Středoškolská soutěž ČR v kybernetické bezpečnosti
1. ročník – 2016/2017
Otázky pro 2. kolo soutěže

Otázka č. 1

PODKLADY K ÚLOZE JIŽ NEJSOU DOSTUPNÉ!

Získejte heslo ukryté v tomto archivu: odkaz již není dostupný.

Otázka č. 2

Odešlete e-mail z e-mailové adresy info@hacking.cz na adresu heslo@kybersoutez.cz. Do těla zprávy uveďte e-mail, který používáte v soutěži. Úkol bude zcela splněn pokud Váš email dorazí do schránky podle zadání a nebude označen příchozím serverem jako SPAM. Pokud bude označen jako SPAM, úkol bude splněn pouze částečně. Pokud se domníváte, že jste úkol splnil(a), zapište do odpovědi v soutěžním portálu slovo "SPLNIL".

Otázka č. 3

PODKLADY K ÚLOZE JIŽ NEJSOU DOSTUPNÉ!

Heslo se na této stránce zobrazí pouze ve chvíli, kdy ji zobrazíte na vrcholku Eiffelovy věže. Ve svém prohlížeči musíte prozradit svoji polohu.

Otázka č. 4

Please read the following text carefully. This will help you to create a URL and lead you on to a web page. You will find there a string of symbols. Write this string down as the answer to this question.

The URL is created by starting with the string „http://aaa.adresa.domena/01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A/slovox/password.html“

and transforming it using these rules:

1) Decipher the string „01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A“ by means of the hash function SHA1;
2) Replace the string „adresa“ by the English expression for „kybernetická bezpečnost“;
3) URL address is located in the CZ domain;
4) Replace the string „slovo“ by the first name of the President of AFCEA Czech Chapter“. Put in the name without diacritical marks;
5) Replace each letter „a“ by the letter „w“.

7E0 CZ 2016
CYBER SECURITY COMPETITION

Otázka č. 5

PODKLADY K ÚLOZE JIŽ NEJSOU DOSTUPNÉ!

Bylo zjištěno, že z interního serveru průmyslové firmy, zabývající se 3D tiskem byla odcizena výrobní dokumentace klíčové součástky. Při vyšetřování incidentu byl zajištěn záznam provozu na síti, který obsahuje komunikaci hackera se serverem. Napadený server má v interní síti firmy adresu 192.168.195.203. Předpokládá se, že útočník využil kompromitovaný systém s adresou 192.168.195.138.

Záznam provozu je umístěn v souboru, který najdete zde: odkaz již není dostupný.

Hlavní úkol:

- Ze záznamu komunikace zrekonstruujte soubor obsahující výrobní data a z něj zjistěte výrobní kód produktu (ve tvaru xx-xx-xxxx)

Vedlejší úkoly:

- Zjistěte jaké uživatelské jméno a heslo bylo použito při útoku
- Zjistěte, na kterém kontinentu byl umístěn server, na který byla odcizená data přenesena

Doporučení:

- Pro analýzu zachycených dat je vhodné použít nástroj Wireshark (www.wireshark.org).
- Pro zjištění obsahu komunikace v rámci jednoho TCP spojení nabízí wireshark funkci „follow TCP stream“
- Pokud chceme data TCP streamu dále zpracovat, je vhodné je uložit jako raw data.

Otázka č. 6

PODKLADY K ÚLOZE JIŽ NEJSOU DOSTUPNÉ!

Přihlaste se na portál odkaz již není dostupný s uživatelským jménem "EarqZr" a heslem "k6UAJ8" a stáhněte si soubor "code.infected". Soubor obsahuje obfuskovaný kód užitý při reálném kybernetickém útoku (**Upozornění:** obsah souboru by mohl být v určitých případech potenciálně škodlivý, doporučujeme tedy dbát zvýšené opatrnosti při práci s ním).

Vaším úkolem je provést analýzu obsahu uvedeného souboru a odpovědět na následující otázky.

1) V jakém programovacím jazyku je obfuskovaný kód napsaný?
2) Jaký je dekadický RGB zápis ekvivalentní obsahu první proměnné, která určuje nastavení barvy?
3) Jaká hodnota musí být nastavena v proměnné 'pass' aby byla splněna podmínka kontrolující její obsah?

Otázka č. 7

Your organization requested to implement a technology, which will prevent the „in-memory" type of cyber-attacks, using the tools like MimiKatz. The solution has to protect all stored login information and domain names against techniques like „Pass-The-Hash" or „Pass-The-Ticket".

What is the name of the function in OS Windows 10 Enterprise, which addresses this problem? Which attribute should be set to make the function resistant against disabling it by a user with administrator rights on the protected station?

Otázka č. 8

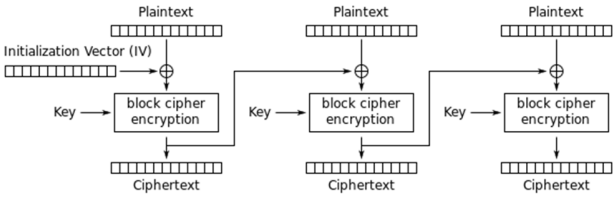
Jaké opatření by zvýšilo odolnost organizace proti útokům typu Pass-The-Hash? Zde jsou možnosti:

1) Rozdělení organizace do logických vrstev
2) Zakázání interaktivního přihlašování do nižších vrstev (např. doménových administrátorů na servery)
3) Vyškolení administrátorů v oblasti IT bezpečnosti
4) Nasazení monitoringu na bázi shromažďování a vyhodnocování událostí (eventů ze serverů)
5) Nasazení monitoringu na bázi sledování síťového provozu
6) Zkrácení doby platnosti přihlašovacích údajů (např. doba platnosti Kerberos ticketu)
7) Nasazení aplikace pro krátkodobé přidělování administrátorských oprávnění
8) Zakázaní internetového přístupu ze serverů
9) Zavedení vyhrazených administrátorských stanic

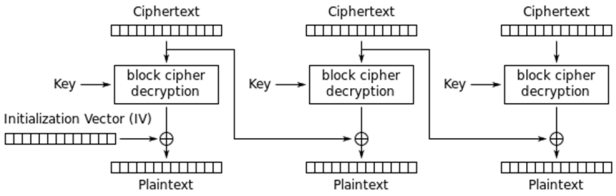
Jako odpověď uveďte číslo, které je součtem všech čísel správných odpovědí.

Otázka č. 9

Máme zašifrovanou zprávu, která má 7 bloků a každý blok má 64b. Kolik % zprávy je možné dešifrovat, pokud vznikne kompletní ztráta 2. bloku, 1b změna v 4. a 7. bloku? Úkol řešte pro CBC (Cipher Block Chaining).



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Otázka č. 10

PODKLADY K ÚLOZE JIŽ NEJSOU DOSTUPNÉ!

Cílem této úlohy je dešifrovat soubor zašifrovaný neznámým ransomwarem. Naštěstí víte, že se jednalo o běžný textový soubor. To by sice pro dešifrování nestačilo, ale dostanete k dispozici ještě také část komentovaného kódu ransomwaru, kterým byl soubor napaden.

Soubor i část kódu získáte na **odkaz již není dostupný.** Pro jednoduší práci s šifrovým textem Vám ho zobrazíme kódovaný Base64.

Možností řešení je více, ale pokud neradi skriptujete, doporučujeme využít Cryptool2 https://www.cryptool.org/en/cryptool2, který Vám může výrazně usnadnit práci.

7E0 CZ 2016
CYBER SECURITY COMPETITION

Úkoly pro FINÁLE soutěže

Úkol č. 1 – Týmová úloha

Tajné heslo je zakódováno níže. Jako klíč byla použita pasáž z Lipsum (viz. níže). Podaří se vám heslo dešifrovat, když napovíme, že se jedná o neprolomitelnou Vernamovu šifru (one-time pad)?

150d0 31f10 41054 51509 03491 94555 044a0 30447 03030 04d5d 13101 00619

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque hendrerit lorem vel nibh dignissim eleifend. Fusce non dignissim ligula, a suscipit felis. Nam congue congue neque, malesuada efficitur massa viverra sed. Nullam id justo ut quam rhoncus elementum sed vitae metus. Cras finibus blandit hendrerit. Fusce et sapien dui. Praesent vulputate lacinia pulvinar. Nunc tincidunt placerat leo non sodales. Vivamus pretium, dui vitae dictum luctus, dolor risus placerat leo, nec consequat lorem nisl eu nulla. Mauris aliquam felis ut turpis dictum, eget sodales diam luctus. Fusce lorem magna, egestas in nunc eu, eleifend finibus odio. Sed arcu sapien, gravida vitae leo eu, facilisis euismod metus. Donec mi magna, tristique sed nisl et, lacinia placerat nibh. Quisque sollicitudin sapien nisi, quis accumsan eros feugiat in. Sed facilisis eros sed odio consequat, ut ultricies sem iaculis.

Úkol č. 2 – Týmová úloha

PODKLADY K ÚLOZE JIŽ NEJSOU DOSTUPNÉ!

Najděte vlajku.

Úkol č. 3 – Týmová úloha

ÚLOHA VYŽADUJE SPECIFICKÝ HW

Máte k dispozici základní vývojářskou sadu DS-START-01.

Povoleno je využití webových zdrojů na www.iqrf.org, YouTube kanálu s tutoriály IQRF (zejména doporučujeme shlédnout díl **Network Set up with IQRF DCTRs**, díl **Network Control with IQRF DCTRs** a díl **How to make a network with IQRF OS 4.0**), a dále webový šifrovací nástroj http://testprotect.com/appendix/AEScalc.

Úkol:

1. Vytvořte zabezpečenou plně funkční síť IQRF sestávající z 1 koordinátoru a 1 nodu. Hesla pro bezpečné připojení členů sítě i pro uživatelské šifrování přenášených dat si zvolte.
2. Pomocí vhodného DPA příkazu zaslaného z terminálu v IQRF IDE blikněte červenou LED na nodu.
3. Vyčtěte obsah zašifrované RAM na nodu a dekódujte jej pomocí externího nástroje. Využijte Custom DPA Handler „UserEncryption“, který je součástí Startup Package.

Úkol č. 4 – Týmová úloha

ÚLOHA VYŽADUJE SPECIFICKOU INFRASTRUKTURU

Jste v roli penetračního testera, který má za úkol ověřit bezpečnostní opatření společnosti Advanced Water Solutions.

Vedení společnosti vám dalo za úkol, v rámci prověrky, získat interní projektovou dokumentaci unikátního technologického zařízení na levnou produkci vody ze vzdušné vlhkosti. Získanou dokumentaci předejte na flashdisku.

Připravili jste si průnik pomocí nezabezpečené WIFI uvnitř Advanced Water Solutions.

Vyšlete jednoho zástupce týmu provést prověrku bezpečnostních opatření. Může si vzít se sebou jeden notebook.

Úkol č. 5 – Týmová úloha

ÚLOHA VYŽADUJE SPECIFICKOU INFRASTRUKTURU – ÚLOHA NENÍ DOSTUPNÁ

Pro plnění úkolu můžete využívat Internet a jsou Vám k dispozici následující předinstalované nástroje:

- Webový prohlížeč,
- Burp Suite Free Edition,
- Notepad++,
- WinSCP.

Uvedené nástroje jsou plně dostačující pro řešení soutěžního úkolu, nicméně můžete použít jakýkoliv jiný nástroj, který zda není uvedený.

Úkol č. 6 – individuální test

Question 1:

What is Information security (INFOSEC)?

A. A collection of legal, organisational, technological and educational means aimed at providing protection of cyberspace.
B. Implementation of general security measures and procedures for protection of information against loss or compromise (loss of confidentiality, integrity and reliability), or as the case may be for their detection and adoption of remedial actions.
C. Use of such security measures in communications which prohibit unauthorised persons to obtain information which could be gained from access to communication traffic and its evaluation, or which ensure the authenticity of the communication process. Computer security as applied to data communications – data transfer.
D. The general approach to the development and use of capabilities to operate in cyberspace, integrated and coordinated with other areas of operation, to achieve or support the set objectives by using identified means, methods and instruments in a certain timetable.

Question 2:

What is Cyber Security?

A. Protection of confidentiality, integrity and accessibility of information in the Internet network.
B. Defence against a cyber-attack and mitigation of its consequences. Also, the resistance of the subject towards an attack and a capability to defend itself effectively.
C. A collection of legal, organisational, technological and educational means aimed at providing protection of cyberspace.
D. Military activity using electromagnetic energy in support of offensive and defensive actions to achieve offensive and defensive supremacy.

Question 3:

What is Authentication?

A. Provision of assurance that a claimed characteristic of an entity is correct.
B. The process of rights granting to a subject to perform defined activities in the information system.
C. Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
D. Complex activity including the analysis of computer virus behaviour, analysis of virus code, finding of the virus and its removal from files, or rectification of damage caused by the virus. More also in disassembly, debugger, tracing, code emulation.

Question 4:

What is Threat?

A. A potential cause of an unwanted incident which may result in damage to a system or organisation.
B. Danger, the possibility of damage, loss, failure.
C. Use of a data processing system to extract selected properties in the behaviour of a physical or abstract system.
D. Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.

Question 5:

What is Vulnerability?

A. Provision of assurance that a claimed characteristic of an entity is correct.
B. A quantitative measure of damage or loss as a consequence of a compromise.
C. Problem whose primary cause is known, or for which a method is established, to decrease or remove the impact of the problems on a service, using a substitute solution.
D. The weakness of an asset or control that can be exploited by one or more threats.

Question 6:

What is Firewall?

A. The method of designing data communication protocols, in which logically separate functions are abstracted from their underlying structures by inclusion or information hiding.
B. An electronic device connected to a telephone line to monitor the dialed numbers and alter them.
C. Data link protocol used to establish a direct connection between two nodes in local area networks.

D. Network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Question 7:

What is Risk?

A. A potential cause of an unwanted incident which may result in damage to a system or organisation.
B. Danger, the possibility of damage, loss, failure.
C. The possibility that a certain threat would utilise vulnerability of an asset or group of assets and cause damage to an organisation.
D. Use of a data processing system to extract selected properties in the behaviour of a physical or abstract system.
E. Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.

Question 8:

What Windows Command Line command shows MAC address of your computer?

A. IPCONFIG /ALL
B. SETLOCAL
C. SHOWNET /MAC
D. DRIVERQUERRY

Question 9:

What is Cloud computing?

A. Computer program that can intercept and log traffic that passes over a digital network or part of a network.
B. Type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.
C. A collection of software instructions, which performs a specific tasks executed by a computer.
D. Network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Question 10:

Who is not a Cracker?

A. A person who engages in the study and analysis of details of programmable systems most often for an intellectual inquisitiveness and keeps on improving this ability.
B. Somebody who enjoys programming and who programs well and fast.
C. Expert for a certain operating system or a program, e.g. UNIX.
D. An individual trying to obtain unauthorised access to a computer system. These individuals are often harmful and possess means for breaking into a system.

