1-BOB

1-Amaliy test

1. Quyidagilardan qaysi biri passiv razvedka harakati hisoblanadi?

Mahalliy qog‘ozda qidirish

Inson resurslariga qo‘ng‘iroq qilish

nmap -sT buyrugʻi yordamida

O‘rtadagi odam hujumini o‘tkazish

Firibgar qaynoq nuqtasi sozlanmoqda

DES algoritmidan keyin maxfiylikni ta’minlashning asosiy usuli sifatida NIST tomonidan qaysi shifrlash tanlangan?

3DES

Ikki baliq

RC4

AES

Qaysi vosita 802.3 muhitiga odam-in-the-middle hujumini o'tkazishga qodir?

Ettercap

Qobil va Hobil

Wireshark

nishoncha bilan oʻchirish

An'anaviy xavfsizlik devori va IPS o'rtasidagi farq nima?

Xavfsizlik devorlari jurnallarni yaratmaydi.

IPS paketlarni tashlab bo'lmaydi.

IPS qoidalarga amal qilmaydi.

IPS paketlarni ajratishi mumkin.

Nega maqsadli tarmoqni sekin-asta skanerlash muhim?

IDSni ogohlantirishga yo'l qo'ymaslik uchun

Tarmoqni sekin skanerlash kerak emas.

Xavfsizlik devoridan qochish uchun

Xizmatlar boshlanmagan bo'lishi mumkin, shuning uchun asta-sekin boshlash kech boshlangan xizmatlarni qo'lga olishingizni ta'minlaydi.

Siz kompaniyangizning IT bo'limida katta menejerisiz. Ijtimoiy muhandislik hujumlarining oldini olishning eng tejamkor usuli nima?

HIDSni o'rnatish.

Barcha yamalar dolzarb ekanligiga ishonch hosil qiling.

Barcha elektron pochta harakatlarini kuzatib boring va nazorat qiling.

Foydalanuvchilarni anglash bo'yicha treninglarni amalga oshiring.

Axloqiy xakerlik doirasining qaysi bosqichida jurnal ma'lumotlarini o'zgartirasiz yoki o'chirib tashlaysiz?

Skanerlash va ro'yxatlash

Kirish imkoniyati

Tan olish

Treklarni qoplash

Hacker maqsadli ish stantsiyasida quyidagilarni amalga oshirmoqda:

nmap -sT 192.33.10.5. Tajovuzkor qaysi bosqichda?

Treklarni qoplash

Ro'yxatga olish

Skanerlash va ro'yxatlash

Kirish imkoniyati

Qaysi shifrlash algoritmi nosimmetrik oqim shifri?

AES

ECC

RC4

PGP

Penetratsiya testini o'tkazishda eng muhim jihat nima?

Rasmiy yozma kelishuv olish

Barcha harakatlar va faoliyatni hujjatlashtirish

Jiddiy tahdidlarni zudlik bilan bartaraf etish

Axborotni ta'minlash guruhi bilan to'g'ri aloqani ta'minlash

Siz ulkan texnologik kompaniya uchun CISO. Siz 2017 yilda joriy etiladigan yangi mobil qurilmalaringiz uchun shifrlash shifrini amalga oshirish bilan shug'ullanasiz. Qaysi shifrlash standartini tanlaysiz?

RC4

MD5

ECC

Skipjack

SYN skaneri nimani amalga oshiradi?

Bu to'liq TCP ulanishini o'rnatadi.

Bu faqat "yarim ochiq" aloqani o'rnatadi.

Bu maqsad bilan ACK aloqasini ochadi.

Maqsadli tizimdagi barcha yopiq portlarni aniqlaydi.

ARP so'rovining asosiy zaifligi nima?

LANdagi barcha xostlarga manzil so'rovini yuboradi.

Manzil foydalanuvchi va maxfiy soʻz bilan ochiq matn koʻrinishida qaytariladi.

Manzil so'rovi DoS-ga olib kelishi mumkin.

Manzil so'rovi tajovuzkorning MAC-manzili bilan buzilishi mumkin.

Siz ommabop ijtimoiy veb-sayt uchun CISO. Yaqinda veb-serverlaringiz SSL Heart Bleed nol kunlik ekspluatatsiyasi bilan buzilganligini bilib oldingiz. Qarshi himoya qilish uchun sizning eng ehtimoliy birinchi harakatlaringiz nima bo'ladi?

Barcha tizimlarni yamalang.

Yangi kriptografik kalitlarni yaratish.

Internetga qaraydigan veb-xizmatlar oʻchirib qoʻyildi.

Nozik ma'lumotlarga kirishni cheklash.

Hozirda muvaffaqiyatli o'rtadagi odam-in-the-middle hujumini amalga oshirayotgan hujumchi qaysi bosqichda?

Kirish imkoniyati

Kirishni saqlab qolish

Tan olish

Treklarni qoplash

Qaysi ekspluatatsiya usuli dushmanga URL ichidagi SQL so'rovlarini sinab ko'rishga imkon beradi?

SQL-in'ektsiya

XSS

Nayzali fishing

Rails qarshi usuli bo'yicha Ruby

Microsoft Windows 7 OS uchun standart TTL qiymatlari nima?

64

128

255

256

SQL in'ektsiyasi zaifliklarini baholash va sinovdan o'tkazish uchun qaysi kirish qiymatidan foydalanasiz?

SQL testi

ma'mur va parol

|| yoki |!

1'or'1'='1

Xavfsizlik haqida gap ketganda, Telnet bilan SSH-dan foydalanishning salbiy tomoni nimada?

SSH trafik va hisob ma'lumotlarini shifrlaydi.

Koʻrmassan. Albatta, sen oʻshaning nima qilishini koʻrmassan.

Ma'lumotlar aniq ko'rinishda yuboriladi.

Qanday kalitlardan foydalanayotganingizni bilmaysiz.

O'lim pingi birinchi marta qaysi yilda paydo bo'ldi?

1992

1989

1990

1996

Quyidagi viruslardan qaysi biri eng yuqumli bo'lgan?

Melisa virusi

Men sizni virusni sevaman

Blue Cross virus punter

Stuxnet

Siz yordam xizmati guruhining bir qismisiz. Siz foydalanuvchingizdan kompyuteringiz vaqti-vaqti bilan sekinlashishi haqida chipta olasiz. Foydalanuvchi shuningdek, vaqti-vaqti bilan hujjatlar yo'qolib ketganini yoki asl joyidan boshqasiga ko'chirilganligini ta'kidlaydi. Foydalanuvchi kompyuteriga masofaviy ish stolini tekshirib koʻring. Yangi jarayonlar boshlanganini ko'rish uchun eng ehtimoliy joy qaerda?

Vazifalar boshqaruvchisidagi "Jarayonlar" paneli

C:\temp

Vazifalar boshqaruvchisidagi Loglar paneli

C:\Windows\System32\User

Tarmoq muhandisi sifatida siz simsiz aloqa orqali ikkita korporativ ob'ektni bog'lash vazifasini oldingiz. Ushbu ob'ektlar bir-biridan 20 mildan ortiq masofada joylashgan, har bir joyda 400 dan ortiq xodimlarni o'z ichiga oladi va 20,000 AQSh dollari byudjetga ega. Har bir sayt bitta rejimli tolali ulanishga ega. Bo'shliqni ko'paytirish uchun qaysi antennadan foydalanasiz?

Ko'p reymli tolali tolali

Juda kichik diyaframli terminal (VSAT)

Omni yo'nalish antennasi

Yo'nalishli antenna

Tekshirish summasi nimani anglatadi?

Ma'lumotlar manziliga yetib kelganini

Uch tomonlama TCP / IP qo'l siqish tugagan

Tranzit yoki dam olish paytida ma'lumotlarda o'zgarishlar bo'lganligi

Ma'lumotlar xotirasidan keyin hajmi

Quyidagilardan qaysi biri RSAning ro'yxatdan o'tgan asosiy kuchli tomonlaridan biri?

1,024 bit

256 bit

128 bit

512 bit

E-pochtani rad etishni ta'minlash uchun qaysi algoritmni amalga oshirishni tanlaysiz?

AES

DSA

3DES

Skipjack

Quyidagilardan qaysi biri poyga holatini tasvirlaydi?

Bir vaqtning o'zida ikkita shart ro'y beradi va foydalanuvchining yuqori ruxsatlari bilan o'zboshimchalik bilan buyruqlar bajarilishi mumkin bo'lsa, keyinchalik dushman tomonidan ishlatilishi mumkin

Bu erda ikkita shart bir-birini bekor qiladi va foydalanuvchi imtiyozlari darajasiga qarab o'zboshimchalik bilan buyruqlar ishlatilishi mumkin

Bu yerda bitta foydalanuvchi hisobi uchun ikkita shart bajariladi

Bu yerda ikkita shart yuqori foydalanuvchi imtiyozlari bilan bir vaqtda bajariladi

Sizning oxirgi mijozlaringiz tashqi tarmoqdagi biron bir veb-saytga kira olmasliklarini xabar qilishadi. Tarmoq ma'muri sifatida siz ba'zi haqiqatlarni aniqlashga qaror qilasiz. Tekshiruvingiz natijasida siz ularning IP-manzilidan foydalanib, LANdan tashqarida tashqi veb-saytlarga ping qilish imkoniyatiga ega ekanligingizni aniqlaysiz. Domen nomlari o'lchamlari bilan veb-saytlarga ping qilish ishlamaydi. Muammoga nima sabab bo'lishi mumkin?

Xavfsizlik devori DNS piksellar sonini bloklamoqda.

DNS server to'g'ri ishlamaydi.

Tashqi veb-saytlar javob bermayapti.

HTTP GET so'rovi xavfsizlik devoridan chiqib ketishdan tashlanmoqda.

Siz mahalliy shahar uchun xavfsizlik ma'muriyatisiz. Siz yangi IPS o'rnatdingiz. Uni ulash va ba'zi asosiy IPS qoidalarini qo'llashdan tashqari, boshqa hech qanday konfiguratsiya amalga oshirilmagan. Ertasi kuni ertalab kelasiz va jurnallarda IPS tomonidan yaratilgan juda ko'p faoliyat borligini aniqlaysiz, shuning uchun ko'rish juda ko'p vaqt talab qiladi. IPSdan jurnallarning katta oqimiga nima sabab bo'lishi mumkin?

Kesish darajasi belgilandi.

Tarmoqda DoS hujumi bo'lgan.

LAN kommutatsiya aylanishini boshdan kechirdi.

Hech qanday baza o'rnatilmagan.

Qaysi usul mijoz tomonidagi hujum deb hisoblanadi?

Saytlararo skript (XSS)

O'rtadagi odam hujumi

Sug'orish teshigi hujumi

Xizmatdan bosh tortish (DoS)

Penetratsion sinovchi sifatida faqat siz va kompaniyaning bir nechta tanlangan shaxslari sinovdan o'tadigan maqsadli tarmoqni bilib olasiz. Siz shuningdek, kompaniyaning nomi va joylashuvidan tashqari maqsadingiz haqida nol ma'lumotga egasiz. Bu qanday baholash turi deb ataladi?

Kulrang qutini sinash

Oq qutini sinash

Qora qutini sinash

Blue box sinov

Hujumchi sifatida siz maqsadingizni topdingiz. Keyingi ikki hafta davomida xodimlarning muassasaga kirishini va tashqariga chiqishini kuzatish va kuzatish bilan shug'ullanasiz. Shuningdek, old stol etkazib berilgan katta paketlarni, shuningdek, kirish nishonlari bo'lmagan odamlarni qanday ishlashini kuzatasiz. Nihoyat siz o'tkazilayotganini ko'rgan xavfsizlik patrullarining mustahkam jadvalini tuzasiz. Siz nima qilyapsiz?

Moʻljalning kattaligi

Kirish imkoniyati

Kirishni saqlab qolish

Tan olish

Qaysi skanerlash vositasi hacker uchun aniq natijalarni beradi?

NCAT

nishoncha bilan oʻchirish

Ping

Nslookup

Nima uchun tajovuzkor Ncat yordamida ochiq TCP ulanish tekshiruvini o'tkazishi

kerak?

Tajovuzkor tizimga hujum qilishni xohlamaydi.

Tajovuzkor nmap funktsiyasidan foydalangan holda xato qildi.

Tajovuzkor tarmoq xizmatlariga ulanishga harakat qilmoqda.

Tajovuzkor ulanish uchun qanday portlar ochiq ekanligini ko'rishga harakat qilmoqda.

Nima uchun tajovuzkor optik tolali liniyaga kirishdan qochishni xohlaydi?

Tolali liniyaga kirish juda ko'p pul sarflanadi.

Agar noto'g'ri bajarilsa, u butun ulanish signalining pasayishiga olib kelishi mumkin, shuning uchun maqsadli tashkilotning istalmagan e'tiborini jalb qiladi.

Tarmoq trafigi sezilarli darajada sekinlashadi.

Liniyaga tegish IPS / IDS-ni ogohlantirishi mumkin.

Siz maqsadingizning veb-serveriga muvaffaqiyatli kirgan tajovuzkorsiz. Siz maqsadli tashkilotning veb-saytida veb-saytni buzdingiz va ma'muriy imtiyozlar bilan o'zingizning hisob ma'lumotlaringizni yaratishingiz mumkin. Ma'lumotlarni eksfiltratsiyadan oldin keyingi harakat nima?

Siz yaratgan yangi foydalanuvchi hisobiga kiring.

Orqaga qayting va jurnallarni o'chirib tashlang yoki tahrirlang.

Seansdan chiqishingizga ishonch hosil qiling.

Boshqa sessiyaga ko'chib o'tganingizga ishonch hosil qiling va tizimdan chiqing.

Kerberosdan foydalanishning asosiy kamchiligi nima?

Nosimmetrik kalitlar xavfsiz bo'lmasa, buzilishi mumkin.

Kerberos zaif kriptografiyadan foydalanadi va kalitlarni osongina buzish mumkin.

Kerberos assimetrik kriptografiyadan foydalanadi va uni osongina ishlatish mumkin.

Dushman tizimga yoki xizmatga kirish uchun chipta berish chiptasini qayta ijro etishi mumkin.

Windows tizimidagi maxfiy soʻz fayli qayerda joylashgan?

C:\Windows\temp

C:\Win\system\config

C: \ Windows \ accounts \ config

C:\Windows\system32\config

Agar dushman XMAS tekshiruvini o'tkazsa, yopiq portlarda qanday javob oladi?

RST

RST/ACK

Javob yoʻq

FIN/ACK

Nima uchun dushman o'z yukini maqsadli qurbonga yuborishdan oldin kodlashi kerak?

Foydali yukni kodlash qo'shimcha foyda bermaydi.

Foydali yukni kodlash orqali dushman aslida foydali yukni shifrlaydi.

Kodlangan foydali yuk xavfsizlik devorini chetlab o'tishi mumkin, chunki foydali yuk bilan bog'liq port yo'q.

Yukni kodlash IPS / IDS aniqlashni chetlab o'tishi mumkin, chunki u imzoni o'zgartiradi.

Qaysi maxfiy soʻz xavfsizroq?

!9Apple

pass123!!

P@$$w 0rD

keepyourpasswordsecuretoyourself

Quyida keltirilganlardan qaysi biri DNS zaharlanishini yaxshiroq ta'riflaydi?

Dushman qurbonlarning MAC manzilini o'zlari bilan almashtiradi va almashtiradi.

Dushman ularning zararli IP-manzilini jabrlanuvchining domen nomi uchun IP-manzili bilan almashtiradi.

Dushman qonuniy domen nomini zararli domen nomi bilan almashtiradi.

Dushman domen nomiga moslangan qonuniy IP-manzilni zararli IP-manzil bilan almashtiradi.

Quyidagilardan qaysi biri dushmanga autentifikatsiya qilish uchun sertifikatlarni qalbakilashtirishga imkon beradi?

Wireshark

Ettercap

Qobil va Hobil

NCAT

WEPda qaysi shifrlash standarti qo'llaniladi?

AES

RC5

MD5

RC4

Siz ofisingizning ichida o'tiryapsiz va avtoturargohda noutbukga ulangan baland antennaga o'xshash narsa bilan g'alati odamni ko'rasiz. Begona odam nima qilishi mumkin?

O'zlarining shaxsiy elektron qurilmalarini qo'pol ravishda kuchaytirish

Urush haydash

Jangchi

Bluesnarfing

Tarmoq ma'muri sifatida siz eshittirish manziliga ping yuboradigan tanish IP- manzilni ko'rasiz. Nima sodir bo'layotganiga ishonasiz?

Smurf hujumi

DNS bilan zaharlanish

O'rtadagi odam hujumi

Gatewayni yuqtiruvchi troyan virusi

Qaysi biri xizmatdan bosh tortishni (DoS) yaxshiroq ta'riflaydi?

Jabrlanuvchining kompyuterida virus yuqtirilgan.

Noto'g'ri tuzilgan kalit kommutatsiya aylanmasida.

Dushman sertifikatni soxtalashtirmoqda.

Dushman veb-serverda iloji boricha ko'proq "yarim ochiq" ulanishlarni ochib, maqsadli tizimning barcha mavjud xotirasini iste'mol qilmoqda.

Windows SAM faylida, qaysi atributlar dushmanga berilgan hisob administrator hisobi ekanligini ko'rsatadi?

500

1001

ADM

ADMIN\_500

Shimoliy va Janubiy Amerika uchun qaysi mintaqaviy Internet registri javobgar?

PISHGAN

AMERNIC

Laknik

ARIN

Quyidagi harakatlardan qaysi biri maqsadni skanerlashda so'nggi qadamdir?

Zaifliklarni skanerlang.

Jonli tizimlarni aniqlang.

Ochiq portlarni kashf eting.

Operatsion tizim va serverlarni aniqlang.

Quyidagilardan qaysi biri ICMP Type 8 kodini eng yaxshi ta'riflaydi?

Uskuna filtrlanmoqda

Tarmoq yoʻnalishi notoʻgʻri yoki mavjud emas

Echo soʻrovi

Moʻljallangan manzilga etib boʻlmaydi

Quyidagi parametrlardan qaysi biri yaxshi tanilgan portlarni koʻrsatadi?

0 uchun 1023

0 uchun 255

1024 uchun 49151

1 dan 128 gacha

Urush terish nima?

Modemda DoS-ni olib borayotgan dushman

Qaysi modemlar ochiq ekanligini koʻrish uchun dushman terilmoqda

Modemni yovuz egizak sifatida ishlatadigan dushman

Yopiq modemlarni tekshiruvchi dushman

Nmap buyrug'i uchun quyidagi kalitlardan qaysi biri operatsion tizimni izlaydi?

-sO

-sFRU

-A

-sX

Windows-dagi buyruq satri interfeysidan foydalanib, domen ichidagi barcha tizimlarni ko'rsatish uchun dushman qanday buyruqdan foydalanadi?

netstat -R /domen

Aniq koʻrinish /<domain\_name>:d omain

aniq ko'rinish /domen:<domain\_name>

netstat /domen:<domain\_name>

Siz aeroport terminalida yo'lovchisiz. Siz terminalga qaraysiz va planshetidan foydalanayotgan yosh ayolning yelkasiga qaragan odamni ko'rasiz. U nima qilyapti deb o'ylaysiz?

Urush haydash

Yelkada bemaqsad qilish

Urush yelkasi

Yelka kriko

Siz maqsadli saytda SQL in'ektsiyasi zaifliklarini baholashni muvaffaqiyatli o'tkazgan tajovuzkorsiz. SQL in'ektsiyasi qismi sifatida o'zingizning zararli ma'lumotlar bazangiz bilan maqsadli ma'lumotlar bazasini qo'shish uchun qaysi kalit so'zni ishlatasiz?

ITTIFOQ

QO'SHISH

TANLASH

QOʻSHILISH

Qaysi parametr xotiradagi ma'lumotlarning bir qismiga kodni in'ektsiya qilish kontseptsiyasini tasvirlaydi, bu esa abritar buyruqlarni bajarishga imkon beradi?

Bufer toʻldirish

Halokat

Xotiradan toʻlib-toshma

Ma'lumotlar toshqini

Quyidagi usullardan qaysi biri aloqani tashabbuskor qilish va o'rnatish orqali tashqi tarmoq va xususiy tarmoq o'rtasida vositachi vazifasini bajaradi?

Proksi-server

Xavfsizlik devori

yo'naltirgich

Oʻzgartirish

Tajovuzkor sifatida siz o'chirib qo'yilishi kerak bo'lgan xizmatdan foydalangan holda maqsadingizdan muvaffaqiyatli foydalandingiz. Xizmatda siz qulaylik bilan foydalanishingiz mumkin bo'lgan zaifliklar mavjud edi. Bu erda nima bo'lishi mumkin?

Administrator to'g'ri yamalarni qo'llamadi.

Veb-server noto'g'ri sozlangan.

Siz asal bilan shug'ullanyapsiz.

Xavfsizlik devori toʻgʻri moslanmagan.

Linux tizimida kirgan oxirgi foydalanuvchining faoliyati bilan bog'liq bo'lgan log fayli qani?

/var/log/user\_log

/var/log/xabarlar

/war/people/lustlog

/var/log/last\_user

SSH qaysi standart portdan foydalanadi?

Port 22

Port 21

Port 443

Port 25

Pentester sifatida siz mijozingiz uchun tizimlar guruhida baholash uchun yollanasiz. Sizga muhim aktivlar ro'yxati, domen kontrolleri ro'yxati va virtual shareddlar ro'yxati taqdim etiladi. Boshqa hech narsa taqdim etilmadi. Siz qanday turdagi sinovlarni o'tkazyapsiz?

Oq shlyapa sinovlari

Kulrang shlyapa sinovi

Kulrang qutini sinash

Qizil shlyapa sinovlari

Quyidagilardan qaysi biri olov yurish atamasi nimani anglatishini eng yaxshi tasvirlaydi?

TTL qiymatini xavfsizlik devori 1 tomonidan kamaytirish, port ochilishini ko'rsatadi.

Ping toshqini bilan xavfsizlik devorida xizmatdan bosh tortishga sabab bo'ladi

Xavfsizlik devorida ping tekshiruvini o'tkazish

TTLni sozlash qaysi serverlar va boshqa hostlarning mavjudligini aniqlash uchun yo'riqnoma o'tkazdi

3-qatlamni skanerlash va ro'yxatga olishni amalga oshirish uchun qaysi vositadan foydalanish mumkin?

Qobil va Hobil

Yahyo ripper

Ping-eater

nishoncha bilan oʻchirish

IP protokoli bilan qanday port raqami yoki raqamlar bog'liq?

0 uchun 65535

Portlar yoʻq

53

80

Qaysi ikkita protokol aloqasiz?

IP va TCP

IP va FTP

IP va UDP

TCP va UDP

Tizimni ruxsat bilan so'roq qiladigan shaxsning roli qanday?

Oq shlyapa

Kulrang shlyapa

Qora shlyapa

Qizil shlyapa

Patch boshqaruvi nima?

Mavjud bo'lganda yamalarni tarqatish

Yamalarni ishlab chiqarish muhitiga joylashtirilishidan oldin sinov muhitida sinovdan o'tkazish

Oy oxirida yamalarni tarqatish

Sizning tarmog'ingizda hozirda qanday zaifliklar mavjudligini aniqlash va tahdidni bartaraf etish uchun darhol yamalarni joylashtirish

FTP OSI modelining qaysi qatlamida joylashgan?

Seans

Dastur

Tarmoq

Transport

Qaysi ekspluatatsiya yurak qon ketishi xuruji bilan bog'liq?

Bufer toʻldirish

O'rtadagi odam

Fraggle-hujum

Smurf hujumi

Nmap'dagi qaysi kalit XMAS skanerini chaqiradi?

-sX

-sS

-xS

-sT

Quyidagilardan qaysi biri barmoq izi skanerini yaxshiroq ta'riflaydi?

Zaifliklarni qidirish

Nmap uchun -sX kalitidan foydalanish

Skanerdan maʼlumot bazasiga mos xususiyatlar

Yong'in bilan qanday portlar ochilganligini tekshiring

Qaysi variant veb-ilovalarni maqsad qilib olgan mijoz tomonidagi hujumni tasvirlaydi?

SQL-in'ektsiya

O'zaro faoliyat saytlarida zararli dasturlarni yuborish

Saytlararo skript yaratish

SQL sayt skripti

DNS orqali qaysi portdan foydalaniladi?

80

8080

53

25

Linux-da, qaysi fayl to'liq ism, telefon kabi foydalanuvchi ma'lumotlarini ko'rishga imkon beradi

Raqam va ofis haqida maʼlumot?

soya fayli

passwd fayli

foydalanuvchima'lumot fayli

foydalanuvchiaccount fayli

Paket analizatorida FIN bayrog'i qaerda o'rnatilganligini qaerdan ko'rishingiz mumkin?

TCP – sarlavha

TCP - PaketStencils

UDP – Bayroqlar

Bayroqlar

DoS hujumini yaratish uchun fraggle hujumi qaysi turdagi paketdan foydalanadi?

TCP

IP

ICMP

UDP

NOP (ishlamaydigan protsedura) ni chaqirish uchun qaysi ko'rsatma qiymati ishlatiladi?

0x99

0x91

0xGH

0x90

Bannerlarni olish uchun qanday protokoldan foydalanasiz?

FTP

Qo'shimcha yordamchi dastur

DNS

Telnet

IPv6 ichida quyidagi funktsiyalardan qaysi biri endi ishlamaydi?

ko'p manzilli

Har qanday cast

Unicast

Translyatsiya qilish

Muayyan konfiguratsiyalar va hujjatning bosqichma-bosqich ko'rsatmalari bilan serverni o'rnatganingizda nima yaratasiz?

Baza chizig'i

Jarayon

Texnik maslahat

Koʻrsatma

Dastur ikkita portdan foydalanadi?

Telnet

ICMP

HTTPS

FTP

Quyidagi protokollardan qaysi biri vaqti-vaqti bilan mijoz va serverni o'zaro autentifikatsiya qilish uchun bir-birlariga qarshi chiqishga majbur qiladi?

CHAP

OVOZ CHIQARUVCHI

PAP

PPE

Quyidagilardan qaysi biri hisobni boshqarishning hayot aylanishiga kiradi?

Hisob qaydnomasini yaratish

Murojaat rad etildi

Foydalanuvchi autentifikatsiya qilish

Yuqoridagilarning hech biri

Quyidagi harakatlardan qaysi biri nozik ma'lumotni qidirib axlat konteynerini qidirib yurgan odamning harakatini tasvirlaydi?

Axlatdan sakrash

Dumpster partiyasi

Axlat sho'ng'ishi

Dumpster sho'ng'ishi

Veb-serverga ulanish uchun qanday ikkita umumiy port ishlatiladi?

80 va 25

80 va 8080

443 va 53

20 va 21

Mahalliy saqlash va uchinchi tomon bulutli saqlash xavflarini ko'rib chiqayotganda, qaysi bayonot eng to'g'ri?

Bulutli saqlash yanada xavfsizroq, chunki tijorat sotuvchisi xavfsizlik bo'yicha mutaxassislarni o'qitdi.

Saqlash mahalliy bo'lsa, siz saqlash xizmatlari uchun javobgar va javobgar bo'lasiz.

Siz bulut provayderini zarar uchun sudga berishingiz mumkin.

Bulutda an'anaviy mahalliy saqlash infratuzilmasiga qaraganda ko'proq xavfsizlik qatlamlari mavjud.

Port raqami bilan birlashtirilgan IP-manzilni nima deb ataysiz?

TCP/IP

Ulanishga asoslangan protokol

TCP/IP soketi

Soket

Tasniflash yorlig'i quyidagilardan qaysi biri bilan bog'liq?

Mavzu

Fayl

Obʼekt

Jild

Quyidagi vositalardan qaysi biri rasmiy ravishda CA tomonidan imzolanmagan sertifikatlarni yaratishga imkon beradi?

Qobil va Hobil

nishoncha bilan oʻchirish

Ettercap

Qorong'i eter

RAID moslamasining qaysi biri ishlamaydi yoki endi ishlatilmaydi?

RAID-1

RAID-3

RAID-5

RAID-2

Ushbu protokol autentifikatsiya qilish maqsadida ishlatiladi; U aniq matnli foydalanuvchi nomlari va parollarni shifrlash shakllari yoki qiyinchilik vositasisiz yuboradi. Bu tasdiqlash protokoli nima?

CHAP

OVOZ CHIQARUVCHI

PAP

MSCHAP

"Biror narsa" qaysi autentifikatsiya omili turining bir qismi hisoblanadi?

1-tur

3-tur

2-tur

Ko'p faktorli autentifikatsiya qilish

Ikki yoki undan ortiq autentifikatsiya usuli qo'llanilsa, u chaqiriladi?

ko'p bosqichli autentifikatsiya faktori

Ko'p faktorli autentifikatsiya qilish

Ko'p sonli faktorli autentifikatsiya qilish

Multiauthentication faktori

Quyidagilardan qaysi biri bilan bog'liq bo'lmagan kalit?

MD5

AES

Skipjack

PGP

Qaysi operatsion tizim tuzilishi tarmoq mudofaasi uchun vositalar to'plamini taqdim etadi?

Kali Linux

Windows Server 2012 R2

FreeBSD

Xavfsizlik piyozi

Qaysi operatsion tizim tuzilishi tarmoq hujumi (maqsadingizga hujum qilish) maqsadlar uchun vositalar to'plamini taqdim etadi?

Kali Linux

Windows Server 2012 R2

FreeBSD

Xavfsizlik piyozi

Antivirus dasturining asosiy kamchiligi nimada?

Bu juda sekin bo'lishi mumkin.

U virusning eng so'nggi ta'riflariga ega bo'lishi kerak.

Ko'plab xost resurslarini talab qilishi mumkin.

Buni boshqarish uchun ko'p harakat talab etiladi.

Tarmoqni himoya qilish uchun IDS / IPS echimini amalga oshirish uchun quyidagi dasturlardan qaysi birini ishlatasiz?

Kali Linux

Windows Vista

NCAT

Mirkat

UDP paketi uchun maksimal bayt hajmi qancha?

65,535

65,507

1,500

65,527

Hujumchi sifatida, razvedka bosqichida maqsadingizning oyoq izini shakllantirish uchun birinchi bo'lib quyidagi manbalardan qaysi birini boshlaysiz?

–sO kaliti bilan nmap

Kali Linux

Gazetadagi yordam qidirilmoqda bo'limi

Vakolatli foydalanuvchi sifatida yordam xizmatiga qo'ng'iroq qilish

FIN bayrog'i o'rnatilgan paketni yuborishda, port ochiq bo'lsa, maqsad nima bilan javob beradi?

RST qaytariladi.

Javob qaytarilmaydi.

RST / ACK qaytariladi.

SYN/ACK qaytariladi.

Kommutatsiyada MAC toshqinini o'tkazishning natijasi qanday?

Kalit javob bermaydi.

Bu DoSni yaratadi.

Kalit xuddi markaziy kabi ishlaydi.

Kalit odatdagidek ishlashda davom etadi.

Wireshark-da ma'lum bir IP-manzilni qidirish uchun quyidagilardan qaysi biri to'g'ri yo'l?

ip.addr = 192.168.1.100

ip == 192.168.1.100

ip = 192.168.1.199

ip.addr == 192.168.1.100

Quyidagilardan qaysi biri 2-turdagi kirishni boshqarish usuli?

Barmoq izi

PIN-kod

GPS manzili

Token kirish kartasi

Qaysi turdagi hujum quyidagi vaziyatni eng yaxshi belgilaydi? E-pochtada "Kruizingiz bilan tabriklaymiz!" mavzusi bilan havola mavjud. E-pochta o'quvchiga kruizni talab qilish uchun giperhavolani bosishni buyuradi. Havolani bosganda, o'quvchiga onlayn shaklda ism, ijtimoiy sug'urta raqami va tug'ilgan sana kabi bir qator savollar beriladi.

E-pochta orqali phishing

Nayzali fishing

Ijtimoiy injiniring

Shaxsni o'g'irlash

Maqsadli tizimda DDoS-ni bajarish uchun ishlatiladigan zombi kompyuterlar tarmog'i chaqiriladimi?

Botnet

Balchiq ovlash

Ijtimoiy injiniring

To'g'rilar doir

Shifrlangan qulflar, mantraplar va bollardlar nima deb hisoblanadi?

jismoniy nazorat qilish

Texnik nazorat qilish

Atrof-muhitni loyihalash orqali jinoyatchilikning oldini olish

Jismoniy to'siqlar

Quyidagilardan qaysi biri X.509 standartini tavsiflaydi?

U LDAP tuzilishini belgilaydi.

Bu nosimmetrik shifrlash algoritmi.

Xavfsizlik uchun qum qutisi usulidan foydalanadi.

Unda raqamli sertifikat yaratish standarti tasvirlangan.

Quyidagilardan qaysi biri steganografiyani eng yaxshi ta'riflaydi?

Nosimmetrik shifrlash algoritmiName

Sizning shaxsiy kalitingizdan foydalanishga ruxsat berish

Rasmdagi ma'lumotni yashirish yoki uni audio formatda yashirish

Almashtirish va almashtirish yordamida maʼlumotlarni shifrlash

Ko'p hollarda quyidagi tasniflardan qaysi biri asal bo'ladi?

Jalb qilish

Tuzoq qilish

Ijtimoiy injiniring

Asal

802.11a kirish nuqtasi qaysi tarmoqli kengligida ishlaydi?

54 Mbit / s

1 Gb / s

5 GHz

2.4 GHz

CEH imtihonining boshqaruv kengashi nima?

(ISC)2

Evropa Kengashi

CompTIA

Microsoft

DHCP qaysi transport qatlami protokoli bilan ishlaydi?

IP

TCP

ICMP

UDP

Diagrammaga ko'ra, IANA ID nima?

292

94089

AQSh

4083493300

Quyidagi skrinshotga ko'ra, Terminal qanday jarayonni identifikatsiyalashda ishlaydi?

1

708

243

1186

Quyidagi rasmda ko'rsatilganidek, qanday hujum turi amalga oshirilmoqda?

Zarbalar

DDoS

To'g'rilar doir

Bot hujumi

Bu erda ko'rsatilgan uch tomonlama qo'l siqishni yakunlash uchun nima etishmayapti?

ACK/SYN

ACK

TCP/IP

SYN/ACK

Quyidagi skrinshotda qaysi jarayon 386 MB xotira oladi

kompyuter?

Firefox

kernel\_task

Finder

Oyna serveri

Quyidagi rasmda qanday hujum turi ko'rsatilgan?

O'rtadagi odam

To'g'rilar doir

DDoS

Nayzali fishing

Qaysi skanerda eng ko'p portlar skanerlangan?

Ping

SYN yashirincha

SIND

DUP

Quyidagi ekran tasvirida ko'rsatilganidek, foydalanuvchi parolini xash uchun qanday algoritm ishlatilgan?

SHA-512

Kerberos

AES

SHA-256

Qaysi fayl yoki dasturda 644 bilan ruxsatnoma o'rnatilgan?

AQSh dollari

aniq

Hajmi

Installer.failurerequests

Wireshark pcap faylida berilgan ma'lumotlardan, veb-serverga ulanadigan manba qaysi operatsion tizim?

OS X

Microsoft

Linux

RaspbiyaName

2-BOB

Amaliy test 2

1.Quyidagilardan qaysi biri ma'muriy nazorat hisoblanadi?

biometrik qurilma

Mantrap

Xavfsizlik siyosati

Kirish boshqaruvi ro'yxati

C sinfidagi tarmoqda, tarmoq ma'murlari subnet niqobi /27-dan foydalanayotgan bo'lsalar, qancha tarmoqni rejalashtirishlari mumkin?

8

32

16

1

Telnet uchun standart port raqami nima?

21

23

53

443

Wiley ASCII matnini oʻn oltiburchak formatga aylantirish.

57 69 6c 65 79

63 f3 1i 79 51 ab

11 Fe A5 6C 81 3h

87 105 105 101 121 132

Qaysi algoritm yaxlitlik yoki maxfiylikni ta'minlamaydi?

DSA

AES

RC4

PGP

Quyidagi qisqartmalardan qaysi biri Shimoliy Amerika IP makonini boshqaruvchi institutni anglatadi?

ICANN

PIR-TAHRIR

ARIN

APNIC

ARP OSI modelining qaysi qatlamida joylashgan?

Namoyish qatlami

Dastur qatlami

Jismoniy qatlam

Tarmoq qatlami

Tepaga o'ralgan ustara simli 8 fut balandlikdagi devor qanday o'lchov hisoblanadi?

To'xtatuvchi chora

Profilaktika chorasi

Tuzatish chorasi

Sanoat o'lchovi

Quyidagi standartlardan qaysi biri WPA2 kabi simsiz xavfsizlikni ta'riflash va amalga oshirishga havola qiladi?

802.1x

802.11ac

802.11b / g / n

802.11i

Linuxda qaysi ruxsat qiymati o'qish va bajarishga imkon beradi?

A. 5

B. 7

C. 4

D. 1

Quyidagilardan qaysi biri DHCP jarayonini to'g'ri tavsiflaydi?

Kashf qilish, taklif qilish, so'rash, tasdiqlash

So'rov, kashf qilish, taklif qilish, tasdiqlash

Taklif qilish, tan olish, so'rash, kashf qilish

Tan olish, taklif qilish, so'rash, kashf qilish

AES ichida bitlarda qanday kalit o'lchamlari ishlatiladi?

64 va 128

128, 192 va 256

128 va 256

256

Quyidagilardan qaysi biri mantiqiy bombani tasvirlaydi?

E-pochta ilovasi orqali yetkazib berilgan va ishga tushirilgan zararli kod

Yadro operatsion tizimiga oʻrnatilgan zararkunandalik dasturlar

Vaqt, sana yoki hatto ma'lum bir klaviatura bosilishi kabi muayyan shartlar bajarilmaguncha harakatsiz yotadigan zararli kod va uning foydali yukini bajaradi

O'zboshimchalik bilan kodni bajarish mumkin bo'lgan CPU registrlarini buzadigan zararli dastur

Botnetni boshqarish uchun quyidagi dasturlardan qaysi biri asosan ishlatiladi?

Qo'shimcha yordamchi dastur

FTP

El.pochta

veb-server

Siz moliyaviy firmangiz uchun jamoa rahbarisiz. Siz kun oxirida barcha hamkasblar stolini tozalash, axlatni bo'shatish, nozik hujjatlarni parchalash va boshqa muhim hujjatlarni tegishli konteynerlarda saqlashlari kerak bo'lgan siyosatni o'rnatasiz. Bunday siyosatning umumiy nomi nima?

Toza xona siyosati

Toza stol siyosati

Sanitariya siyosati

Siyosatni yigʻish

Siz o'z ichki tarmog'iga ega bo'lgan tashkilotda ishlaysiz. Ushbu ichki tarmoq geografik jihatdan ajratilgan kompaniyalarning joylariga ham kengaytirildi. Qaerda

bo'lishidan qat'iy nazar, siz hali ham ichki tarmog'ingizga kirishingiz mumkin; ammo, xavfsizlik masalalari tufayli siz Internetdan foydalanishingiz taqiqlangan. Qanday turdagi

Tarmoq sharoitlarini boshdan kechiryapsizmi?

VPN

Internet

ekstranet

Intranet

OSI modelida elektron darajadagi shlyuzlar qaysi qatlamda ishlaydi?

Seansning qatlami

Maʼlumot bogʻlash qatlamiName

Tarmoq qatlami

Yangi qatlam

Qaysi zahira usuli faqat biti o'rnatilgan fayllarni arxivlashga nusxalaydi?

Toʻliq

& Chiziqlar

Hisoblangan

Differentsial

Maskaradning yana bir atama nima?

Doppelganger

Sharpa

Taqlid qilish

Ikki tomonlama shaxs

Yadroga o'rnatilgan zararli dasturlarni antivirus va zararli dasturlarga qarshi dasturlar kabi mahsulotlar bilan aniqlash juda qiyin. Ushbu turdagi zararli dasturlarning nomi nima?

Mantiqiy bomba

Rootkit

Vampire tegish

Yong'oq

Qattiq disklar uchun shifrlash kalitlarini saqlaydigan anakartda joylashgan qurilma komponenti uchun qanday nom berilgan, dushmanning qattiq diskni olib tashlashiga va boshqa kompyuterda foydalanishiga yo'l qo'ymaydi?

Qattiq diskni shifrlash

Kripto-shrift

asbob-uskunalar xavfsizlik moduliName

Ishonchli platforma moduli

Quyidagi parolni buzish usullaridan qaysi biri eng tezkor?

Lugʻatga hujum

Qo'pol kuch

Tug'ilgan kunga hujum

Xeshni teskarisiga moslashtirish

Linux-da foydalanuvchi hisobini noyob tarzda aniqlash uchun qanday dizayner ishlatiladi?

gid bilan

SID

UID

PID

Nmap-dan foydalanib, qaysi switch buyrug'i UDP ulanishlarining xostni skanerlashini ta'minlaydi?

-sS

-sX

-PT

-sU

Quyidagilardan qaysi biri yuqori darajadagi ota-ona domenini ko'rsatadi?

.org

Xavfsizlik ma'muri Telnet-dan foydalanganda quyidagilardan qaysi biri foyda beradi?

Trafik aniq yuboriladi.

Maxfiy soʻz kodlanmagan.

Xavfsizlik ma'murlari dushman nima qilayotganini ko'rishlari mumkin.

Xavfsizlik ma'murlari dushman nima qilayotganini ko'ra olmaydi.

Siz kino ishlab chiqarish kompaniyasida ishlaydigan xavfsizlik ma'murisiz. Ulardan biri

sizning kundalik vazifalaringiz ogohlantirilganingizda IDS jurnallarini tekshirishdir. Siz juda ko'p to'liq bo'lmagan uch tomonlama qo'l siqishlarni olganingizni payqadingiz va sizning xotira ishlashi veb-serveringizda sezilarli darajada pasayib ketdi va mijozlar juda sekin ulanishlardan shikoyat qilmoqdalar. Haqiqiy muammo nima bo'lishi mumkin?

To'g'rilar doir

DDoS

Smurf hujumi

SYN flood

"Tarmoq noma'lum" xabari qanday xabar turi va kodi hisoblanadi?

Type 3, Code 6

3 turi, kod 0

0 kiriting

5-tur, kod 1

Quyidagi chastota rejimlaridan qaysi biri dushman tomonidan shovqin yaratmaslik yoki siqib qo'ymaslik uchun mo'ljallangan?

To'g'ridan-to'g'ri ketma-ketlik tarqalish spektri

Chastotalarni o'zgartirish uchun keng tarqalgan spektr

Ortogonal chastota bo'linishi multiplexing

Vaqtni taqsimlovchi bir nechta erkin foydalanish

Xavfsizlik ma'muri sifatida siz DMZ ichidagi serverlaringiz bilan bog'lanishga harakat qilayotgan turli xil IP ulanishlarini tekshirasiz. Bir necha oy oldin sizning serverlaringiz Eronda ro'yxatdan o'tgan IP-dan juda o'xshash hujumlar va tekshiruvlarni olganligini payqadingiz. Bu safar siz Braziliya, Gretsiya, Sudan va Janubiy Afrikadan kelgan IP-lar bilan shunga o'xshash taktikalarni ko'rasiz. Nima deb o'ylaysiz?

Xakerlik guruhi birlashdi.

DMZ-dagi serverlaringiz hackerlar uchun juda jozibador deb topildi.

Hacker proksi-serverdan foydalanmoqda.

Sizda DMZ-da torrent server o'rnatilgan.

Quyida keltirilgan veb-saytlardan qaysi biri telefon raqamlari, administratorning elektron pochtasi va hatto domenni ro'yxatga olish organini o'z ichiga olgan veb-sayt haqida bepul ma'lumot beradi?

Nslookup

qazish

Whois.net

Ping

RFC 18 haqida nima ahamiyatga ega?

Bu yo'naltirilmaydigan IP-manzillarni bildiradi.

Bu veb-proksi serverlardan foydalanishni bildiradi.

Unda DMZlardan foydalanish tasvirlanadi.

IPsec-dagi autentifikatsiya sarlavhasini qamrab oladi.

ICMP echo so'rovi quyidagi turlardan qaysi?

8-tur

3-tur, kod 1

0 kiriting

5 turi, kod 0

HIDS ko'pincha aniqlash uchun qaysi usuldan foydalanadi?

Imzo bazasi

Anomaliya bazasi

Xavfsizlik devori qoidalari

anomaliya

Sertifikat soʻrayotganda quyidagilardan qaysi biri foydalanuvchi haqiqiyligini tasdiqlaydi?

Sertifikatlash markazi

Sertifikat bekor qilinganlar roʻyxati

X.509 va Kerberos

Ro'yxatdan o'tkazish organi

Hacker shifrlash algoritmini buzishning turli usullaridan foydalanmoqda, masalan, yon kanal hujumlari, chastota tahlili, shuningdek, bitni aylantirish. Hacker nima qilmoqda?

Qo'pol kuchlash

Hisobga olish maʼlumotlarini yorib tashlash

Raqamli sud ekspertizasi

Kriptoanaliz

Quyidagilardan qaysi biri to'g'ri XOR chiqishi?

0 0 = 1

1 0 = 0

1 0 = 0

1 1 = 0

Sniff uchun, Ethernet yoki simsiz tarmoqdan ramkalarni tortib olish uchun tarmoq adapteringiz qaysi rejimga sozlanishi kerak?

Aktiv

Fohishaboz

Yashirin

CSMA/CD rejimi

WPA2 da qaysi autentifikatsiya protokoli ishlatiladi?

CCMP

3DES

AES

SAKRASH

Siz mahalliy bank uchun IT xavfsizligini nazorat qiluvchi ma'mursiz. Oldingi kundan boshlab jurnallarni ko'rib chiqayotganingizda, sizning mijozlaringizdan bir vaqtning o'zida keladigan veb-serveringizni maqsad qilib olgan UDP paketlarining juda yuqori tezligini payqadingiz. Aybdor nima bo'lishi mumkin?

Smurf hujumi

DDoS

SYN toshqin hujumi

Fraggle-hujum

TCP uch tomonlama qo'l siqishning so'nggi bosqichi qaysi?

ACK

SIND

SYN/ACK

Qo'shma Joylar

Token - bu tasdiqlash omilining qanday turi?

1-tur

2-tur

3-tur

4-tur

Qora shlyapa sifatida ishlaysiz, siz juda mashhur ijtimoiy media veb-saytini taqlid qiladigan veb-serverni turishga qaror qilasiz. Siz shuningdek, hamkasblaringiz kompyuterlarida xost faylini yangilaydigan skriptni yaratish va bajarishga qaror qilgan norozi xodimsiz. Bu ularning DNS keshini zaharladi. Sizning hamkasblaringiz ertalabki mashg'ulotlarini ushbu mashhur ijtimoiy media veb-saytiga borib, so'ralganda shaxsiy ma'lumotlarini taqdim etishadi. Afsuski, ular uchun ular veb- saytingizga kirmoqdalar va keyinroq foydalanish uchun ularning hisob ma'lumotlarini saqlaysiz. Siz qanday hujum turini o'tkazdingiz?

O'rtadagi odam

Pharming

Nayzali fishing

Phishing

XMAS skanerini yoqish uchun ishlatiladigan TCP sarlavhasi uchun bayroq bayti quyidagilardan qaysi?

00101001

11001011

11101000

00101100

Quyidagilardan qaysi biri "yumshoq" boshqaruvni tasvirlaydi?

Foydalanuvchi shartnomasi

Kirish boshqaruvi ro'yxati

Biometriya

Xavfsizlik xizmatchisi

Orqa eshik dushmanga qanday imkoniyatlarni beradi?

Orqa eshiklar ma'lumotlar dasturini buzishi mumkin.

Ular TPMdagi kriptografik kalitlarni yo'q qilishadi.

Ular past darajadagi formatlash operatsiyalarini ta'minlaydi.

Ular mijozga masofadan turib kirishni ta'minlaydi.

Quyidagilardan qaysi biri elektron autentifikatsiyani amalga oshirishda foydalanish uchun inson ruhiy atributlari to'plamini tasvirlaydi?

Shaxsiy identifikatsiya guvohnomasi

Soch va barmoq izlari

Biometriya

3 turi nazorat

Quyidagilardan qaysi biri yagona nosimmetrik kriptografiya oqimi shifri?

RC6

Zarb balig'i

RC4

ECE

Quyida keltirilganlardan qaysi biri rad etmaslikni ta'minlash uchun ikkita hash qiymatini taqqoslaydi?

DSA

ECE

MD5

SHA-1

Qora shlyapa sifatida siz foydalanmoqchi bo'lgan savdo markazida WAP-ni aniqlaysiz. Siz WAP dan foydalanayotganini aniqlaysiz. WAP-dan foydalanish uchun qaysi usuldan foydalanasiz?

RC4 bo'lgan shifrlash algoritmi

Ishga tushirish vektori (IV)

Maxfiy soʻz

Foydalanuvchi ismi va maxfiy soʻzi

Hujumingizning izlari bosqichini tugatgan oq shlyapa sifatida, siz maqsadingiz haqida ma'lumot to'plash uchun turli vositalarni ishlatib, davom etasiz. Siz portlarda qanday xizmatlar taklif qilinayotganini aniqlay oldingiz. Siz qanday hisoblar mavjudligini ko'rishingiz va turli xil almashish xizmatlarini ham aniqlashga muvaffaq

bo'ldingiz. Qaysi bosqich

Siz ichkarida ishlayotganmisiz?

Xizmat proksi

Beparvo skanerlash

Barmoq izi

Ro'yxatga olish

Nmap-dan foydalanib, ping süpürme va operatsion tizimni aniqlash yordamida 192.168.0.0 / 24 maqsadli subnetini skanerlash uchun to'g'ri buyruq nima?

nmap -sP -O 192.168.0.0/24

nmap -sP -V 192.168.0.0/24

nmap -sT -P 192.168.0.0/24

nmap -ps -o 192.168.0.0/24

Quyidagi xizmatlardan qaysi biri 110 portida ro'yxatdan o'tgan?

SNMP

RPC

POP3

LDAP

DNS so'rovlarini o'tkazish uchun Unix tizimlarida quyidagilardan qaysi biri mahalliy ravishda o'rnatilgan?

Ping

nishoncha bilan oʻchirish

Nslookup

qazish

Quyidagi saytlardan qaysi biri DNS so'rovlari ma'lumotlarini olishda samarali?

Bannerlarni tortish uchun quyidagilardan qaysi birini ishlatishingiz mumkin?

Telnet

Ping

Nmap -sP

del \*.\*

Penster sifatida umumiy topilmalaringizga qo'shimcha ravishda qanday tarkibni o'z ichiga olishingiz mumkin?

Yamalangan tizimlar ro'yxati

O'chirilgan hisoblar ro'yxati

Aniqlangan zaifliklar ro'yxati

Bekor qilingan sertifikatlar ro'yxati

IEEE port bazasida autentifikatsiya qilish nima?

TACACS

Diametri

802.1x

TACACS+

Quyidagi hujumlardan qaysi biri 53-port yoki boshqa UDP portlaridan foydalanib, Windows tizimiga parchalangan UDP paketlarini yuboradi, bu tizimning ishdan chiqishiga olib kelishi mumkin?

Zarbalar

Bonk

Stackni sindirish

Skurf

Quyidagilardan qaysi biri ma'lumotlarni buzish va buzish uchun xost yoki insonning o'zaro ta'siriga muhtoj bo'lmagan dastur?

Yong'oq

virus

TroyanName

Zararkunandalik dasturlar

Foydalanuvchi tasodifiy paydo bo'lgan pop-up oyna reklamalarini olayotganini xabar qiladi. Foydalanuvchi kompyuterni qayta ishga tushirishga majbur bo'lgan juda ko'p oynalar mavjud bo'lgan paytlar ham bor. Muammo nima bo'lishi mumkin?

Ish stansiyasiga troyan oʻrnatilgan.

Adware o'rnatilgan.

Pop-uplarni yaratadigan veb-sayt hali ham ishlamoqda.

Rootkit o'rnatilgan.

Quyidagilardan qaysi biri biznes yoki tashkilotning kiberhujumlarga qarshi himoya qilishi va ularga qarshi turishi mumkin bo'lgan darajasini tasvirlaydi?

Chuqurlikda mudofaa

Xavfsizlik chorasi

Baza chizigʻini moslash

Xavfsizlik holati

Yagona kirish (SSO) strategiyasining bir kamchiligi nimada?

Autentifikatsiya qilish uchun yagona muvaffaqiyatsizlik nuqtasini taqdim etadi.

Xavfsizlik siyosati uchun replikatsiya yo'q.

Maxfiy soʻzlar oddiy matn koʻrinishida saqlanadi.

Foydalanuvchi hisoblariga osongina kirish mumkin.

Qaerda ekanligingizga bog'liq bo'lgan autentifikatsiya omili nima?

1-tur

2-tur

3-tur

4-tur

Quyidagilardan qaysi biri parollarni oddiy matnda topishning maqbul usuli?

SSH aloqasini ushlab qo'yish

TCP oqimidan keyin

SSL trafigini kesib qo'yish

Jon Ripper yordamida hisobni buzish

Kontentga manzillanadigan xotira jadvali nima?

IP manzillar jadvali

NetBIOS nomlarini koʻrish uchun ishlatiladigan jadval

Portlarga tegishli MAC-manzillar jadvali

IP manzillarga bog'langan domen nomlari ro'yxati

Qora shlyapa ICMP xabarining qismlarini jabrlanuvchining tizimiga yuboradi. Tizim barcha paketlarni qabul qilganda, ularni qayta yig'adi va keyin ishdan chiqadi. Qaysi hujum bunday xatti-harakatlarga olib keladi?

O'lim pingi

To'g'rilar doir

Fraggle-hujum

ICMP toshqini

Quyidagilardan qaysi biri SSO autentifikatsiya standartida nosimmetrik kalitlardan foydalanadi.

KUNAM

Diametri

Kerberos

HIDLAR

Shaxsiy IP-manzilni shlyuzdagi umumiy manzilga o'zgartiradigan protokol nima?

NAT

PAT

GNAT

NAT-T

Intrussiyani aniqlash tizimlarida qaysi kombinatsiya ishlatiladi?

NIDS va SIDS

HIDS va SIDS

IDS va IPS

HIDLAR VA NIDLAR

Siz yong'in sodir bo'lganda media firmasining kutilgan yo'qotishlarini aniqlash vazifasini bajargan xavfsizlik ma'murisiz. Siz firma o'z aktivlarining yarmini yo'qotishni kutishi mumkin deb hisoblaysiz, bu 10 million dollarga teng. Bundan tashqari, yong'in ehtimoli har 10 yilda bir marta ekanligini aniqlaysiz. Yillik yo'qotishni kutish muddati (ALE) qanday?

500,000 AQSh dollari yo'qotish

$ 1,000,000 yo'qotish

$ 250,000 daromad

$ 250,000 yo'qotish

Qaysi federal qonun dam olish va tranzitda tibbiy yozuvlarni ta'minlashni talab qiladi?

Teng tekislik

HIPAA

FISMA

PATRIOT qonuni

Hujumchining (qora shlyapa) himoyachiga (potentsial qurbon) nisbatan bir afzalligi nima?

Vaqti

Onlayn xakerlik forumlari

Pul

Metasploit

Quyidagilardan qaysi biri simsiz tarmoqda xavfsizlikka kirish bilan bog'liq?

WPA

802.1x

Radius

TACACS+

Quyidagilardan qaysi biri SQL ma'lumotlar bazasidagi Clients jadvalini o'chiradi?

jadval mijozlarini yangilash

\* MIJOZLARDAN TANLANG

JADVAL MIJOZLARINI QOʻYISH

jadval klientlari

Maqsadli tizimda yoki tarmoqdagi zaifliklarni tekshirish uchun quyidagi vositalardan qaysi biri ishlatiladi?

Pishqiriq

NCAT

Nessus

Metasploit

Xavfsizlik ma'muri sifatida turli korporativ ofislarga ko'prik o'tkazish uchun simsiz tarmoqlardan foydalanish rejalari bilan bog'liq xavfsizlik xavotirlari mavjud. Ushbu idoralarning joylashuvi tufayli an'anaviy ulanishlar iqtisodiy jihatdan taqiqlanadi. Quyidagi antennalardan qaysi biri istalmagan signalni ushlab qolish ehtimolini cheklab, eng yaxshi qamrovni ta'minlaydi?

Omni

Fan

Yagi

Sun'iy yo'ldosh tishxonasi

Quyidagi shifrlash usullaridan qaysi biri Phil Zimmerman tomonidan ishlab chiqilgan?

AES

PGP

DES

DEA

IPv6 manzillashning qaysi sxemasidan foydalanadi?

32 bit

128 bayt

32 bayt

128 bit

Quyidagilardan qaysi biri zaiflikni eng yaxshi ta'riflaydi?

Potentsial amalga oshirilayotgan tahdid

Qarshi chora mavjud emas

Tahdidli aktyor

Hodisa

Kompaniyadagi yangi foydalanuvchiga minimal imtiyozlar to'plami beriladi. Ular lavozimga ko'tarilib, turli lavozimlarga o'tishlari bilan ko'proq imtiyozlarga ega bo'lishda davom etmoqdalar. Bu nima deb nomlanadi?

Ko'lami creep

Mavqeini kesish

Access creep

Imtiyozlar darajasi

Tarmoqdagi qurilmani nima deb ataysiz?

Uskuna

KompyuterComment

Svitvitchi

Kirish qurilmasi

Jabrlanuvchi haqida yashirincha ma'lumot to'playdigan dasturni nima deb ataysiz?

TroyanName

josus dastur

Zararkunandalik dasturlar

O'g'irlash dasturi

Xizmat to'plami identifikatori (SSID) nechta belgini o'z ichiga oladi?

32

64

20

128

Internet kalit almashinuvi (IKE) protokolining maqsadi nima?

Foydalanuvchi maʼlumotlarini uzatish

Foydalanuvchi profillarini toʻplash

Jamoatchilikka kalitlarni tarqatish

Maxfiy kalitlarni almashtirish

Biometrikaga kelsak, noto'g'ri rad etish darajasi (FRR) va noto'g'ri qabul qilish darajasi (FAR) teng bo'lsa, bu kesish nimani anglatadi?

O'tish xato darajasi

Xato tenglashtirish

Yigʻindi

O'tish darajasi teng

Ma'lum qonuniy dastur kabi ko'rinishga ega bo'lgan dastur, ammo aslida zararli tabiatan qanday zararli dastur hisoblanadi?

josus dastur

Rootkit

reklama dasturlari

TroyanName

SFTP qaysi standart portdan foydalanadi?

20

21

22

20 va 21

Quyidagilardan qaysi biri IEEE 802.3 muhitini tasvirlaydi?

CSMA/CD

Simsiz aloqa xavfsizligi

foydalanuvchilar kirish nazorati ro'yxati

Port bazasida autentifikatsiya qilish

Siz yuridik firmaning tizim ma'murisiz. Sizga ma'lum bo'lishicha, bir necha foydalanuvchilar ilovalarni ochishda o'zlarining elektron pochta manzillarini kiritganlarida, ularning kompyuterlari pop-up oynasiga ko'ra tizim buzilishini tiklash uchun qo'lda qayta yuklashni talab qiladi. Muammo nima bo'lishi mumkin?

Troyan qatl etildi.

Mantiqiy bomba ishga tushirildi.

Foydalanuvchilar sabr qilmaydilar.

Foydalanuvchilar patch yangilanishining o'rtasida edilar.

Quyidagi xizmatlardan qaysi biri TCP porti 389 bilan bog'liq?

LDAP

IMAP

kichik va o'rta biznes

RPC

Tizim tayinlangan ochiq va maxsus kalitlar bilan sertifikat yaratadi. Ushbu tizim uni raqamli imzo qo'yadi. Bu tizimning roli nima?

Ro'yxatga olish markazi

Sertifikatlash markazi

Kerberos tizimiStencils

Server/mijoz muhiti

Xavfsizlik ma'muri sifatida siz xodimlarning ma'lumotlarga kirishini faqat ma'lum shaxslar bilan cheklashni xohlaysiz. Qanday kirish turini amalga oshirasiz?

Bilish kerak

Imtiyozlarning eng kam darajasi

Mavjudlikni kamaytirish

Shifrlash jarayonini sozlash

Microsoft Office va boshqa ofis to'plamlari ilovalari zararli dasturlarning bajarilishi yoki tarqalishining oldini olish uchun o'chirilishi kerak bo'lgan xususiyatga ega. Qaysi xususiyatni o'chirish kerak?

Pochta

FTP-mijoz

Avtomatik yangilash xususiyati

Makros xususiyati

Ishonchli kalitlarga ega bo'lish uchun sertifikatlangan tashkilotning nomi nima?

Hukumat xavfsizligi

Issiq sayt

Eskraj

Offsite zaxiralash

HTTPS qaysi standart TCP portidan foydalanadi?

443

8080

80

22

Foydalanuvchi resursga bir marta autentifikatsiya qilsa va keyin qayta autentifikatsiya qilmasdan qo'shimcha ilovalarga kirishga ruxsat berilsa, autentifikatsiyaning qaysi shakli ishlatiladi?

Bir marta ro'yxatdan o'tish

Nonce kirish

Kerberos

Yagona kirish

Yo'riqnoma nimani ajratadi?

To'qnashuv domenlari

Eshittirish domenlari

Almashtirish

Joʻnatish usullari

0-turi qaysi UDP porti bilan bog'liq?

U 53-port bilan bog'liq.

U barcha port oralig'ini, ya'ni 0 dan 1023 gacha foydalanadi.

ICMP port raqamlari bilan bog'liq emas.

Portlar 0 turi uchun dinamik ravishda ishlab chiqariladi.

Quyidagi saqlash texnologiyalaridan qaysi biri eng o'zgaruvchan hisoblanadi?

Qattiq disk

USB flesh-uskunasi

Protsessor keshi

DDR3

Windows tizimining maxfiy soʻz fayli quyidagi kataloglardan qaysi birida joylashgan?

C:\System32\Windows\config

\etc\win\config

C: \ System\Windows\config

C:\Windows\System32\config

Hisobning har qanday mumkin bo'lgan parol kombinatsiyasini taxmin qilish harakati qanday?

Qo'pol kuch

Xeshni uzatish

Lugʻatga hujum

Ijtimoiy injiniring

Linux-dagi egaga, guruhga va boshqalarga ob'ekt uchun o'qish, yozish va bajarish imtiyozlarini berish uchun qanday buyruqdan foydalanasiz?

Chmod 666

Chmod 777

Chmod 7

Chmod 532

Linux-da yuklash uchun turli operatsion tizimlar o'rtasida o'tish uchun quyidagilardan qaysi biri ishlatiladi?

Yagona bootloader

Ctrl+S

Grand Unified Bootloader

Ctrl+F4+S

Quyidagilardan qaysi biri tizimni penetratsion sinovdan o'tkazish uchun ramka hisoblanadi?

Metasploit

Qobil va Hobil

Nessus

Xavfsizlik piyozi

Windows'da faylni bekitish uchun qanday buyruqdan foydalanishingiz mumkin? Javob. +h attrib <fayl nomi>

B. h+ <fayl nomi>

C. Fayl nomi attrib +h

D. attrib +h <fayl nomi>

Quyidagilardan qaysi biri to'g'ri MAC manzili?

00-12-3e-ff-d4-98

3i-45-fa-90-25-1b

ff-ff-ff-ff-ff-fg

65-23-ab-cb-a9

Paket xavfsizlik devori qurilmasi OSI modelining qaysi qatlamida ishlaydi?

Qatlam 2

Qatlam 4

Qatlam 7

Qatlam 3

Qora shlyapa sifatida siz bir qator pastki tarmoqlarni skanerlaysiz va ba'zi xavfsizlik vositalari yo'q bo'lganini aniqlaysiz. Bundan tashqari, noto'g'ri konfiguratsiyaning aniq belgilari yoki tafsilotlarning etishmasligi mavjudligini aniqlaysiz. Ehtimol, ma'mur yangi boshlovchi bo'lishi mumkin va hali ham o'z tarmog'ini qattiqlashtirish bo'yicha arqonlarni o'rganmoqda. Bu erda nima bo'lishi mumkin?

Asal

Asal

Notoʻgʻri moslamalar

Endi ishlatilmayapti pastki tarmoq

Zararli dasturlarga qarshi dasturlardan foydalanishning eng katta kamchiligi nima?

Qayta ishlash resurslarini oladi.

Unda viruslarning dolzarb ta'riflari bo'lishi kerak.

Zararli dasturlarga qarshi dasturlar qimmat.

U markaziy yoki mustaqil ravishda boshqarilishi mumkin.

DES algoritmining nomi nima?

DEA

DES

Ikki baliq

3DES

Heartbleed dushmanga nima beradi?

Ekspluatatsiya qilingan vaqtda moʻljallangan serverning xotira tarkibi

A Uy do'sti

O'sha paytda dushmanning xotirasi tarkibi

U dushmanga hech qanday ma'lumot bermaydi.

Foydalanuvchi Internetdan musiqa faylini yuklab olganligi haqida xabar beradi. Ular faylni ochganlarida, u dasturni o'rnatgandek tuyuldi va keyin foydalanuvchidan qattiq diskini shifrlash uchun kalitni olish uchun PayPal hisobiga $ 500 dollar

to'lovini yuborishni so'rashdi. Foydalanuvchi yo'q

ish stoliga kirish. Muammo nima bo'lishi mumkin?

Foydalanuvchi yolg'onni boshdan kechirmoqda.

Foydalanuvchi ransomware dasturini yuklab oldi va o'rnatdi.

Foydalanuvchi zararli dasturlarni o'rnatdi.

Foydalanuvchi notoʻgʻri musiqa faylini yuklab oldi.

Qaysi Wi-Fi standarti 2.4 va 5 gigagertsli radio diapazoniga va 100 Mbit / s tezlikka ega?

802.11i

802.11

802.b

802.11n

Bu qanday infratuzilmani tasvirlaydi?

PKI

O'rtadagi odam hujumi

Ijtimoiy injiniring

Kerberos muhiti

Ushbu diagrammada asosan qaysi turdagi protokol qo'llaniladi?

Translyatsiya qilish

ARP so'rovi

Ping

DHCP ijarasi

Quyidagi diagrammadan qaysi IP-manzilni aniqlay olasiz?

192.168.1.255

192.168.1.118

255.255.255.255

192.168.1.1

Ekran tasvirida qanday kodlash turi qoʻllaniladi?

ASCII

Oltilik

Binar format

UTF-8

Quyidagi ekran tasvirida qanday TLS versiyasini topish mumkin?

1.2

1.3

312

1

Quyidagi diagrammada dushman nima qilishga harakat qilmoqda?

O'lim pingi

Veb-serverni aniqlash

SQL-in'ektsiya

Internetni buzish

Quyidagi ekran tasvirida ko'rinib turganidek, dushman veb-brauzerdagi URL satrida nima qilishga harakat qilmoqda?

Imtiyozlar darajasi

Katalogni oʻzgartirish

Yashirin SQL in'ektsiyasi

SQL bilan jadvalni oʻchirish

Keyingi skrinshotda mijoz qaysi DNS tizimni so'rov qilyapti?

Google Google

Port 53

Port 64234

Yoʻq

Quyidagi skrinshotga muvofiq root-ning foydalanuvchisi uchun maxfiy soʻz nima?

ildiz

x

Maxfiy soʻz yoʻq.

x: 0:0

Snort-dagi quyidagi logga asoslanib, fayl yuklab olinadigan manzilli port nima?

56209

23

49190

Port mavjud emas.

Quyidagilardan qaysi biri foydalanuvchi hisobi hisoblanadi?

usbmux

nur

ossecr

hech kim