citeforma
Digital Security

R. Bravo ©

Identificação:
1. módulo do Curso: 10672 - Introdução à utilização e proteção de dados pessoais
2. nome completo: Matheus Malty Rubin
3. n.º de aluno: Y

Data de entrega: 30/11/2024

= I =

Enquadramento

Sugerem-se os motores de busca:
- bing.com
- Google.com
- Youtube.com

-=o0o=-

Os dois 'sites' habituais para encontrar legislação atualizada e/ou consolidada, são:
- www.pgdlisboa.pt
- www.dre.pt

-=o0o=-

Objetivos gerais:
No final da execução desta tarefa deverão ter ficado com conhecimento e informação sobre:
- legislação relevante sobre o ciberespaço e prova digital;
- quais os principais atos tipificados como crime;
- se trabalha ou se está relacionado com uma entidade que faz parte dos operadores essenciais de informação;
- a relevância do Direito da CIberSegurança (incluindo a dos dados pessoais) para um 'analista digital' e ou um membro da comunidade Ciber;

= II =

Tarefas: 15.
Tempo aproximado de investimento para execução: 90mn.

Objectivos especiais:
No final da execução das tarefas, deverão ter ficado com consolidação de conhecimento e informação sobre:
. utilização de comandos avançados para localização de informação na 'clear web';
. papel institucional da ENISA, do Cibercentro Português (CNCS) do CIRT e do CSIRT, bem como valências formativas; pelo Quadro de Referência Nacional, percebem pontos importantes da formação e a aplicabilidade prática;
. quais os tópicos valorados pela comunidade de segurança como mais importantes;
. quais as principais ciber-ameaças valoradas como importantes pela comunidade de ciberSegurança;
. doutrina portuguesa e anglófona sobre CiberSegurança;

. personalidades da ca inovação tecnológica e ideias de segurança defendidas;
. principais ‘leis’ de base académica e científica com relevância para a compreensão do tempo no avanço tecnológico;
. uma ideia da organização e do funcionamento da rede TOR, bem como de conteúdos expectáveis;
. uma ideia de sites sobre concretização de ameaças ou de ataques concretizados;
. alguns elementos históricos (menos conhecidos) relativos a decifragem;

1.
Socorrendo-se de motores de busca, procure recordar o que são ‘google dorks’ e como funcionam.

Escreva o comando avançado ‘google’ que lhe permite localizar documentos do formato ‘pdf’, só no ciberespaço nacional, com duas entidades: ‘Paulo Veríssimo’ e um ‘Cristiano Iria’.
RE:
filetype:pdf inurl:pt intext: Paulo Veríssimo AND Cristiano Iria

Qual é o título do documento encontrado e qual o ‘link’?
RE:
acesso bloqueado
RE:
https://repositorio.ul.pt/bitstream/10451/10100/1/ulfc105877_tm_Cristiano_Iria.pdf

1.2
O que é o ‘*unicorn search engine*’? quem é a empresa que o usa?
RE:
O Unicorn search engine é um serviço de pesquisa de dados relativamente desconexos dentro da rede social Facebook, por exemplo, trabalhadores da Intel, que moram em Taiwan. Utiliza um gráfico social para demonstrar estas relações.

1.2.1 o que é, ou para que serve a rede ‘mirai’?
A rede de bots chamada Mirai foi desenvolvida para injetar código malicioso em aparelhos relativamente simples, mas conectados à internet, internet das coisas, e lançar ataques de derrubada de servidores. A rede Mirai utiliza-se das vulnerabilidades como senhas padrões, acesso remoto, firmware não atualizado, para "arrecadar" mais bots. Com uma larga rede de bots, pode-se então realizar a derrubada de servidores mais potentes e mais resistentes a este tipo de ataque.

2. Utilizando o mesmo motor de busca citado, localize:
- O CERT português; para que serve, ou qual a missão?
RE:
Segundo a Autoridade Nacional de Comunicações, o CERT.PT tem como missão tratar e coordenar a resposta a incidentes cibernéticos, produzir alertas e recomendações de segurança, e promovendo uma cultura de segurança em Portugal.

. qual é o endereço web desse site?
RE:
https://www.cncs.gov.pt/pt/certpt/

. o que é e para que serve um CERT?
RE:
O CERT.PT se insere dentro da gama de serviços do Centro Nacional de Cibersegurança (CNCS) e se encarrega de auxiliar no tratamento e resposta a incidentes cibernéticos para um público alargado, desde entidades da administração pública, abrangendo até todas as pessoas singulares ou plurais com sede em Portugal ou que estejam em território nacional.

. o que é e para que serve a rede CSIRT?
RE:
A rede CSIRT é uma liga de pessoas coletivas em função da resposta a incidentes cibernéticos. Mais do que propriamente um time de resposta a incidentes que seus membros possam receber, a CSIRT é um canal oficial de comunicação e estratégia em relação ao que os times de resposta a incidentes possam fazer. Faz parte dos seus objetivos criar estes laços entre seus membros, criar estatísticas nacionais, coordenar os instrumentos necessários à prevenção e resposta rápidas em caso de um grande incidente, uniformizar a nomenclatura e classificações de incidentes a âmbito nacional, e também promover a cultura da cibersegurança em Portugal.

. onde posso (qual é o 'link') para reportar um incidente de segurança ao CNCS?
RE:
https://www.cncs.gov.pt/pt/notificacao-incidentes/

. qual é o endereço eletrónico no site da CNPD para se comunicar uma brecha de segurança de dados pessoais?
RE:
https://www.cnpd.pt/DataBreach/DataBreach_pt.aspx?AspxAutoDetectCookieSupport=1

R. Bravo ©

2.1 localize:
- o Centro Nacional de Cibersegurança (CNCS);
. analise a página de 'boas práticas' do CiberCentro Português;
. o que é a iniciativa 'cidadão ciberseguro' do Centro Nacional Cibersegurança?
RE:
O cidadão ciberseguro é o primeiro de quatro cursos ofertados pelo CNCS que buscam educar os cidadãos portugueses sobre a conduta que têm na internet, a fim de promover maior segurança da população.

e qual é o esforço estimado para esse evento?
RE: O primeiro curso versa em torno de 3 horas.

. o que é a iniciativa 'cidadão ciberinformado' do Centro Nacional Cibersegurança?
RE: O cidadão ciberinformado é o segundo destes quatro cursos. Neste o foco é a veracidade de informações disponíveis online. Aqui são repassadas dicas de como identificar fake-news, como validar asserções e como tratar mensagens e correntes de desinformação.

e qual é o esforço estimado para esse evento?
RE: Assim como no primeiro, a carga horária prevista é de 3 horas.

- quem são e quais são os objetivos destas entidades referidas nestes sítios:
. Redecsirt.pt
RE: Liga de entidades responsáveis por assegurar a segurança da informação que visa proteger tanto seus membros, como os usuários e consumidores de seus membros, estabelecendo um canal de comunicação nacional voltado à resposta de incidentes. Por exemplo, em caso de um incidente de vasta dimensão, esta rede entra em ação coordenada. Mas fora situações de crise, ela busca manter seus membros atualizados sobre as ameaças e unificar a terminologia e as linhas de classificação de incidentes, com reuniões trimestrais.
. Ap2si.org
RE: A Associação Portuguesa para a Promoção da Segurança da Informação promove a conscientização da necessidade de se proteger as informações no meio cibernético.
. First.org
RE: É uma associação voltada para a melhoria da comunicação de times de resposta a incidentes pelo mundo inteiro, visando replicar na defesa da internet a mesma amplitude global que a mesma tomou.
. CIIWA.pt
RE: É uma associação portuguesa de cunho público voltada para a contra-inteligência e guerra cibernética da informação. Promove parcerias com entidades nacionais e internacionais nas áreas da defesa, segurança, governação estatal e empresarial.

. em território nacional, onde se encontra o Curso de Segurança da Informação Classificada?
No domínio nau.edu.pt.

3.
Em relação à European Union Agency for Cybersecurity, localize:
- a página de tópicos do site;
. quantos são os tópicos enunciados?
. quais são os tópicos enunciados?
RE: 21
RE: Estes são: awareness raisin, certification, cloud, criptography, covid19, critical infrastructure, cyber crisis management, cyber threats, cybersecurity policy, education, emerging technologies, foresight, incident reporting, incident response, market, national cybersecurity strategies, research and innovation risk management, standards, training and exercises e vulnerability disclosure.

- localize o relatório 'Threat Landscape Report 2018' do European Union Agency for Cybersecurity;
. quantos e quais são os 'top cyberthreats' ali enunciados?
RE: Quinze são os top cyberthreats enunciados no Threat Landscape report 2018 da ENISA. Estes são: cyber espionage, ransomware, cryptojacking, identity theft, information leakage, physical manipulation/damage/theft/loss, insider threat,data breaches, botnets, spam, denial of service, phishing, web application attacks, web based attacks e malware.
. Quantas e quais são as entidades aí enunciadas que foram exfiltradas ('breaches')?
RE: 15. São elas: Huazhu Hotels Group, Facebook, Twitter, Aadhaar, Exactis, Timehop, GOMO, Company affiliated to FedEx, Orbitz, COMCAST, SingHealth's outpatient clinics, 211 LA County, British Airways, Google e ainda DHS, ALERRT, Ticketmaster, RailEurope e icliniq
. Quantas e quais são as ações de mitigação do tópico 'data breaches'?
RE: 11. Estas são classificar os dados para refletir o nível de proteção necessário; implementar soluções de prevenção de perda de dados tanto em trânsito ou estáticos; encriptar os dados parados e em trânsito; garantir que os acessos são baseados no princípio do mínimo privilégio; desenvolver e implementar políticas de segurança para todos os aparelhos; orquestrar o gerenciamento de updates e patches dentro de um quadro de referência de vulnerabilidades; desenvolver novas políticas para palavras-passe mais robustas e verificação de dois fatores; limitar a quantidade de informação sensível armazenadas em aplicações de web; implementar políticas de proteção contra malwares e ameaças internas; implementar um plano holístico abrangindo tanto a avaliação da exfiltração quanto o desenvolvimento de uma resposta apropriada àquele incidente e por último, reforçar programas de conscientização de segurança para os colaboradores da organização.

R. Bravo ©

4.
Onde encontra a publicação número 133 dos Cadernos do 'IDN' – Instituo Defesa Nacional?
RE:
pesquisei no Google, porque o link Cadernos IDN, dentro do domínio desta instituição só resultou publicações de 2020 até p presente, e menos de 100 números. Pelo link direto do Google, vi que a revista em questão estava sob outro submenu, de Defesa Nacional.
O sítio é https://www.idn.gov.pt/pt/publicacoes/nacao/Paginas/NeD133.aspx

. qual é o tema dessa revista?
RE: Cibersegurança

. faça o download dessa publicação; leia os artigos de pág. 113 a 147;
RE:
primeiro artigo, de Paulo Nunes, é bem pouco atual. Ele chama para que se construa o CNCS, e integra-o nas estratégias nacionais de Cibersegurança e também na de segurança e defesa. Visivelmente foi produzido por um burocrata. Seus conceitos são abstratos e, por vezes, inconsistentes. Mas o que mais me surpreende é o subtom perpassando todo o artigo de que Portugal precisa estar na vanguarda da cibersegurança e caso essas instituições não venham a se concretizar, este "lugar" pode ser desdenhado para apenas obedecer às diretrizes de outros países e outras instituições. É importante notar que o âmbito estatal é mais sensível ao valor da cooperação face à competição, e que este burocrata mantém, mesmo em 2012, uma forte posição de competição e de afundamento no plano das nações, ao invés da básica referência à segurança de todos os humanos que participam na Internet. Todas as frases que colocam os usuários como prioridade de se defender não estão em causa nesta crítica. O autor também versa entre cibersegurança e ciberdefesa, vendo-as a partir da estratégia nacional de segurança e defesa, e da componente histórica, como complementares, alocando a segurança mais na área do monitoramento e deteção, e a defesa mais na área da reação e combate cibernético efetivamente.

Já o segundo artigo é mais pedagógico e introdutório com referência a vários termos técnicos e ao enquadramento geral da prática de segurança da informação dentro das atividades e responsabilidades de uma organização. Este tange certificações como ISO 27001, as guias do NIST da série SP 800, introduz o leitor a uma gama de corpos certificadores e avaliadores. O cerne do artigo articula os cinco pilares principais, que são a governança, tecnologia, processos, pessoas e standards e recomendações do mercado, para a apresentação dos componentes da segurança da informação, mas quando trata dos desafios, à época, da segurança da informação, o autor troca o último componente para "Assurances".

R. Bravo ©

4.1
Onde encontra a expressão ‘QNRCS’ no ‘ciberespaço português’? trata do quê?
RE: Dentro do sítio do conselho nacional de cibersegurança.

- identifique e leia o capítulo ‘definições e abreviaturas’ do QNRC (apenas duas páginas e meia); do que se trata?
RE:
Trata-se de abreviaturas e definições, maioritariamente por instrumentos legais, de termos técnicos utilizados com frequência tanto no documento em questão, quanto nos âmbitos industriais e comerciais da cibersegurança.

5.
Identificação de personalidades:
Quem foram estas pessoas? São responsáveis por algo distintivo na indústria Ciber?
5.1. quem foi Tim Berners-Lee? O inventor da world wide web, co-criador da linguagem HTML, do hypertext transfer protocol (HTTP) e da uniform resources locator (URL).
5.2. quem foi Steve Case? O fundador da AOL, que catalizou o uso comercial da world wide web e consequentemente sua grande difusão dos anos 1990.
5.3. quem foi William Gates the III? Este é mais conhecido como Bill Gates, co-fundador da Microsoft.
5.4. quem foi Fred Cohen? Pioneiro na cibersegurança, Fred Cohen foi quem concebeu o termo vírus de computador, e foi o responsável por várias técnicas de defesa contra vírus.
5.5. quem foi John Forbes Nash? Qual o nome da teoria que lhe valeu um prémio Nobel? John Nash foi um grande pensador matemático. De seu legado, o que mais lhe trouxe reconhecimento foi o equilíbrio de Nash, no campo da estratégia, onde duas ou mais partes, dentro de uma situação, com um conjunto de opções, não se veem pressionadas a alterar suas ações, independentemente da ação das outras partes.

5.4.3 Em aula foram atribuídas duas frases consideradas marcantes quanto ao risco e quanto à inviabilidade total de ciber-segurança, ou de se conseguir fazer total oposição ao ‘hacking’[1]. Foi um cientista chamado Fred Cohen. Quais são as ideias em causa?
RE: Bem, não me lembro das duas frases em sala. Porém, posso materializar aqui comigo duas ideias inerentes à impossibilidade de uma rede 100% segura. A primeira é que a tecnologia está constantemente se desenvolvendo. Vemos atualmente uma expansão massiva da superfície de ataque, aumentando desta forma as vulnerabilidades e tornando penetrável o que anteontem parecia impenetrável. A segunda é a inerente rotatividade dos trabalhadores de uma organização, o que implica em treinos de segurança da informação contínuos e um bolsão de risco, a aumentar e diminuir, a depender das pessoas que legitimamente

[1] ‘não há segurança absoluta’; ‘não há risco zero’;

acessam os recursos da dita organização. É evidente que esta segunda é uma componente da primeira ideia, assim como o risco é uma componente da segurança.

6.1
Identificação de personalidades ligadas à “Indústria Ciber”: localizes estas “leis das tecnologias”; o que significa a:
. Lei de Moore
Revista em 1975, prevê que o número de transistores em um circuito integrado dobra, mais ou menos a cada dois anos, sem grandes aumentos para o consumidor final.
. Lei de Rock
Esta lei prevê que o custo de uma fábrica de chips semicondutores dobra a cada quatro anos.
. Lei de Metcalf
Quanto mais conectada, mais rica é a rede. O valor da rede é exponencialmente proporcional ao número de usuários nela, com exponente 2. Tem um limite.
. Lei de Gilder
A capacidade da banda larga de uma rede de comunicação triplica a cada ano, aumentando em muito a potência desta rede.
. Lei de Kryder
Esta lei prevê que a densidade de discos rígidos para armazenamento dobra a cada 18 mêses, fazendo com que o custo de armazenamento caia e o uso destes aparelhos aumente.
. Lei de Koomey
Esta lei trata da capacidade de processamento por unidade de energia, medida em computações por joule. Diz que esta também dobra a cada 18 mêses.

O que lhe sugerem estas ‘Leis’ apreciadas em seu conjunto?
RE:
Em primeira instância, a apreciação destas leis de TI e comunicações sugerem que a potência do ciberespaço só aumenta, exponencialmente, em diversas frentes ao mesmo tempo. Tomando-as com um pouco mais de detalhe, vale-me o exemplo para demonstrar que todo domínio tem seu limite. Indico isto na última frase do meu rascunho da lei de Metcalf, pois é a menos técnica, mais social, mais volátil e mais visivelmente falha. Falha, porque não é difícil conceber que uma rede ultraconectada possa alavancar condições para sua própria destruição, ou seja, a concretização da desvalorização total da rede, a partir de um certo ápice na relação densidade-valor da mesma. As outras leis, tangendo a capacidade de processamento, a capacidade de arquivamento, a capacidade de velocidade de transferência, a capacidade de otimização energética do processador (excluindo a lei de Rock, sobre o custo das fábricas de semicondutores), soam um tanto mais técnicas e mais facilmente justificadas em explicações técnicas, mas sem dúvida também limitadas. Em verdade, não penso que nenhuma das formulações originais realmente as conceptualizaram já neste formato atemporal, porque não consigo conceber que alguém pense que isso dure para sempre. Afinal, é isso que significa o vetor

atemporal, “indefinidamente”. É esta crítica basal às leis aqui discutidas que me ajuda a dar corpo à demonstração de que todo domínio tem seu limite. Dizem que o conceito de Zeitgeist de Hegel faz essencialmente o mesmo: perspectiviza, coloca em perspetiva histórica. Os domínios das asserções acima, (tecnológico, material, energético, físico, químico, econômico) têm seu limite. Há fatores de contenção desta expansão. E é justamente estes fatores que as indústrias tentam contornar, ou superar, quando almejam e alcançam uma revoluçãozinha interna e lançam aí, em cima desta descoberta cientifico-mercantil, seu novo produto. O argumento base, um tanto malthusiano, é que a matéria-prima para estes produtos é finita. Logo, é impossível que haja qualquer asserção sobre estas capacidades, ou sobre estes domínios, em modo atemporal. Dito isto, reforço que não imagino que nenhum destes físicos tenham acreditado na atemporalidade destas asserções. Em outras palavras, esta reflexão não é válida na prática. Mas ela aponta dois limiares dentro do domínio da capacidade, o da expansão e o do limite. A realidade industrial é uma curva traçada entre estes dois eixos, cheia de “fatores de contenção” que viabilizam ou inviabilizam a concretização das nossas intenções, com quatro quadrantes diferentemente valorizados centrados em uma contradição. A dialética hegeliana supera a contradição na síntese, na abertura de um novo domínio, que por fim, tem seu limite.

6.2 Em que consistem as três leis de Asimov e para que podem servir?
RE:
Primeiro, um robô não pode ferir um humano ou permitir, por inação, que algum mal lhe aconteça. Dois, um robô deve sempre obedecer a ordens de humanos, exceto em casos de conflito com a primeira lei. E a terceira, um robô deve proteger sua própria existência, exceto em casos de conflito com as duas leis anteriores.
As três leis de Asimov, também conhecidas como as três leis da robótica, servem para garantir uma hierarquia entre máquinas e humanos. Atualmente, penso, essas leis vêm sofrendo revisões para ficarem mais acuradas à realidade e menos à ficção científica.

7.
Em não mais que dois parágrafos, responda:

a) Quantos níveis (‘layers’, ou níveis, ou ‘camadas’) de ‘navegabilidade’ e de acesso a informação, considera existir no CiberEspaço?
   RE: Três, que são a clear web, transparente, a deepnet, turva, e a darknet, oculta.
b) Quais são as principais redes que compõem a chamada ‘darknet’?
   RE: I2P, TOR e FreeNET

8.
Que utilidade podem ter estes sites, enquanto eventual analista de dados para a Segurança da Informação na área digital forense?

- http://www.zone-h.org/archive – portal para anunciar algum crime cibernético
- https://defacer.id/ - bloqueado pelo antivirus
- http://www.hack-mirror.com/ - não parece ser nada relevante, potencialmente periogoso.
- https://www.openbugbounty.org/ - portal de conexão entre donos de sítios web e pesquisadores de segurança para achar e remediar vulnerabilidades
- https://hackernoon.com/ - portal de leitura sobre cultura de hacker.
- https://databases.today/ - redirecionado para snusbase.com, um portal de publicação de exfiltrações de banco de dados, fomentados por pesquisadores de segurança e fóruns na DarkWeb.
- https://www.pgdlisboa.pt – fonte de referência de leis em Portugal.
- https://www.enisa.europa.eu (ver o 'tag' publications) – portal de publicação de relatórios sobre cibersegurança da Agência Europeia de Cibersegurança.
- https://cert.europa.eu (ver o 'tag' publications / Threat intelligence) – relatórios mensais sobre os desenvolvimentos em cibersegurança.

9.
Localize os relatórios conhecido por 'IOCTA', disponíveis no site da EuroPol. Faça download do 'IOCTA' de 2021;
- o que é o 'flubot'?
RE:
Flubot é um cavalo de troia utilizado para fraudar interfaces de bancos online. Ele instala máscaras de interfaces e rouba as credenciais financeiras das vítimas. Faz uso de um algorítimo de criação de domínio (DGA) o que viabiliza a rápida migração do servidor de comando e controlo para um novo hospedeiro, caso o atual venha a ser bloqueado ou derrubado. Esta ameaça se espalha por auto-propagação via SMS para os contatos da vítima.

- Quais são as conclusões chave ('key findings') sobre o crime ciberdependente ('cyber-dependent crime') que ali vêm descritas?
RE:
Três são as conclusões principais desta seção: a amplificação do uso de programas afiliados a ataques ransomware buscando brechas na segurança de parceiros na cadeia de produção dos alvos finais; malware tornou-se um modelo de negócio viável, com capacidades como perpassar autentificação de duas fontes e realizar spam de SMS. Por último, um aumento de uma tática mais antiga, que é a extorsão para não cometer um ataque de derrubada de serviços, alegando serem ameaças avançadas e persistentes famosas na segurança da informação, a fim de aumentar a pressão contra as vítimas.

- a expressão 'crisis management' aparece neste relatório? A que propósito?

RE:
Aparece sim, no contexto de introduzir as agências policiais e investigadoras às ferramentas de gerenciamento de crise a fim de melhorar a capacidade cibernética dos agentes policiais.

10.
Descreva por palavras suas no máximo de 3 parágrafos para cada alínea, o que entende por:

a) 'transição digital';
   RE:
   Transição digital é uma alteração de mentalidade que repercute em e se conjura a partir da transformação de processos analógicos para formato digital. Mais do que substituir o papel pelo computador, ela está mais próxima de substituir o armazenamento local de ficheiros, servidores, e aplicativos da empresa em questão, por um modelo coparticipativo com provedores de serviço de nuvem.
   A meticulosidade de mensura dos indicadores de consumo em nuvem, se castateia para dentro da empresa que adota este passo, e transforma seu modelo de negócios para coletar dados e criar métricas ela, por exemplo, de saúde, de produção, de relações, dentro da organização. Com estes dados, outras alterações passam a ser plausíveis, onde antes não eram nem vistas.
   Em suma, a transformação digital é um processo de alteração da forma de se realizar a entrega do produto e/ou serviço que faz uso de muitas tecnologias em conjunto.
b) 'singularidade tecnológica';
   RE:
   Singularidade tecnológica é a ideia de um momento histórico, alegadamente no futuro, quando a inovação tecnológica será tão intensa quanto contínua, a ponto de acordarmos sem saber o que de novo pode acontecer.

11.
Localize os termos 'purple', 'magic' e 'venona'.
- consegue determinar qual o denominador comum entre estas expressões?
RE: Sim, é o serviço de inteligência, que trabalha em favor da proteção dos interesses da respetiva nação, ou país.
- considera que historicamente este tipo de atuações perderam interesse prático?
RE: Sim e não. A segunda guerra, assim como a guerra fria já se vão no horizonte. As comunicações bombam todos os dias mais alto. Os presidentes não mais precisam de uma linha especial para se comunicarem, seus meios de comunicação se multiplicaram, assim como os nossos. Mas ainda hoje temos guerra, vide a lástima de Israel contra Palestina. Os meios bélicos têm se diferenciado vividamente também. O COVID foi somente um teste sobre as reações mundiais em caso de guerras com agentes biológicos. As leis deixam de ser respeitáveis; consequência da singularidade tecnológica. O serviço de inteligência hoje está mais voltado ao cyberwarfare, ou guerra cibernética. Um tipo de guerra fria, onde os agentes ficam

todos lá, convivendo em paz, uns se vendo, outros não, mas sem interferência física no território e na soberania dos outros. Gostaria de pensar que este tipo de guerra fria fosse um exercício para a convivência em paz e sem o medo de sucumbir, como no tom expresso no artigo de Paulo Nunes, comentado acima, mas infelizmente não é o que a realidade nos comprova.

12.
O que entende por Ciência de Dados?
RE: A ciência de dados é a disciplina que estuda as maneiras de se colher o máximo de benefícios possível a partir de um certo conjunto de dados, e foca em especial na prática de tratar, limpar, extrair, converter, polir, a depender do que é que se está almejando conseguir com esta específica aplicação deste conjunto de dados.

13.
Explique por palavras suas o que são estes mecanismos de proteção de redes informáticas:

- uma ‘firewall’: um conjunto de regras que autorizam ou bloqueiam a transmissão de pacotes de informação.
- um ‘iDS’: um sistema de deteção de intrusos tem por tarefa emitir alerta para o administrador de uma rede que existem intrusos dentro, ou ao menos tentando adentrar a rede.
- um ‘iPS’: um sistema de prevenção contra intrusos toma atitudes, como colocar o intruso em quarentena, ou fechar uma certa porta automaticamente, em resposta aos alertas emitidos pelo iDS.
- um ‘EDR’: significa deteção e resposta a “endpoints”, que são efetivamente os computadores de usuários dentro de uma rede. Trabalha e responde a ameaças vindas das margens das redes, tentando autenticar todo aparelho que venha a aceder à rede e monitorando seu comportamento.

Consegue perceber se é possível extrair dados destes dispositivos de segurança acima indicados, para análise posterior a um ciber-incidente? O que eles podem revelar?
RE: Sim, definitivamente. A análise forense destes dispositivos vai depender se foram inicialmente configurados para produzirem logs detalhados das atividades que controlam. Os logs de firewalls, por exemplo, nos dá informação sobre conexões bloqueadas, permitidas, assim como comportamento suspeito que gerou algum alerta. Logs de dispositivos de EDR nos mostram detalhes sobre comportamento de ficheiros, por exemplo, o que nos ajuda a identificar possíveis ataques. OS logs de IPS/IDS nos trazem informações detalhadas sobre o tipo de ataque, o IP de origem, o IP de destino assim como pacotes que foram capturados e bloqueados e seus conteúdos.

14.
Qual é a diferença entre ‘codificar dados’ e ‘cifrar dados’?

RE: Se o professore está se referindo a “encoding” por codificação, então esta serve para transformar o formato da informação para que a mesma possa ser consumida corretamente por outro sistema, que não seria capaz de ler a informação em seu formato original, sem a codificação. A codificação não torna a informação secreta, muito pelo contrário, ela tenta facilitar a compreensão por outra máquina, que usa outras formas de leitura da mesma informação. Já a cifra, esta tem por propósito tornar a informação secreta, tal que só quem tem a chave para decifrar a informação é que conseguirá obtê-la.
Dê exemplos de codificação de dados;
RE: A codificação de dados é utilizada na comunicações de rede, na compressão de ficheiros, e também em conversão de ficheiros de um formato em outro.

15.
O que é um ‘hash’ de um ficheiro, ou, o que é o ‘hashing’?
RE: O hash de um ficheiro é uma sequência de letras e números e alguns símbolos que resulta da computação da informação inserida inicialmente. O processo de hashing não converte a informação em outro modelo, secreto ou não, mas calcula esta sequência de caracteres para a informação inserida. Isto gera uma sequência específica que será comparada com a sequência correta para determinar se a informação inserida foi alterada ou está idêntica à original. Utiliza-se hashing, por exemplo, com palavras passe. Assim, quem obtiver os dados salvos no servidor, nunca irá encontrar as palavras passe, mas somente o hash das palavras passe, que não é reconversível na palavra, a não ser que se saiba o método de hashing utilizado.

16.
Após conclusão destas tarefas, salve o documento, e execute um ‘hash’ sobre este documento, com o algoritmo MD5 e com outro algoritmo à sua escolha.
Porquê fazer ‘hashing’ dos ficheiros com o algoritmo MD5 e mais um algoritmo diferente do primeiro? Alguma razão para isso?
RE: A isto chama-se de hash duplo. Um hash duplo, apesar de raramente necessário, adiciona mais um nível de proteção àquela informação. Os algorítmos de hashing modernos são robustos e apenas um hash eficiente pode providenciar o nível de segurança adequado, porém, para informações altamente confidenciais, um hash duplo pode ser considerado. Seu lado negativo é que utiliza muita capacidade de processamento.

17.
Quais são os pontos principais que qualquer cidadão ou profissional de cibersegurança tem de ter em consideração quando lida com ‘dados pessoais’?
RE: Toda e qualquer pessoa que venha a aceder a dados pessoais deve se perguntar a) para quê, b) até quando e c) por quem a fim de determinar quem pode aceder a tais dados, em função de qual propósito e durante qual período. Também é preciso recolher consentimento escrito quando da recolha destes dados e também providenciar formas de revogação do mesmo consentimento.