherfix.cz*. V repozitáři konfiguračního managementu je možné dále nalézt různé přístupové údaje (klíče, hesla, keytaby) do různých částí infrastruktury. V některých případech byly nalezeny přístupové údaje ke spravovanému prostředí zapsaná v textových souborech. Zjištěné skutečnosti svědčí o nevhodném zacházení s přístupovými údaji, tyto praktiky mohou poskytnout případným útočníkům informace potřebné k hlubšímu průniku do napadené infrastruktury.

Doporučení

Centrální repozitář konfiguračního managementu by měl podléhat vyššímu zabezpečení: nikdy by neměl v nešifrované podobě opustit příslušný služební server, v jeho obsahu by se ideálně neměly nacházet přístupové údaje ke spravovaným systémům ani šifrovací klíče, které používají jednotlivé služby.

5.2 Zpracování webových aplikací

Zpracování interních provozovaných aplikací není na vhodné úrovni odpovídající současným standardům. Aplikace provozované v ASP.NET obsahují ve velkém množství vstupních parametrů od uživatele zranitelnost typu SQL Injection (*portal.cypherfix.cz*).

Doporučení

Přepsat aplikace pomocí moderních metod pro programování webových aplikací za použití některého z frameworků eliminující běžně zneužívané zranitelnosti webových aplikací.

6 Výstupy z testování

Výstupem z provedených testů je:

- závěrečná zpráva (tento dokument),
- seznam jednotlivých nálezů a doporučení (příloha A1),
- pracovní sešit obsahující podrobné informace k nálezům (příloha B1 – samostatný soubor).

7 Závěr

Testované výpočetní prostředí je segmentováno na lokální síť a DMZ s ohledem na provozované agendy. Provoz z veřejného Internetu prochází centrálním firewallem, přístup na aplikační úrovni k vybraným agendám je řízen aplikačním firewallem.

Provedené penetrační testy odhalily zranitelnosti v různých kategoriích, v některých případech také odhalily nevhodné postupy pro nasazování a provoz informačních systémů. Mezi nejzávažnější nalezené nedostatky patří:

- Nevhodné zacházení s údaji kritickými pro provoz infrastruktury,
- Zpracování webových aplikací.

Za přidělenou dobu byly zhodnoceny všechny zranitelnosti nalezené sběrem dat. Ke všem nalezeným nedostatkům bylo vydáno doporučení k jejich odstranění. Penetrační testy by měly být opakovány v horizontu 24 měsíců a bylo by vhodné jejich záběr rozšířit i na širší infrastrukturu spojenou s testovaným prostředím (např. Windows AD nebo pracovní stanice administrátorů).

8 Příloha A1

ID	IP/Hostname	Zranitelnost	Závažnost	Doporučení
	RŮZNÉ A NEZAŘAZENÉ			
1	owncloud.cihperfix.cz	Aplikace ownCloud, která obsahuje detailní informace o interní infrastruktuře realmu CYPHERFIX.CZ (typy serveru, konfigurace, logy) je dostupná bez autentizace a z veřejného internetu.	STŘEDNÍ	Omezit přístup k monitorovacímu systému (ip, autentizace).
	MS WINDOWS			
2	různé	Doménové kontrolery umožňují enumeraci uživatelů přes SMB.	NÍZKÁ	Omezit možnosti neautentizovaných uživatelů při interakci s doménovými stroji (DCE RCP/SMB).
	NETWORKING			
3	různé	SNMP Agent Default Community Name (public)	STŘEDNÍ	Zvážit použití přístupového hesla k SNMP agentům a zavedení řízení přístupu podle IP.
	WEBOVÉ ZRANITELNOSTI			
4	download.cypherfix.cz	Potvrzení licenčního ujednání (EULA) lze obejít manipulací cookies ze strany uživatele.	NÍZKÁ	Opravit aplikaci.
5	portal.cypherfix.cz	SQL Injection via stacked query in http://portal.cypherfix.cz/search	VYSOKÁ	Opravit zranitelnost SQLi, používat escapování parametrů při vstupu dat do SQL dotazu, používat prepared statements.
	WEBSERVERY			
6	portal.cypherfix.cz	PHP < 5.3.11 Multiple Vulnerabilities	NÍZKÁ	Upgradovat SW.

	SSLHELL			
7	portal.cypherfix.cz	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	NÍZKÁ	Omezit používání SSLv2 a SSLv3.