"Фишинг"дегеніміз не?

A) зиянды бағдарламаның түрі

B) криптография әдісі

C) құпия деректерге шабуыл түрі 1

D) сымсыз желі түрі

E) бағдарламалау түрі

Электрондық пошта арқылы зиянды файлдарды жіберуге негізделген шабуылдың қандай түрі бар?

A) DDoS шабуылы

B) Вирус

C) SQL инъекциясы

D) Фишинг 1

E) Ботнет

"VPN" аббревиатурасы нені білдіреді?

A) желілік құрылғылардағы виртуалды жад

B) виртуалды жеке желі 1

C) виртуалды процессор дискісі

D) желіге арналған сыртқы процессор

E) сервердегі виртуалды порт

Төмендегі қауіпсіздік шараларының қайсысы парольді асыра сілтеуге негізделген шабуылдардың алдын алуға көмектеседі?

A) екі факторлы аутентификация 1

B) IP мекенжайларын бұғаттау

C) Қатты дискіні шифрлау

D) электрондық поштаны сүзу

E) Брандмауэр

Желі қауіпсіздігі контекстінде "бекдор" нені білдіреді?

A) деректердің сақтық көшірмесін жасау қызметі

B) жүйеге жасырын қол жеткізуді қамтамасыз ететін зиянды бағдарламалық жасақтама 1

C) маршрутизатордың бөлігі

D) деректерді шифрлау әдісі

E) сымсыз желі технологиясы

=

"SQL инъекциясы" шабуылы нені білдіреді?

A) сымсыз желілерге шабуыл

B) электрондық поштаға шабуыл

C) веб-қосымшаларға шабуыл 1

D) DNS серверіне шабуыл

E) маршрутизаторға шабуыл

Компьютерлік қауіпсіздікте "брандмауэр" дегеніміз не?

A) деректердің сақтық көшірмесін жасау бағдарламасы

B) сымсыз желілерге қосылуға арналған құрылғы

C) вирустарды жою бағдарламасы

D) желілік трафикті басқаруға және сүзуге арналған құрылғы немесе бағдарламалық жасақтама 1

E) желілік адаптер

Төмендегі мәлімдемелердің қайсысы күшті парольдерге қатысты дұрыс?

A) күшті парольдер әрқашан әріптер мен сандардан тұрады

B) күшті парольдер әрқашан қысқа және есте сақтау оңай

C) күшті парольдерді сөздік шабуылдарды қолдану арқылы оңай табуға болады

D) күшті парольдер әдетте ұзын, әр түрлі таңбалардан тұрады және оларды табу қиын 1

E) күшті парольдер әрқашан бір сөзден тұрады

"Блокчейн" дегеніміз не?

A) қорғаныс бағдарламалық жасақтамасының түрі

B) деректерді шифрлау технологиясы

C) орталық басқарусыз цифрлық ақпаратты сақтау және беру тәсілі 1

D) пайдаланушылардың аутентификация әдісі

E) деректерді қысу технологиясы

"HTTPS" аббревиатурасы нені білдіреді?

A) сенімді электрондық пошта

B) жоғары жылдамдықты интернет

C) қауіпсіздіксіз гипермәтіндік хаттама

D) қорғалған гипермәтіндік хаттама 1

E) өте жылдам прокси-сервер

Қандай шабуыл екі құрылғы арасындағы желілік трафикті ұстап, жазуды қамтиды?

A) брандмауэр шабуылы

B) желіаралық маршрут

C) жалған IP мекенжайы

D)ман-орта шабуыл (MITM) 1

E) Фишинг

"Екі факторлы аутентификация"дегеніміз не?

A) екі құпия сөзді қажет ететін Аутентификация

B) екі саусақ ізімен тұлғаны тексеру процесі

C) екі пайдаланушы өздерінің жеке басын растауы керек жүйе

D) екі түрлі растау элементін қажет ететін аутентификация әдісі, әдетте құпия сөз және бір реттік код 1

E) құпия сөздерді сақтаудың қорғалған әдісі

Желі қауіпсіздігі контекстінде "іздердің арқасында" дегеніміз не?

A) деректерді шифрлау әдісі

B) маршрутизаторға шабуыл

C) аутентификация үшін құпия сөз немесе сөз тіркесі

D) пайдаланушының әрекеттері туралы жүйеде қалдырылған ақпарат 1

E) интернетте анонимді серфингке арналған Технология

Төмендегі шаралардың қайсысы "DDoS" шабуылының алдын алуға көмектеседі?

A) Фишинг

B) антивирустық бағдарламалық жасақтаманы орнату

C) электрондық поштаны сүзу

D) IP мекенжайларын бұғаттау 1

E) файлдар мен қалталарға кіруді шектеу

"Зиянды бағдарламалық жасақтама" (малваре) шабуылдары нені білдіреді?

A) құпия сөздерді бұзу әрекеттері

B) вирустар, трояндық жылқылар, құрттар және басқа да зиянды бағдарламалар 1

C) физикалық қауіпсіздік шабуылдары

D) аутентификация әрекеттері

E) желілік құрылғыларға шабуылдар

Қандай протокол интернет арқылы деректерді қауіпсіз тасымалдауды қамтамасыз етеді?

A) HTTP

B) FTP

C) TCP

D) SSL/TLS 1

E) UDP

Сымсыз Wi-Fi желісін қорғау үшін қандай қадамдар жасау керек?

A) барлық құрылғылар үшін ашық қол жетімділікті пайдаланыңыз

B) құпия сөзді орнатпаңыз

C) MAC мекенжайын сүзуді қосыңыз 1

D) шифрлауды өшіру

E) әлсіз құпия сөзді қолданыңыз

Қашықтағы хакердің командаларын орындау үшін көптеген вирус жұққан компьютерлер қандай шабуыл түрін қолданады?

А) Вирус

B) Фишинг

C) Ботнет 1

D) DDoS шабуылы

E) трояндық ат

"IoT" аббревиатурасы нені білдіреді?

A) жасанды интеллект және машиналарды оқыту

B) Интернет бұлтты технологиялар

C) Интернет-сауда

D) Заттар интернеті 1

E) Интернет телефония

Пайдаланушының саусақ іздері немесе ирис сияқты бірегей физикалық сипаттамаларын қандай аутентификация әдісі қолданады?

A) Құпия Сөз

B) Жетон

C) екі факторлы аутентификация

D) биометриялық аутентификация 1

E) RSA кілті

"Инженерлік әлеуметтік әсер ету" шабуылдары нені білдіреді?

A) физикалық қауіпсіздік шабуылдары

B) зиянды электрондық хаттар арқылы вирустарды енгізу

C) веб-сайттарға шабуылдар

D) зиянды кодты желіге енгізу

E) құпия ақпаратты алу үшін адамдарды манипуляциялау 1

Құпия сөз қауіпсіздігін қамтамасыз ету үшін қандай әрекет жақсы тәжірибе болып табылады?

A) барлық есептік жазбалар үшін бірдей құпия сөзді пайдалану

B) есте сақтауды жеңілдету үшін қысқа парольдерді сақтау

C) әрбір тіркелгі үшін күрделі және бірегей құпия сөздерді пайдалану 1

D) әлеуметтік желілерде парольдерді жариялау

E) әріптестермен мерзімді пароль алмасу

"Сымсыз қауіпсіздік" туралы қандай мәлімдеме дұрыс?

A) қауіпсіз сымсыз желілер парольдерді қажет етпейді

B) сымсыз желіде шифрлаудың болмауы қауіп төндірмейді

C) Wpa3 шифрлау WEP-ге қарағанда сенімді болып саналады 1

D) SSID (желі атауы) әрқашан жасырын болуы керек

E) сымсыз желінің қауіпсіздігі маңызды емес

Компьютерді зиянды бағдарламалардан қорғау үшін қандай шаралар қолдану керек?

A) кездейсоқ бағдарламалық жасақтаманы орнатыңыз

B) Операциялық жүйені және антивирустық бағдарламалық жасақтаманы үнемі жаңартып отыру 1

C) ешқашан деректердің сақтық көшірмесін жасамаңыз

D) барлық пайдаланушылар үшін қонақ режимін қосыңыз

E) бірнеше антивирусты орнатыңыз

Төмендегі шабуылдардың қайсысы жүйенің алдын алуға немесе бұғаттауға емес, оған рұқсатсыз қол жеткізуді анықтауға бағытталған?

A) алдын алу шабуылы

B) детективтік шабуыл 1

C) Қорғаныс шабуылы

D) аутентификацияға шабуыл

E) зерттеу шабуылы

Қандай шабуыл үлкен сұраныстарды жіберу арқылы серверді шамадан тыс жүктеуге бағытталған?

A) Фишинг

B) SQL инъекциясы

C) DDoS шабуылы 1

D)ман-орта шабуыл (MITM)

E) IP мекенжайларын бұғаттау

Веб-қосымшаларға шабуыл жасаудың алдын алатын қауіпсіздік шаралары қандай?

A) MAC мекенжайларын сүзу

B) деректерді шифрлау

C) күшті парольдерді қолдану

D) кіріс деректерін тексеру және бағдарламалық жасақтама компоненттерін жаңарту 1

E) барлық желілік порттарды өшіру

Төмендегі шаралардың қайсысы электрондық пошта серверлеріне шабуылдың алдын алуға көмектеседі?

A) спамды жоюға арналған сүзгілерді орнату 1

B) барлық электрондық жәшіктерді өшіру

C) ашық порттарды пайдалану

D) Барлық пошта жәшіктері үшін бірдей құпия сөзді пайдалану

E) ашық Wi-Fi желілерін пайдалану

"Буфердің толып кетуінен қорғау" дегеніміз не?

A) деректерді шифрлау әдісі

B) шабуылдаушы жадтың бір бөлігін қайта жазуға тырысатын шабуылдың алдын алу әдісі 1

C) аутентификация әдісі

D) виртуалдандыру технологиясы

E) желілік хаттаманың түрі

Бұлтты сақтауды пайдалану кезінде деректердің қауіпсіздігін қамтамасыз ету үшін қандай қадамдар жасау керек?

A) деректерді жалпыға қол жетімді форумдарда жариялау

B) барлық бұлттық қызметтер үшін бірдей құпия сөзді пайдаланыңыз

C) деректерді үнемі резервтеу 1

D) барлық деректерді жергілікті компьютерге жүктеп алыңыз

E) чаттарда парольдерді хабарлау