Finále II. ročníku Středoškolské soutěže ČR v kybernetické bezpečnosti (2017/2018)

Vítejte na soutěžním portálu finále Středoškolské soutěže ČR v kybernetické bezpečnosti.

Pod vysvětlivkami a pravidly najdete seznam úkolů. V přiděleném časovém limitu není možné všechny úkoly vyřešit. V klidu a pečlivě si vyberte, které úkoly budete řešit. Některé úkoly může řešit současně jen omezený počet soutěžících, popř. body za vyřešení může získat jen omezený počet řešitelů. Vysvětlivky, které upřesňují omezení (časové, složitost, hodnocení apod.) najdete v následující tabulce. Doufáme, že vám pomohou v optimalizaci vašeho výběru:

Vysvětlivky značek a doplňujících informací

Typ značky / text	Vysvětlující text
bez omezení	Omezující podmínky řešení úkolu- úkol nemá žádná specifická omezení.
Čas: 50 min.	Omezující podmínky řešení úkolu- úkol má časové omezení (uvedená hodnota), které se počítá od doby zahájení řešení úkolu. Čas se nikdy nepřerušuje. Finalista může řešení úkolu ukončit předčasně.
max. 10 osob	Omezující podmínky řešení úkolu- počet řešitelů (uvedené číslo), kteří mohou úkol vyřešit. Rychlejší vítězí- získá body (případně více bodů). Na centrální tabuli hodnocení bude zveřejňována hodnota kolik osob již úlohu vyřešilo.
5 os./50 min.	Omezující podmínky řešení úkolu- počet řešitelů v jednom čase a časové omezení. Úkol může v jednom čase řešit jen uvedený počet řešitelů. Úkol má časové omezení (uvedená hodnota).
Lehký	Složitost úkolu- jedná se o lehký úkol, ke kterému jsou nutné základní znalosti.
Střední	Složitost úkolu- jedná se o středně těžký úkol, ke kterému jsou nutné rozšířené znalosti.
Těžký	Složitost úkolu- jedná se o těžký úkol, ke kterému jsou nutné velmi dobré znalosti dané problematiky.
Velmi těžký	Složitost úkolu- jedná se o velmi těžký úkol, ke kterému jsou nutné velmi dobré znalosti dané problematiky, zkušenosti s řešením takového úkolu. Úkol vyžaduje hodně času na řešení.
15 minut	Hodnota, která indikuje předpokládaný čas, za který je úloha reálně řešitelná. Specialisté na daný úkol mohou být schopni úkol vyřešit za třetinový (1/3) čas.
30 bodů max. 20 bodů	Bodové hodnocení úkolu. Vyjadřuje kolik bodů řešitel získá za správné řešení úlohy. V případě, že je uvedena hodnota "max. 20 bodů", znamená to, že řešitel může získat 0 až 20 bodů v závislosti na rychlosti řešení úlohy, vyřešení všech jeho dílčích částí apod.
K úkolu Stáhni Výbor	Způsob zahájení řešení úkolu. V případě "K úkolu"- klikněte na tlačítko a přejděte na stránku k řešení úkolu, kde najdete další instrukce. V případě "Stáhni"- klikněte na tlačítko a stáhněte si soubor potřebný k řešení úkolu. V případě "Výbor"- kontaktujte člena Soutěžního výboru, aby Vám úkol předal/zpřístupnil. V tomto případě se zpravidla jedná o úkoly, které mají nějaké omezení, například časové, nebo kolik osob jej může řešit najednou apod. Žluté pole bez textu vyjadřuje, že máte zadání a veškeré potřebné pomůcky a soubory k dispozici.

Soutěžní pravidla

Při soutěži je ZAKÁZÁNO:

1. opisovat, komunikovat s jinými soutěžícími;
2. sdílet odkaz na tuto internetovou stránku a všech stránky, na které se odkazuje s jinými osobami;
3. v soutěžní místnosti používat mobilní telefon a jiné komunikační prostředky (vč. vlastního notebooku/PC) k telefonování, chatování a emailování. Využití emailu je

povoleno pouze v případě, že to vyžaduje plnění úkolu;

4. vynášet ze soutěžní místnosti přidělené technické zařízení, nebo vlastní zařízení, se kterými soutěžící plní soutěžní úkoly.

Při soutěži je POVOLENO:

1. opustit soutěžní místnost;
2. konzultovat způsob řešení úkolů osobně nebo telefonicky mimo soutěžní místnost (při platnosti ZÁKAZU č.2);
3. položit Soutěžnímu výboru dotaz. Soutěžní výbor odpoví neprodleně. Soutěžní výbor se zdrží odpovědi, pokud by odpověď byla nápovědou nebo by odpovědí soutěžící mohl získat konkurenční výhodu.

Ostatní pravidla pro finále soutěže jsou k dispozici zde.

Základní pravidla soutěže jsou k dispozici zde.

Seznam úkolů

Veškeré potřebné informace pro řešení jednotlivých úkolů jsou uvedeny, případně budou předány soutěžícímu v době kdy o úkol požádá.

Úkol č. 1 - Bezdrátová síť iQRF

Úkol řešte pomocí nástrojů, které poskytuje technologie IQRF. Přípustné je využití internetových zdrojů, mimo elektronickou komunikaci. Dílčí příklady řešte postupně, navazují na sebe.

Příklad 1

Vytvořte síť IQRF obsahující 1 koordinátor a 1 nod. U vytvořené sítě se hodnotí míra zabezpečení a optimální nastavení pro přenášení dat.

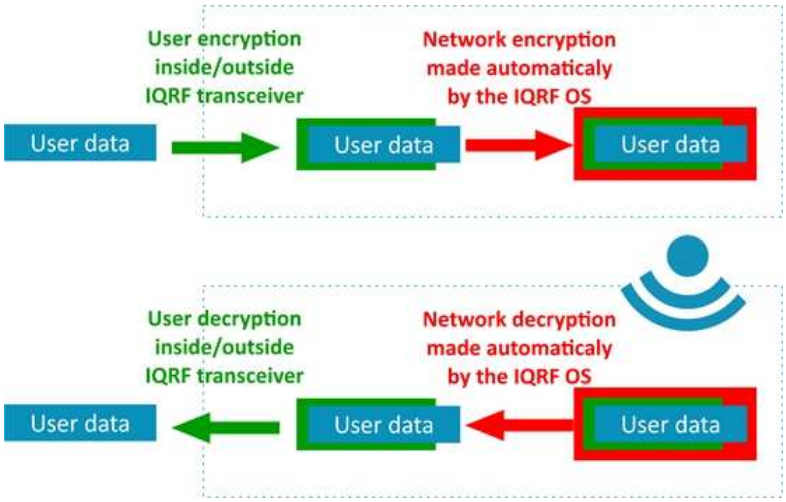
Příklad 2

Zašifrujte s využitím internetových nástrojů pomocí svého User key text „ahoj" a zapište ho s pomocí Custom DPA Handleru CustomDpaHandler-UserEncryption.c do paměti RAM svého nodu. Následně přečtěte zapsaný obsah z periferie RAM svého nodu a ověřte, že je zde zapsán nešifrovaně text „ahoj".

Tipy

Vytvoření sítě: využijte návody dostupné na www.iqrf.org/ds-iot.

Čtení z periferie RAM: První byte PDATA je adresa, druhý byte PDATA je počet bytů. Více na: www.iqrf.org/DpaTechGuide/#3.7%20RAM.



Informace o bezpečnosti IQRF OS 4.02: IQRF OS User Guide (www.iqrf.org-> Support-> Download).

Poznámka:

1. Úkol je dostupný u soutěžního výboru;
2. Úkol může v jednom čase řešit jen limitovaný počet osob.

5 os./40 min. | Těžký | 30 minut | max. 45 bodů | Výbor

Úkol č. 2 - USB flash drive information leakage

A company Clever houses a.s. asked you to help with an investigation of the information leakage. The company specializes in research and development in the

smart buildings field. Not long ago it launched a new product that was in a short time followed by similar products of rival companies.

The management of the company believes this was possible by industrial espionage which resulted in leakage of information about their product. One of the employees of the company was accused and his computer and a flash drive with unknown content were confiscated. Your task is to analyze this flash drive and find out the extent of leaked information.

Notes:

1. Download and decompress the image of the flash drive disk (file "flashdrive.img.gz");
2. Examine the content of the disk. Note that even innocent-looking images can contain data;
3. The answer is a SHA1 checksum of what you find (use the survey form).

bez omezení | Těžký | 60 minut | 50 bodů | Stáhni

Úkol č. 3 - Získejte přístup do Tomcat Manageru

CVE-2007-1860

Poznámka:

1. Odpověď zapište do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Velmi těžký | 60 minut | 50 bodů | K úkolu

Úkol č. 4 - SQL Injection

Zadání text.

Poznámka:

1. Odpověď zapište do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Velmi těžký | 35 minut | 40 bodů | K úkolu

Úkol č. 5 - Útok na zranitelný počítač & Sociální inženýrství

Dnes se budete pohybovat v zapovězené zóně. Do FC Prachovečky se dostala informace o externím asistentovi pro akvizice hráčů v konkurenčním klubu FC Semice jménem Ronald Hanzl. Vyšší management tato informace z prostředí jejich věčného konkurenta opravdu zajímala, a proto se obrátil na místního poskytovatele kybernetických služeb CyberHack Prachovečky, s.r.o. se žádostí o drobnou výpomoc, která je ovšem za hranou zákona.

Z dostupných informací vědí, že Ronald jako externista pracuje ze svého soukromého PC a proto je pravděpodobné, že jeho počítač nebude tak zabezpečený, než běžné firemní PC.

Management Prachoveček by zajímaly zejména informace o hráčích, které aktuálně plánují FC Semice koupit, a sumách, které za ně chtějí nabídnout.

Společnost CyberHack Prachovečky, s.r.o. ví, že z celého oddělení se vyznáte v průnicích do cizích PC a v nejrůznějších formách sociálního engineeringu nejlépe. Požádala vás proto, o zajištěníl průniku do Ronaldova PC, např. prostřednictvím doručení škodlivého kódu e-mailem, a získání cenných souborů s plánovanými akvizicemi.

Jeho e-mail je hanzlronald@protonmail.com, ale pozor, Ronald sice není žádný PC odborník, běžný spam však neotevírá.

Jestli se to podaří, Vánoční odměny v CyberHack Prachovečky, s.r.o a pletky se zákonem určitě proběhnou :-)

Poznámka:

1. Odpověď odešlete emailem na adresu karel@kybersoutez.cz. V předmětu emailu uveďte vaše přijmení a číslo úkolu.

bez omezení | Velmi těžký | 30 minut | 100 bodů |

Úkol č. 6 - Faktorizace špatně vygenerovaného RSA klíče

Bob se rozhodl si sám vygenerovat RSA klíč. Využil k tomu následující kód:

```
# my_math from https://codegolf.stackexchange.com/questions/10701/fastest-code-to-find-thenext- prime

from my_math import *

i = ***redacted***

p = next_prime(i)

q = next_prime(p + 5**35)

print "Dělitel 1:" + str(p)

print "Dělitel 2:" + str(q)

n = p*q

print "n = " + str(n)
```

Následně zveřejnil n a e. Dokážete prolomit jeho parametry? Řešením této úlohy je netriviální dělitel čísla n.

```
n = 323170060713110073007148766886699519604441026697154840321303454275246551388678908931972014115229134636887179609218980194941195591504909210950881523864482831206308773673009960917501977503896521067960576383840675698127319108945905649342670494117001327744669050631918014234702686998450479134370422638200059009829613719552961442034686761104035479336068989847330026647794304679922785384442662607022015087193364918124362340153670754946875510342050837968568149005195864582729382343186909741709977213043996090170470863927803196517625451425910896131873753929477996735742476189164250472704977110443444052258740827655171704084 13

e = 65537
```

Poznámka:

1. Odpověď odešlete emailem na adresu karel@kybersoutez.cz. V předmětu emailu uveďte vaše přijmení a číslo úkolu.

bez omezení | Velmi těžký | 90 minut | 100 bodů |

Úkol č. 7 - Zranitelná webová aplikace - Capture the Flag

Najděte vlaječku ve tvaru SSKB{...}

Poznámka:

1. Odpověď zapište do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Střední | 40 minut | 40 bodů | K úkolu

Úkol č. 8 - Capture the Flag II.

Vývojáři vyvinuli aplikaci, která ukáže vlaječku jen po zadání správného hesla. Nicméně při vývoji udělali chybu a my nyní nemůžeme hodnotu zjistit. Získáte vlaječku ve tvaru SSKB{...}?

Poznámky:

1. K řešení je potřeba si stáhnout pracovní soubor do PC.
2. Odpověď zapiště do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Střední | 30 minut | 25 bodů | Stáhni

Úkol č. 9 - Base64

Podobně jako v druhém kole jste získali část kódu nekvalitního ransomwaru a text tímto kódem zašifrovaný. Tentokrát je však luštění o něco těžší neboť cryptool si s takto šifrovaným textem většinou neporadí. Víte, že otevřený text je běžný textový soubor v ascii kódování bez nestandardních znaků.

Cílem je text dešifrovat a získat z něj váš unikátní kód.

Poznámky:

1. Šifrovaný text získáte v odkazu.
2. Odpověď zapiště do přiloženého dotazníku a odevzdejte jej výboru.

max. 20 osob | Těžký | 45 minut | 60 bodů | K úkolu

Úkol č. 10 - Trezor ve sklepě

Ve sklepních prostorách velmi dobře chráněného objektu se nachází pancéřový trezor, který obsahuje klíčové dokumenty pro splnění mise. Bohužel se jedná o starou, poctivou a mechanicky pevnou konstrukci, kterou není možné otevřít násilím. Prostory, ve kterých je trezor umístěn, jsou bez oken či kamer a tak není možné číselný kód otevírající trezor opticky pozorovat.

Členové vašeho týmu identifikovali nadějný způsob, jak číselnou kombinaci zjistit. Zjistili, že v místnosti s trezorem je zvukové čidlo alarmu, které je aktivní i v okamžiku zadávání kódu. Zároveň zjistili závislost mezi počtem „cvaknutí“, při otáčení kombinačního zámku a číslem, které bylo kombinačním zámkem navoleno.

Dle přiloženého schématu sestavte zapojení, které umožní získat signály ze zvukového čidla v místnosti, a získejte číselnou kombinaci, která otevírá trezor.

Platí přitom tato pravidla:

1. Jedno cvaknutí kombinačního zámku znamená inkrementaci čísla o jedno výše;
2. Kombinační zámek obsahuje 10 číslic. Číslice jsou seřazené za sebou 1,2,3..9,0 (posledním- nejvyšším číslem- je nula);
3. Nastavování každého čísla v kombinaci zámku začíná vždy z výchozí pozice (1. cvaknutí = 1), mezi zadáním dalšího čísla existuje časová prodleva, nutná k dosažení výchozí pozice;
4. Pro otevření trezoru je třeba nastavit správnou kombinaci 6 číslic;
5. Organizace, které trezor patří, změní kombinaci kódového zámku vždy, pokud se použije 3x stejná, po sobě jdoucí, kombinace čísel pro otevření trezoru;
6. V časovém okně, které máte k dispozici, máte možnost zaznamenat celkem 3 úspěšné pokusy o otevření trezoru.

Poznámka:

1. Odpověď zapiště do přiloženého dotazníku a odevzdejte jej výboru.
2. Postupujte dle pokynů člena výboru.

5 os./60 min. | Velmi těžký | 45 minut | max. 100 bodů | Výbor

Úkol č. 11 - Ransomware

Vaším úkolem je provést analýzu škodlivého PDF souboru obsaženého v přiloženém archivu- heslo k němu je "infected". Při analýze buďte velmi opatrní- doporučujeme pro ni použít od sítě oddělený virtuální stroj- soubor obsahuje malware užitý při reálném kybernetickém útoku, který by mohl potenciálně způsobit velmi nežádoucí chování systému v případě nákazy.

Otázky k řešení (pro odpovědi použijte dotazník):

1. Jak se jmenuje soubor přiložený v PDF (tedy ne samotný PDF soubor) a o jaký typ souboru se jedná?
2. Jak se jmenuje JavaScriptová funkce, která by se měla spustit po otevření PDF?
3. Co uvedená funkce provede?
4. Jak se jmenuje funkce, která se spustí po otevření vloženého souboru a s jakým se zavolá parametrem?
5. Na základě analýzy tohoto (vloženého) souboru lze odhadnout, jaké jazykové nastavení užívala jeho šablona, resp. jeho autor (v souboru existují určité indikátory ukazující na specifické jazykové nastavení, které neodpovídá EN). O jaký jazyk zřejmě jde a proč?
6. Větší počet globálních proměnných ve skriptu v tomto (vloženém) souboru začíná stejnou předponou- která to je?
7. Ve funkci Assimptota6 ve skriptu ve vloženém souboru je v předposledním řádku (začíná znakem "C", končí znakem "2") obfuskované jméno metody. Jaká metoda to je? Zapište deobfuskované jméno.

Přístupové údaje na odkazovaný portál:

1. Username: jmt1hw
2. Password: 0q78dI

Poznámka:

1. Odpovědi zapište do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Střední | 25 minut | max. 12 bodů | K úkolu

Úkol č. 12 - Transformace URL adresy

Pozorně si přečtěte následující text, který Vám pomůže vytvořit URL, které Vás dovede na webovou stránku, na které najdete řetězec znaků. Tento řetězec znaků zapište jako odpověď na tuto otázku.

URL vytvoříte tak, že řetězec "http://aaa.adresa.doména/01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A/slovox/password.html" upravíte postupně podle následujících pravidel:

1. Řetězec „01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A“ dešifrujete pomocí hashovací funkce SHA1;
2. Řetězec „adresa“ nahradíte anglickým výrazem pro kybernetickou bezpečnost (bez mezer a jiných než abecedních znaků);
3. URL adresa se nachází v CZ doméně;
4. Řetězec „slovo“ nahradíte křestním jménem úřadujícího prezidenta České pobočky AFCEA. Jméno uvedete bez diakritiky;
5. Každé písmeno „a“ nahradíte písmenem „w“.

Poznámky:

1. Body získá jen prvních deset řešitelů. První 10 bodů, druhý 9 bodů, ..., desátý 1 bod.
2. Odpověď zapište do přiloženého dotazníku a odevzdejte jej výboru.

max. 10 osob | Lehký | 10 minut | max. 10 bodů |

Úkol č. 13 - Test z terminologie z oblasti kybernetické a informační bezpečnosti

Test je složen z 12 otázek v angličtině.

Poznámka:

1. Vyplnění testu je limitováno časem. Čas se počítá od momentu převzetí testu. Pokud není test odevzdám v časovém limitu, počet obdržených bodů bude krácen o 50%.
2. Odpovědi zapište do přiloženého dotazníku a odevzdejte jej výboru.

Čas: 10 min. | Lehký | 10 minut | max. 20 bodů | Výbor

Úkol č. 14 - GDPR (DPO)

Jste nový DPO (pověřenec pro ochranou osobních údajů- dle nového nařízení Evropské unie GDPR) na městském úřadě v Ústí nad Labem. Máte ověřit, zda se na webu úřadu nevyskytují osobní údaje, konkrétně kombinace: rodné číslo + jméno osoby.

Obsah webu je stažen ve složce Data na USB.

Aby bylo možné provést analýzu nástrojem Tovek Tools, nainstalujte si tento program a použijte template pro analýzu GDPR.

Ve kterých složkách se vyskytují alespoň 3 dokumenty, které obsahují takovéto údaje? (bez započtení dokumentů v případných podsložkách).

Poznámka:

1. USB vám předá soutěžní výbor.
2. Odpověď odešlete emailem na adresu karel@kybersoutez.cz. V předmětu emailu uveďte vaše přijmení a číslo úkolu.

bez omezení | Střední | 45 minut | 30 bodů | Výbor

Úkol č. 15 - Kryptoanalýza

Bigramovou kryptoanalýzou vyřešte šifru. Výsledek zašlete v těle emailu na adresu karel@kybersoutez.cz. V předmětu emailu uveďte vaše přijmení.

Šifra:

kszcm eaelj eorxx yojap slsni acaxx

buetp intem nncxx etpko oiyza aeexx

reoef ncpav rpxxx

Poznámka:

1. Odpověď odešlete emailem na adresu karel@kybersoutez.cz. V předmětu emailu uveďte vaše přijmení a číslo úkolu.

bez omezení | Těžký | 30 minut | 30 bodů |

Úkol č. 16 - ADR a Minitraps

Organizace zavádí nový systém pro zvýšení bezpečnosti ICT prostředí. Implementátor provádí iniciální nastavení systému.

Odpovězte na následující otázky na základě snímků obrazovek, které jsou ke stažení v odkazu.

1. O jaký typ bezpečnostního řešení se jedná?
2. Zhodnoťte na základě snímku obrazovky na obr. 1, zda je systém naimplementovaný správně. Zdůvodněte rozhodnutí jednou větou.
3. Jaký je účel Minitraps (někdy také nazývané Breadcrumbs) v řešení?
4. Na snímku obrazovky na obr. 2 si lze všimnout symbolu červeného brouka u stanice 192.168.200.94. Na snímku na obr. 4 je pak obrazovka po kliknutí na ikonku pro zobrazení detailu. O čem tyto obrazovky vypovídají?

Poznámka:

1. Odpovědi zapište do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Střední | 10 minut | max. 15 bodů | Stáhni

Úkol č. 17 - Capture the Flag III

Jedna služba na serveru, který se spustí po naimportování a spuštění boot2flag.ova do virtualboxu je náchylná na častý typ zranitelnosti. Najděte a využijte tuto zranitelnost k získání vlajky.

K dispozici máte dvě nápovědy:

1. Web server;
2. Injections.

Poznámka:

1. Soubor boot2flag.ova najdete na USB, které vám předá soutěžní výbor.
2. Odpověď zapiště do přiloženého dotazníku a odevzdejte jej výboru.

bez omezení | Těžký | 45 minut | 50 bodů | Výbor

Úkol č. 18 - Frekvenční analýza & Fake email

Dešifrujte tento text pomocí frekvenční analýzy znaků. Výsledek zašlete v těle emailu na adresu karel@kybersoutez.cz, přičemž váš email se musí tvářit jako by byl odeslán z adresy soutez@kybercentrum.cz. V předmětu emailu uveďte vaše přijmení.

Šifrovaný text:

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL. QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: "DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?"

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Poznámky:

1. Šifrovaný text je v angličtině.
2. Základní informace o frekvenční analýze jsou zde.
3. Odpovězte emailem dle pokynů uvedených výše.

bez omezení | Těžký | 30 minut | 40 bodů |

Úkol č. 19 - Webový server

Zjistěte následující údaje o doméně www.kybersoutez.cz a odpovězte na níže uvedené dotazy:

1. Na jakém operačním systému běží server, na němž je provozována doména www.kybersoutez.cz?
2. Jaká je fyzická IP adresa domény www.kybersoutez.cz?
3. Jaký redakční systém používá doména www.kybersoutez.cz?
4. Používá doména www.kybersoutez.cz SSL certifikát. Pokud ano, jaký?

Poznámky:

1. Odpovědi zapište do přiloženého dotazníku a odevzdejte jej výboru.
2. Body budou přiděleny jen v případě, že odpovíte správně na všechny otázky.
3. Body získá jen prvních patnáct řešitelů.

max. 15 os. | Lehký | 5 minut | 10 bodů |

Úkol č. 20 - Rozdíl mezi kybernetickou bezpečností a kybernetickou obranou

Vytvořte prezentaci (min. 1 slide nebo 1 strana A4) pomocí níž vysvětlíte rozdíl mezi kybernetickou bezpečností a kybernetickou obranu. Prezentaci odešlete na adresu karel@kybersoutez.cz, přičemž do předmětu zprávy napište vaše přijmení a číslo úkolu.

Poznámky:

1. Prezentace může obsahovat text a obrázky;
2. Prezentace nesmí obsahovat mluvené slovo nebo video ani odkaz na ně;
3. Prezentace musí být samovysvětlující, tj. bez toho, aby jste vy nebo někdo jiný museli vysvětlit co není z prezentace na první pohled zřejmé.
4. Body získá jen prvních dvacet řešitelů.
5. Odpovězte emailem dle pokynů uvedených výše.

max. 20 os. | Střední | 25 minut | max. 25 bodů |

Změna údajů vyhrazena. Aktualizováno dne: 18.4.2018

Kontakt

E-mail: soutez@kybersoutez.cz

Hashtagy

#kybersoutez

#budkyber

Copyright CyberSecurity.cz (c) 2018

Design PJG