Služby Forenzní laboratoře

Aleš Padrta

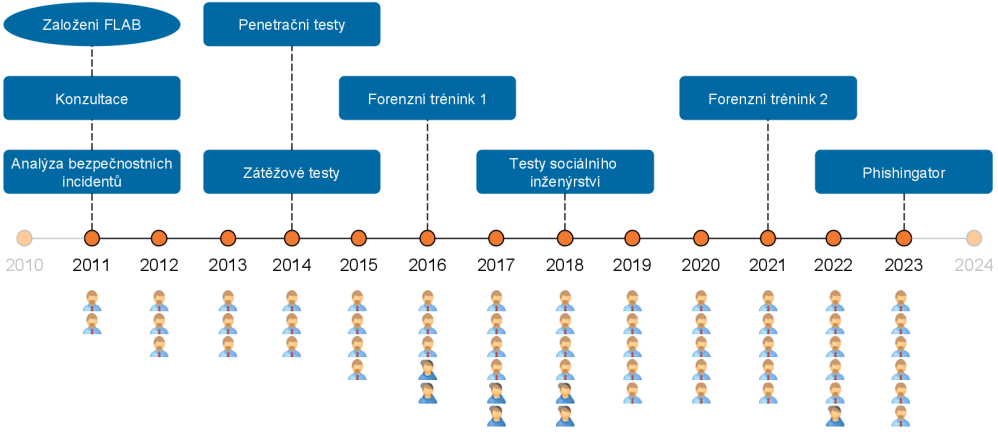
apadrta@cesnet.cz

Forenzní laboratoř CESNET

cesnet

- Forenzní LABoratoř = FLAB
  - Pracovní skupina, vznik 2011
  - Primárně – analýza bezpečnostních incidentů
    - ⇒ Průkazné doložení závěrů
    - ⇒ Název pracovní skupiny
- Postupné rozšiřování služeb
  - „Customer driven“ (podle poptávky)
  - Konzultace
  - Penetrační a zátěžové testy
  - Testy sociálního inženýrství
  - Školení
  - Doplňkové služby (drobné služby a požadavky)

Vývoj v čase


Založení FLAB
Penetrační testy
Konzultace
Forenzní trénink 1
Forenzní trénink 2
Analýza bezpečnostních incidentů
Zátěžové testy
Testy sociálního inženýrství
Phishingator
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

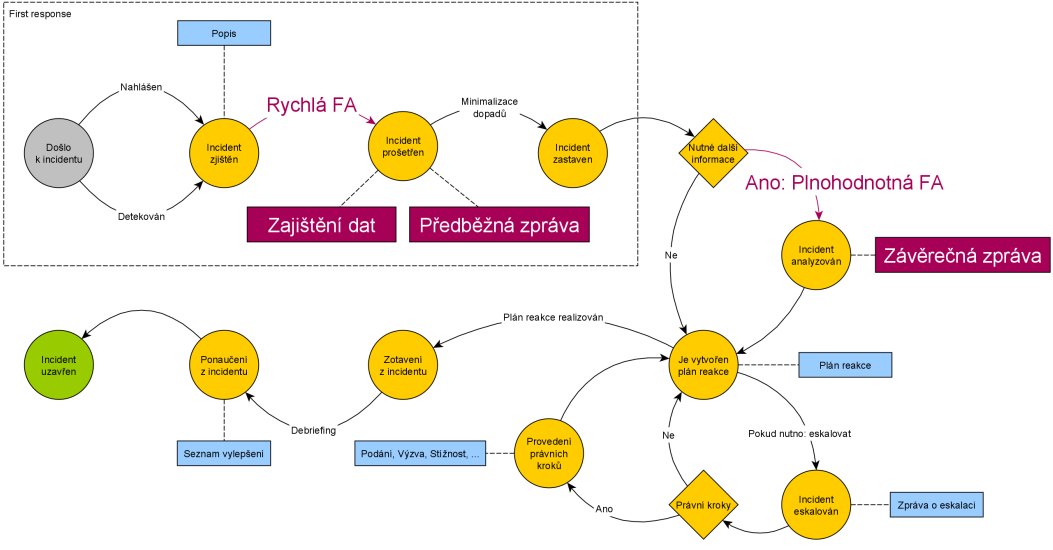
Analýza bezpečnostních incidentů

Analýza bezpečnostních incidentů

cesnet

- Reakce na bezpečnostní incident
  - Závažná rozhodnutí $\Rightarrow$ potřeba důvěryhodných informací
  - Dopad na jednotlivce
  - Dopad na organizace
- Forenzní analýza
  - Důvěryhodnost podkladů pro analýzu
  - Důvěryhodnost průběhu analýzy
  - Závěry $\Rightarrow$ kvalitní informace pro rozhodování
- Využití služby
  - Incident bude třeba eskalovat / závažná rozhodnutí
  - Během incidentu / po incidentu

Analýza vs. incident handling/response



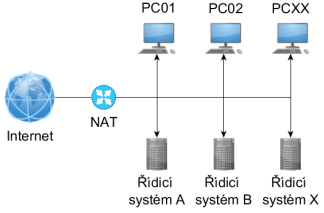
Průběh zakázky

cesnet

1. **Úvodní konzultace**
   - Typ incidentu/analýzy
   - Časový rozsah
   - Posouzení možností
2. **Definice zadání**
   - Pomoc s formulací otázek
   - Specifikace vstupních dat (podpora při zajišťování dat)
   - Kontakty, . . .
3. **Administrativa**
   - NDA, smlouva
4. **Vlastní analýza**
   - Analýza průběhu incidentu
   - Nalezení odpovědí na otázky
   - Dokumentace postupu
   - Doložení závěrů
5. **Předání výsledků**
   - Závěrečná zpráva
   - Prezentace výsledků (VC/osobně)
   - Závažná zjištění – průběžně

Příklad

- Problém v továrně
  - Kompromitované zařízení
  - Šíření malware
  - Narušování výroby
- Cíl
  - Zjistit příčinu
  - Podpora pro eskalaci
- Analýza
  - Systematický postup
  - Časová osa
  - Malware `Trickbot`
  - Šíření = nevhodná architektura sítě



- Výsledek
  - ⇒ Obnovení výroby
  - ⇒ Úprava sítě
  - ⇒ Vzdělávání uživatelů

Jak o službu požádat?

- Domluva na úvodní konzultaci
  - flab@cesnet.cz
- Více informací
  - https://flab.cesnet.cz/cs/sluzby/analyza

Školení – Forenzní tréninky

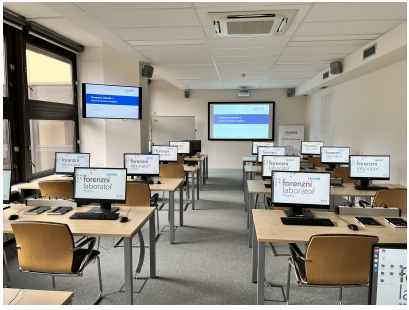
Školení – Forenzní tréninky

cesnet

- Důvod vzniku
  - Komplikace při součinnosti + zbytečná prodlení
- Přínosy školení
  - Seznámení s činností analytika
    - $\Rightarrow$ Opuštění romantických představ
    - $\Rightarrow$ Samostatné zajištění dat
    - $\Rightarrow$ Provádění „rychlé“ analýzy
    - $\Rightarrow$ Efektivnější komunikace s (externími) analytiky
  - Neuzavření cesty k důvěryhodným závěrům
  - Externí analytik (např. FLAB) – jen „plnohodnotná“ analýza

Školení – Forenzní tréninky

- Cílová skupina
  - Pracovníci bezpečnostních týmů
  - IT pracovníci
  - „Skladníci ve šroubárně“
- Způsob školení
  - Malá skupina
  - Postupné představení témat
  - Teoretický úvod
  - Praktické cvičení (možná pomoc lektorů)
  - Předpokládané řešení



Forenzní trénink 1: Úvod do for. analýzy

cesnet

- Dvoudenní školení
  - Základní principy
  - Analýza paměťových médií
- Výukové bloky
  - Úvod do forenzní analýzy
  - Zajištění podkladů
  - Časová osa souborového systému
  - Časová osa událostí
  - Případ s MS Windows
  - Prezentace výsledků

Forenzní trénink 2: Síť

- Dvoudenní školení
  - Volné pokračování
  - Analýza síťového provozu
- Výukové bloky
  - Úvod do síťové forenzní analýzy
  - Síťové toky a Netflow
  - Zajištění podkladů
  - DNS – Domain Name System
  - Protokoly
  - Závěrečný případ

Jak se přihlásit?

- Pořádání kurzů 1–2× ročně
- Obvykle v jednom týdnu
  - Úterý + středa – Forenzní trénink 1
  - Čtvrtek + pátek – Forenzní trénink 2
- Přihlášení
  - Budoucí kurzy – sluzby@cesnet.cz
  - Již naplánované – registrace na webu www.cesnet.cz
- Více informací
  - https://flab.cesnet.cz/cs/sluzby/skoleni

cesnet

Penetrační testy

Penetrační testy

cesnet

- Simulace činnosti útočníka = hledání zranitelností
  - Chyby v návrhu
  - Chyby v implementaci
  - Nevhodné používání

- Přínos
  - Identifikace problémů k nápravě
  - Oprava ještě před zneužitím

- Využití služby
  - Preventivní opatření
  - Plánovaný test sítí, služeb, systémů

Průběh zakázky

cesnet

1. Úvodní konzultace

- Zjištění potřeb
- Specifikace cílů / oblasti
- Prioritizace cílů
- Odhad časové náročnosti

2. Administrativa

- Definice zadání
- Cenová nabídka
- Termín realizace
- NDA, smlouva

3. Vlastní testování

- Sběr informací
- Automatizované skeny
- Manuální testování
- Nedestruktivní forma

4. Vyhodnocení

- Závěrečná zpráva
- Seznam nálezů
- Doporučení k nápravě
- Prezentace výsledků

Příklad

cesnet

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

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.

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.ez	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.ez	PHP < 5.3.11 Multiple Vulnerabilities	NÍZKÁ	Upgradovat SW.
	SSLHELL			
7	portal.cypherfix.ez	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	NÍZKÁ	Omezit používání SSLv2 a SSLv3.

Jak o službu požádat?

- Domluva na úvodní konzultaci
  - flab@cesnet.cz
- Více informací
  - https://flab.cesnet.cz/cs/sluzby/pentesty

Zátěžové testy

Zátěžové testy

cesnet

- Ohrožení dostupnosti systémů
  - Útoky DoS (Denial of Service), DDoS (Distributed DoS)
  - „Útoky“ legitimním zájmem
- Možnosti zahlcení
  - Přenosová kapacita (uplink, vnitřní trasy)
  - Síťové prvky (směrovače, firewally apod.)
  - Koncové systémy (databáze, weby apod.)
- **Odolnost systému = jak velkou zátěž ustojí?**
- Využití služby
  - Preventivní opatření
  - Detekce úzkých hrdel + jejich optimalizace

Průběh zakázky

cesnet

1. **Úvodní konzultace**
   - Zjištění potřeb
   - Popis cílové infrastruktury
   - Probrání postupu
   - Odhad časové náročnosti
2. **Administrativa**
   - Definice zadání
   - Cenová nabídka
   - Termín realizace
   - NDA, smlouva
3. **Zátěžové testování**
   - **Spolupráce se zákazníkem**
   - Spuštění sady testů
   - Změna konfigurace systémů
   - Opakování

     $\Rightarrow$ naladění systémů
4. **Vyhodnocení**
   - Závěrečná zpráva
   - Zhodnocení testů
   - Doporučení vhodných úprav

Příklad

cesnet

- Informace od zákazníka
  - Reklamní akce – samostatný webový portál
  - Očekává 6 000 současných přístupů
  - Ustojí stávající infrastruktura zájem?
- Zátěžový test
  - Simulace zájmu – postupné zvyšování počtu
  - Do 1600 bez problému
  - Postupné zpomalování $\Rightarrow$ kolem 1800 nepoužitelné
  - Zákazník – sledování systémů
- Konzultace $\Rightarrow$ úpravy infrastruktury
  - 9000 bez problému, kolem 9500 nepoužitelné
  - Další zvýšení = posílení HW

Jak o službu požádat?

- Domluva na úvodní konzultaci
  - flab@cesnet.cz
- Více informací
  - https://flab.cesnet.cz/cs/sluzby/zatezovetesty
- **Dočasně nedostupná**
  - Prohíhá přesun testovací infrastruktury

Testy sociálního inženýrství

Testy sociálního inženýrství

cesnet

- Zajištění IT bezpečnosti
  - Technická opatření
  - Bezpečné chování $\Rightarrow$ lidé jsou důležití
- Cíl útočníka – uživatelé / administrátoři
  - Sociální inženýrství (sběr dat, vykonávání činností)
  - Sběr přihlašovacích údajů = stačí „jednorázová“ manipulace
  - Komunikace – nezbytná pro pracovní povinnosti
- Efektivita útoku
  - Automatické rozesílání
  - Nejčastěji $\Rightarrow$ elektronická pošta
- Sběr přihlašovacích údajů + elektronická pošta $\Rightarrow$ phishing

Testy sociálního inženýrství

cesnet

- Ochrana uživatele
  - Antispamová kontrola – nemůže být 100%
  - Lokální antivirová kontrola – nemůže být 100%
  - Vlastní úsudek – nic lepšího není

- Cvičné phishingové zprávy
  - Neškodná simulace reálných zpráv
  - Zjištění míry odolnosti uživatelů

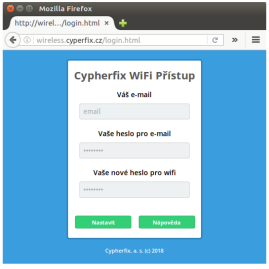
- Rozšíření – primární cíl = školení
  - Úvodní přednáška (teorie)
  - Praktický test (cvičná phishingová zpráva)
  - Komentář k praktickému testu

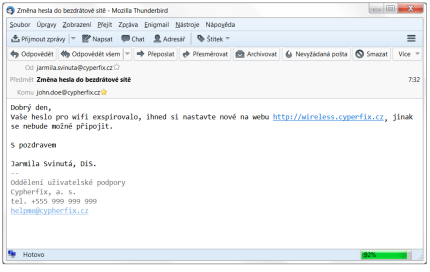
Průběh zakázky

cesnet

1. **Úvodní konzultace**
   - Zjištění požadavků
   - Probrání postupu
   - Odhad časové náročnosti
2. **Administrativa**
   - Definice zadání
   - Cenová nabídka
   - Termín realizace
   - NDA, smlouva
3. **Realizace**
   - Školení uživatelů
   - Rozeslání cvičných zpráv
   - Analýza reakcí uživatelů
   - Doškolení uživatelů
4. **Vyhodnocení**
   - Závěrečná zpráva
   - Prezentace výsledků

Příklad





Název oddělení	Počet uživatelů	Návštěva stránky	Úspěšné přihlášení
Ředitelství	42	20 (47,6 %)	7 (16,7 %)
ICT	41	30 (73,2 %)	4 (9,8 %)
Finanční oddělení	38	12 (31,6 %)	8 (21,1 %)
Správa účelových zařízení	101	45 (44,6 %)	38 (37,6 %)
Oddělení vývoje kryptoměn	137	54 (39,4 %)	11 (8,0 %)
Oddělení šifrovacích algoritmů	123	37 (22,6 %)	9 (7,3 %)
Celkem	**482**	**198 (41,1 %)**	**77 (16,0 %)**

Jak o službu požádat?

- Domluva na úvodní konzultaci
  - flab@cesnet.cz
- Více informací
  - https://flab.cesnet.cz/cs/sluzby/testy-socialniho-inzenyrstvi

Doplňkové služby

Doplňkové služby

cesnet

- Základní služby
  - Vyžadují znalosti
  - Vyžadují vybavení
- Doplňkové služby
  - $\Rightarrow$ Využití znalostí a vybavení pro další účely
  - Konzultace
  - Školení a semináře
  - Obnova dat
  - ...
- Domluva na realizaci doplňkové služby
  - flab@cesnet.cz

cesnet

Dotazy