Národní finále

6. ročníku Národní soutěže ČR v kybernetické bezpečnosti

Ukázka soutěžních úloh

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

1 - BEACON

One of indicators of malware infection is so-called beaconing. After successful attack, the infected host initiates a command & control (C2) connection to the infrastructure of the malicious actor. This is the way ho the malware asks his creator for further instructions. Using the C2 connection, the attacker can 'remote control' the activity of the malware at the infected host.

Beacons often connect to attacker's infrastructure in strictly regular intervals set by their creators.

Data

You have been given a file with network logs in json format as follows:

[{""timestamp"": ""1642685001"", ""ip_src"": ""10.39.155.216"", ""ip_dst"": ""10.10.8.1"", ""port_src"": ""52367"", ""port_dst"": ""1311"", ""protocol"": ""T""},...

Each record represents IP connection between 2 IP addresses that was recorded in a monitored network.

The data fields are:

- timestamp: Time when the connection started in UNIX timestamp format
- ip_src: Source IP address
- ip_dst: Destination IP address
- port_src: Source port
- port_dst: Destination port
- protocol: (T=TCP, U=UDP)

Data file name is:

1-data_nskb.json

****Goal****

The goal is to find beacon connections from an infected host IP address to a C2 IP, the connections repeatedly occur in regular interval.

****Flag****

The flag should be entered in the following format (no whitespaces allowed):

FLAG{beacon_destination_IP_addr,beacon_interval_in_sec}

Example: FLAG{1.0.0.0,3600}"

2 - LOGY

Národní centrum kybernetických operací zajistilo logy z napadeného stroje. Přiložený evtx log ze samostatně stojícího PC obsahuje události z období, kdy na něj byl proveden útok.

Zjistěte, co vše páchal útočník.

****Flag****

Vlajka je Vaším cílem, jen pozor, výsledek je ve formátu

FLAG={...} Pozor vlajka je CASE sensitive.

3A - ZÁJMOVÁ OSOBA

Vojenské zpravodajství v své rámci činnosti potřebuje dohledat určité informace k zájmové osobě. Tou je paní Jana Berger. Jediné, co o ní je k dispozici je, že v roce 2016 se objevila v reality show Popelka.

Paní Jana Berger sama sebe povoláním prezentovala jako modelka. Realita je však jiná, a pokud chcete, můžete ji odhalit.

****Otázka:****

1. Zadejte datum narození manžela Jany Berger ve formátu DDMMRRRR

3B - ZÁJMOVÁ OSOBA

Vojenské zpravodajství v své rámci činnosti potřebuje dohledat určité informace k zájmové osobě. Tou je paní Jana Berger. Jediné, co o ní je k dispozici je, že v roce 2016 se objevila v reality show Popelka.

Paní Jana Berger sama sebe povoláním prezentovala jako modelka. Realita je však jiná, a pokud chcete, můžete ji odhalit.

****Otázka:****

2. Zadejte mobilní telefonní číslo na manžela Jany Berger ve formátu ######### (bez mezer)

4 - BRITISH CYPHER

This report was found in a captured officer of the enemy army. Decrypt this message:

GRSYQ NAPXZ AOQPM KONCR NZURQ TCEDK ZRKBD KTIOP IMUHC YDCVD PQKZR ISCMQ

UICHK ODCAO YNCSP DVAOK KSUBS CTYKI BQAIC SOUMT ZREZS YYNRK MHCKR OYCQB

YNPTZ VBTOC KRHPP BZRKO DCCOD CISHQ CKEZE DAODK YNZRU RAORP BQVDE CONTI

QAXXX

Look for the password for the British cipher from the end of the nineteenth century among the general partners of the competition on their website.

You are browsing the homepage of the site. The man on this page will lend you his last name.

****Flag****

The answer is 15th and 22nd word of decrypted text written in following format:

word15;word22

5 - TAJNÝ ÚČET

Zpravodajská služba sledovala mafiána, který měl vyzradit číslo

tajného účtu ve Švýcarsku, na kterém je ukryto velké množství peněz z nelegální činnosti.

Bohužel mafiána někdo zradil a byl zabit. Mrtvola mafiána svírala

v ruce papír, který se dostal do Vaší forenzní laboratoře s úkolem

zjistit jestli neobsahuje číslo tajného účtu. Vyřešíte tento úkol?

6 - PCAP ANALYSIS

Úkolem tohoto zadání je získat heslo k přiloženému .rar souboru a následně root flag. Veškeré potřebné indície lze zjistit z analýzy přiloženého pcap souboru, který zaznamenal mimo jiné i komunikaci s lokálním serverem.

7 - HVIZD

Nezveřejňuje se.

8 - ASYMETRIC CYPHER

Geniální programátor vymyslel nový způsob asymetrického šifrování dokážete ho prolomit?

PS: Máte k dispozici veřejní klíč a část kódu na straně klienta.

9 - DANGEROUS EXE FILE

Analyze the attached fb.exe file, which does not look suspicious, but is dangerous!!! What type of attack does it contain?

There are known multiple names of this attack, use the most common name with two words.

10A - DATA ANALYSIS

Během aktualizace linuxového serveru objevil administrátor na disku v adresáři /var neobvykle velký binární soubor.

Protože před nedávnem došlo na jiném serveru ve firmě k úniku seznamu uživatelů, zajímá se IT oddělení, zda v souboru nebudou data související s útokem. Pokud by soubor obsahoval e-mailové adresy, musí být všichni nalezení uživatelé informováni o ohrožení jejich údajů.

Jako člen bezpečnostního týmu máte za úkol zjistit, zda soubor obsahuje emailové adresy a žádnou nepřehlédnout.

Najděte v zadaném binárním souboru všechny platné e-mailové adresy.

Odpověď

Jako správnou odpověď uveďte počet nalezených emailových adres.

Jako bonus můžete řešit úlohu 10B

Potřebné soubory

10-email.bin

10B - DATA ANALYSIS

Toto je bonusová část k úloze 10A. Nejprve musíte vyřešit úlohu 10A.

Správné řešení spočívá v tom, že všechny nalezené platné e-mailové adresy uložíte do nového souboru ve stejném pořadí, v jakém byly umístěny v binárním souboru, přičemž každou oddělíte od další znakem PIPE. Za poslední emailovou adresou znak PIPE není! Adresy uložte do souboru v ASCII kódování.

Odpověď

Následně spočítáte SHA256 HASH souboru a ten uvedete jako správné řešení

11 - PROUDOVÁ ŠIFRA

Použita vysokorychlostní proudová šifra, která byla poprvé představena v únoru 2003 na 10. workshopu FSE. V květnu 2005 byla zařazena do projektu eSTREAM sítě ECRYPT.

Dešifrujte:

U2FsdGVkX1/kG5P5EfyZ0fbQ3/19wLtohQ+jAdJEG7pz0+Fu27BgR6Khu/WyDdFau7w3chwm1UmAs46Jeab9d2N7+0HT/3wBQmwXXV4N3+r8XhiDtrV0SO4zXaCL1vw=

Šifra používá 128bitový klíč a víte, že přímo souvisí s doménou https://www.kybersoutez.cz/

Vlajka:

Jako důkaz, že jste úlohu vyřešili, postupujte dle pokynu v šifrovém textu.

12 - KLASICKÁ ŠIFRA

Vyluštěte šifrový text a zadejte jako důkaz o vyřešení název díla, ze kterého je daná ukázka. Použita je jedna ze základních klasických šifer.

UOSQI YUXYA KYBVF QSXQB CJQLV DPXYX CKJFQ SVNWM PIEJF YWSXF YXCQW VNYXC QEYKD VIDXC YBYKD NVXCY SDNSY BRQXY PRVEC JSQDP WQFBV QBQKJ XCYWE JFYAX JXQNE JXCJY FMEVX CSFYS JNMZJ NVFBJ NEVPO VWSXY PYCQK IEYBV UDAYV FUYFY OBQSW VFBJC EIVSV EVPIQ WSVDR EQBVD

NCYEV DIQNP QCQEQ XJSBY NVSJN QIENB MQRMX YKDFB VUJBY EVPIE UOSMF SUJFC YUOKJ XCYUO XJUYB YRMSJ QSYNW MXJKD CQNOS YAYWB QVFUY DCYNS QQVBK YSBQP JCEJU VWYSQ CQRMA JBQXY SBQPY KEVPI EVXCE YSISQ XCQIV WOSQF DXJKJ XCVIV SXCQE YWQSN BJPND NCYEV DPEVF BQWVU YCSQA YXCYB YPDXB DSBQI QWSVO VPYRM XJKYS IVEJP VFQCC SDXCX JNBJO MBYIE YUCVD XYCQN EMUOS YQSJI XYBQB JUOSY PJIEV RDWJS XYAYX CYPQC KMFPO SYWSF PODED QDFJW YSPYI VSVPE JUYBV DNSYB RVDXF JCJWV FBJCE OFYPW MXNVW QPYAX YKBYX IQSVU OFJSN DWYSY IVFPW YUOSX JPWQS XYKDX CYABM XYBAQ NVKJB DSMCM WYBQP QXYXY IEYWN VBUYK IEVRD WJSFX CQSQB QIJSX YFJBQ IQNFP QSODS QPQUQ SRDWJ CVFUY NCYEY AYXCY XIQSM FXJKS XJDPW EJFPY FYCXJ BQVFU JXYIE VRVDP JPQEV FYBXB JKAQN VRMAQ NQXJC QADIS BQXJS QIVAJ SQAYO VPJFV CXPJF VCYKC YUOPF JEQCN CYEQX BJKDP WFQEV NMIDC VFQSQ PQIVC EQFVD DPXJB QKYPF MNSMP YFYWJ NWMUV WYSQK PQKDK SQSIQ NXYBQ VNQKP JNPQK MXSYS QBQIQ WSVOV PYCVC QNMKD PYRMC BQVIQ NCVVB XYIEJ PIDXV RJSXF MKVFY UNQKB QPYFW JSQQS UOMKJ XCQQD CVEIQ DSVUV YSOV

13 - KLASICKÁ ŠIFRA II.

Vyluštěte šifrový text a zadejte jako důkaz o vyřešení jméno autora citátu. Použita je jedna ze základních klasických šifer.

EUSAO OEVVR UIDZO ANNZT AUODM LONJT SEPBE AKMHS ECNTI HOOUA HOXEI IDEEA ZLEAR ENEOT DNSZE CEJEE AOTMM UHKOT RIPTN OYIED OAAJO SPSEZ VINPI IUSAV SVIIK CKBZY EIZEI OLNEV PZTAU TDEEE VNUZJ HETXJ STONS ZUONP TNRSE AKCUO JENZJ DNCSU IECYR IEJTI OHTRS OHVIA ROLPT VDHCE OPDPZ EHBAY EIPVM KSNPT SOYZS OLVYI CUSEA KSCLR ZVIDX

14 - RUNNING STACK BUFFER OVERFLOW ATTACK

Nezveřejňuje se

15 - CYBERSEC EXPERT

Nezveřejňuje se

16 - THE UGLY BOTNET

Nezveřejňuje se