5. ročník Národní soutěže ČR v kybernetické bezpečnosti

Ukázka soutěžních úloh 2. kola a finále

Datové soubory a přílohy se nezveřejňují. Některé úlohy není možné řešit bez on-line prostředí a doplňujících souborů.

EY	Reverse Proxy	Na této adrese: https://www.sskb-ey21.tech běží blog o kybernetické bezpečnosti, který se snaží informovat čtenáře o nejrůznějších zranitelnostech. Blog však sám adekvátně zabezpečen není. Dokážeš zneužít nesprávnou konfiguraci k získání vlajky?
MO	Díra na webu	Při zvědavém brouzdání po internetu jste nalezli přihlašovací formulář na adrese http://ks2021.ncko.cz/. Jako zkušeného hackera Vám přeběhl mráz po zádech, jak jste ucítili příležitost formulář prolomit. Tak hurá na to a najděte vlajku.
CETIN	ROT8000	**籤籐籯**籟簹簹簹 **籹絀籮**籿糈麤糔 **籤籐籯簍**簼 **麤**籿 衹籿麤籮类籽糔籱籿 **麤籲簍籲籽糈籿**籽糔籱籿 **籹**类籿籼籽絀籮麤糔簷 **籙**籿籴籾麤 籽籮籼籽糈籽籮 **糴糔**籽籼籴糐 **粔**籽籪籴粂籔 **籹**籪籴 籽籮籽糔 籱籽籮麤 **粔絀籮米**衹糐籔 **紱籮 米麤籮** 籿 **米籮米籲籬**籱 籿粂籾紱籲籽糔 籿 **籽**籿衹籽籿 **籼粂籼籽**糐衹籾 **鯨 籽米簷 籹**籿籼籾籽 **粔**籽籪籴絖 衹籮粔籲籽糈类籿麤籽糔 籪簪籮籬籮麤粂 籿 籟簹簹簹 **籹**籿粔籲籬簷 **簿**籪籴籿 **麤絖**籴籪粔 籿粂絀籮紿籮糔 **籽**糐籽籿 糗籿籿籱粂 **粔**籪麤籮米籽籮籃 **籤籐籯**籟簹簹簹

Dešifrujte zadaný text. Co máte zadat jako důkaz, že jste úlohu správně vyřešili, je uvedeno v textu, který dešifrováním získáte.

Flowmon	Captured traffic	Zjistěte, jaká zranitelnost byla využita k útoku na server 192.168.255.2. Zadejte CVE zranitelnosti ve formátu CVE-####-####, kde # je reprezentováno čísly. Viz. přiložený soubor 2_captured_traffic.pcap.
Trend Micro	IoT Systém	U jednoho z průmyslových IoT systémů ve firmě bylo 10. října 2017 zjištěno neobvykle vysoké zatížení procesoru.

		Technická podpora neobjevila žádnou příčinu. Proto podle vnitřního předpisu provedla restart zařízení, poté zálohu dat a systém přeinstalovala. Níže naleznete částečnou zálohu systému před reinstalací. Ověřte domněnku, že byl systém napaden útočníkem a odpovězte na tyto otázky: • Jaké uživatelský účet byl napaden (uživatelské jméno)? • Jaký spustitelný soubor útočník nainstaloval a spustil? • K čemu toto zneužití systému mělo útočníkovi sloužit (vyberte odpověď)? 1. Následné útoky DDoS 2. Těžba kryptoměn 3. Ransomware 4. Rozesílání spamu 5. Nevím
Trend Micro	Stolen Data	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 iterní síti firmy adresu 192.168.195.203. Předpokládá se, že útočník využil kompromitovaný systém s adresou 192.168.195.138. 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