حملات سایبری منع سرویس و توزیع شده (DOS & DDOS)

فصل اول:

انواع هکرها:

۱. Hacktivism دارای انگیزه سیاسی
۲. کلاه مشکی
۳. کلاه سفید ؛ برای hardening و ارتقاء امنیت و تدافعی
۴. کلاه خاکستری
۵. از جان گذشته : هدف آن مقصد خاص و با علت خاصی است.

تهدید:

از دست رفتن اطلاعات ، برند سازمان و محرمانگی

مهمترین حمله ها:

۱. Dos
۲. Ddos

از نوع حملات زیرساختی و سرویس های شبکه هستند.

رایج ترین نرم افزارهای مخرب :

۱. Adware
۲. Spyware
۳. Virus
۴. Worm
۵. Trojan
۶. Ransomware
۷. Rootkit
۸. Exploits
۹. Miners و criptomining
۱۰. Keylogger

کی لاگر Key Logger، ثبت عملیات صفحه کلید و ارسال برای مهاجم

باج افزار یا Ransomware که اطلاعات مهم را رمزگذاری می کند و سپس طلب پول و رمزارز می کند .
نکته اینکه اگر پول بدهیم هم رمز را باز نمی کند. و راه حل ان اینست که فقط پیش گیری کنیم.

روت کیت، دسترسی کامل به مهاجم می دهد و پنهان می ماند.

اکسپلویت، استفاده از آسیب پذیری سیستم تا بهره برداری از آن

ماینر یا کریپتوکراسی ، شخص دیگر از کامپیوتر ما برای استخراج bitcoin استفاده می کند.

یک تروجان می تواند از راه دور به پرینتر شما دسترسی پیدا کند.

بایستی کنار آنتی ویروس spyfounder هم باشد که اگر جاسوس افزار به شکلی وارد سیستم شد و آنتی ویروس نتوانست شناسایی کند spyfounder حتما شناسایی می کند. spyhunter هم مناسب است.

سایت https://www.malwarebytes.com برای جلوگیری و protect کردن حملات

معروف ترین تروجان ها RAT ها هستند.

برای شناسایی آنها trojan scanner , virus scanner هم وجود دارد و سریع بدافزارهای را شناسایی می کند و از آنتی ویروس قوی تر است.

https://brave.com manage engine desktop . central enterprise

انواع rootkit :

کاربر root که با ریستارت کار می کند و با ssh وصل می شود.

و backdoor که هر کاربر و با telnet وصل می شود.

Kernel/user/boot/firmware/memory/vitual

کشف کننده rootkit و https://www.gmer.net پردازنده gmer

سایت http://www.hitmanpro.com/en-us از ارز دیجیتال استفاده می کند که رد پایی از آنها نماند که بعدا پیدایشان کنند.

بات نت BotNet **:**

Bot->robot->botnet کدهای مخربی هستند که بدون اطلاع صاحبانشان در سیستم ها اجراء می شوند و اغلب برای ddos استفاده می شوند.

تاثیرات مخرب botnet:

۱. حمله
۲. سرقت
۳. اسپم
۴. جعل
۵. آپلود

روش های پیشگیری از botnet :

۱. بروز رسانی سیستم عامل
۲. بازنکردن ایمیل مشکوک
۳. بازنکردن دانلود مشکوک
۴. لینک مشکوک
۵. آنتی ویروس

دو نوع کلی حمله سایبری:

۱. فعال
۲. غیر فعال

انواع حملات فعال سایبری:

۱. Dos
۲. Arp poisning
۳. Ping flood
۴. Ping of death
۵. Man in the middle

در حمله Dos ، یک نفر به یک مقصد خاص، حمله انجام می دهد.

انواع حملات غیر فعال سایبری:

۱. Buffer overflow
۲. Format string attack
۳. شنود و اسکن پورت

تهدیدات مربوط به هر لایه از osi :

Sniff, Mac address spoofing / arp poisioning / vlan hopping	layer 2
Mitm attack	layer 2,3,4,7
Ip spoofing, ip routing spoof , icmp , smurf	layer 3
Tcp hijacking	layer 4
Ddos, dns spoofing	layer 7
Encryption, file format , malicious code	layer 6
Session hijacking , rdp	layer 5
Syn , udp , tcp/ip flood , hijack	layer 4
Wire tapping / jamming	layer 1

لایه های شبکه در امنیت خیلی مهم است. ٪۷۰ حمله ها مربوط به لایه اپلیکیشن است.

اگر در فایل hosts که با notepad باز می کنید . در انتهای فایل غیر از ip ۱۲۷.۰.۰.۱ ip دیگری بود یعنی سیستم هک شده است.

دستور cmd و arp -a

اگر یک ip دو تا mac یکسان داشت مورد حمله arp قرار گرفته ایم. Arp poisoning

باید برای هر حمله و برای هر لایه paln و طرح داشته باشیم و آگاهی و update باشیم راجع به حملات می تواند تا حدودی زیادی جلوگیری نماید. گاها حملات بزرگ در دنیا در سطح پایین صورت می گیرد.

فصل دوم:

گام های یک حمله سایبری:

۱. شناسایی
۲. اسکن
۳. دسترسی gain access
۴. استخراج اطلاعات
۵. پاکسازی (توان بازگشت پس از حمله حتی بعد از انجام اقدامات امنیی توسط قربانی)
۶. حمله

نحوه انجام حملات DDOS :

۱. ساخت بات نت
۲. فرمان حمله
۳. ترافیک سنگین
۴. اختلال سرویس

در حمله DDOS ، چند نفر به یک مقصد و یا سامانه انجام می دهد. شبکه و سرور مورد نظر را وادار به ناتوانی درارائه سرویس عادی با هدف قرارن پهنای باند شبکه یا اتصال پذیری می نماید.

فاکتورها و نحوه تشخیص و شناسایی حملات DDOS

۱. افزایش ناگهانی ترافیک
۲. کاهش عملکرد شبکه
۳. خطای ۵۰۳
۴. افزایش استفاده از cpu

با ابزار **wireshark** امکان مانیتورینگ میسر است.

سایت https://check-host.net/check-http مشخص می کند که اینکه حمله سنگین ddos به سایت انجام شده یا نه؟

اقدامات بعد از حمله:

۱. Cve
۲. Cvss

و استفاده از آنها در مدیریت امنیت که به ما کمک می کنند روی آسیب پذیری ها و نمایش عمومی.

نصب نرم افزار manage engine event log برای نمایش log ها.

دسته بندی حملات DDOS :

۱. حملات لایه کاربردی یا Application : htp flood, udp flood , icmp flood
۲. حملات پروتکل protocol : لایه ۳ و ۴ syn flood

حمل معروف syn flod که مرحله hand shake را اثر می گذارد .مربوط به پروتکل tcp در شبکه است.

درخواست برقراری ارتباط ….hello

آمادگی برای ارتباط … syn , ack و syn flag برای آغاز ارتباط

برقراری ارتباط ack flag برای تصدیق رسیدن یک بسته

فایروال waf باعث جلوگیری از حملات لایه application می شود.

باید فایروال جلوی بسته های ping , icmp را بگیرد که ازحمله syn flood جلوگیری شود.

New inbound rule wizard

Window defender firewall and advanced …..

حملات ….. , ddos , buffer overflow توسط فایروال WAF سطح app جلوگیری می شود.

حملات volumetric : بات نت

بات نت: از ایمیل ip camera , email باز و adware و کلیک کردن ها روی سایت های آلوده که باعث می شود کد مخرب وارد سیستم شود و در شبکه پخش می شود و از طریق botmaster حملات گروهی را شکل می دهد. مستر : قسمت مدیریتی و فرماندهی bot net ها است.

Web of trust یک پلاگین می آورد.

https://chromewebstore.google.com/wot_website_security_safe/

اگر این پلاگین را نصب کنیم، به محض ورود به یک سایت، اگر آلوده باشه آن سایت به ما می گوید و privacy خوبی دارد.

Netcraft-extention سایت هایی که حاوی فیشینگ است را شناسایی می کند و سیستم را در مقابل فیشینگ محافظت می کند

حملات passive :

عموما شنود و جمع آوری اطلاعات هست. حمله سایبری صرفا از بستر اینترنت نیست و ۹۰٪ سازمانهایی که مورد حمله سایبری قرار گرفته اند به اینترنت وصل نبودند و vlan , segmentation , zone بندی دارند.

حملات سایبری صرفا خارج از شبکه ای نیست و حملات داخل شبکه بیشتر از حملات خارج از شبکه است.

با صدور مجوز و یا عضویت یک کاربر غیرمجاز بوجود آید از محیط بیرون (راه دور یا اینترنت و …..)

هکر، در زمانی هایی که ترافیک سایت بر روی سایت است و دسترسی بالا است (مناسبت های عید و ...) کار خود را شروع می کند و ترافیک جعلی را به سمت سایت می آورد.

چگونه حملات DDOS را کاهش دهیم:

۱. بروز رسانی
۲. Patch
۳. فایروال
۴. Ids, os قوی و سوئیچ و روتر
۵. **مسیریابی سیاه چاله** : مسیریابی ترافیک مخرب و نا مشروع به سمت سیاه چاله
۶. کنترل نرخ درخواست ها
۷. Waf

قبل از بروز حمله DDOS چه باید کرد:

۱. فایروال ، استفاده از فایروال نرم افزاری و سخت افزاری (SNORT) ، زیرساخت های Honeypot DDos protection , و تامین امنیت حرفه ای شبکه
۲. Ddos protection
۳. تامین امنیت
۴. Honeypot

حدود ۹۰٪ از مهار حملات dos & ddos با استفاد از فایروال مناسب با config مناسب است و فایروال متناسب با زیرساخت شرکت و troughput فایروال متناسب با پردازش دیتایی در شرکت باشد.

بعد از بروز حمله DDOS :

۱. فیلتر ترافیک ورودی شبکه
۲. فیلترینگ ip بر اساس تاریخچه
۳. تغییر آدرس ip
۴. Load balancing

بهترین ابزارها برای جلوگیری از حملات DDOS :

۱. Firewall
۲. Switch
۳. Routers

جادوی سیاه: drive by download بدون کلیک کردن و حتی دانلود، بدافزار روی سیستم نصب می شود (مثلا با کپی کردن) . هر پنجره ای را بعد از مطالعه حتما ببینید و آنها را پشت سر هم و قطاری باز نکنید. افزونه های امنیتی ublock origin , noscript برای جلوگیری از ورود کدهای مخرب به سیستم را می گیرد که اینها پلاگین هستند.

فرایند در ویندوز. شماره اختصاصی فرایند (process ID (PID که در task manager می آید.

اگر یک سرویس از حافظه زیادی استفاده می کند یعنی سیستم هک شده است. isas هم باید در system32 باشد مثل service و winlogonنه جای دیگر. مثله c:\windows\connectionstatus

ابزار process hacker می تواند بدافزار را شناسایی کند و ابزار processMon , process Explorer نمایش فعالیت ها و detail را می دهد. از pestudio برای تحلیل برای تحلیل در soc استفاده می کنند و هر artifact مشکوک را اعلام میکند.

فرایندهای ویندوز مناسب بدافزارها:

۱. Svchost
۲. Explorer
۳. Csrss
۴. Winglogon
۵. Service
۶. Isass

برخی بدافزارهای ویندوز:

۱. Ctfmon
۲. Winlogintaskmgr

چرا فرآیندها محیط مناسبی برای بدافزاها می باشند:

۱. دسترسی آسان
۲. نقاط ضعف
۳. عدم شناسایی آسان

ابزار process hacker , pestudio pocmon

ابزار خوب ویندور برای مشاهده خرابی ویندور reliability monitor است. که در search ویندوز می آید. از pestudio برای تحلیل در soc استفاده می کنند و هر artifact مشکوک را اعلام می کند

اگر سیستم خود به خود هنگ می کند یا restart می شود :

Search->view reliability and problem history لیست سرویس های منجر به موضوع را نشان می دهد.

متد های مورد استفاده در حملات Dos , DDOS :

Icmp flood: حجم بالایی از درخواست های icmp (ping) در یک شبکه باعث پاسخگویی تمام Host (هاست های) شبکه می شود و پاسخ به سمت access point داخل شبکه مسیردهی می شود و باعث از کارافتادی سوئیچ می شود.

حمله قطره اشکی یا Teardrop attack : از طریق managed ip و با overlap ، load بالایی برای کارت شبکه بوجود می آورد.

NUKE : با ارسال درخواست های اشتباه ping اقدام به ازکارانداختن شبکه می نماید . حمله winnuke با استفاده از ضعف netbios و ارسال یک رشته اطلاعات به پورت ۱۳۹ انجام می شود.

R_U_Dead_Yet : این حمله با استفاده از session هایی که توسط webapp در انتظار درخواست هستند ، انجام می شود.

Slowloris: که اکثر session های وب سرور را باز نگه می دارد. و RUDY با ارسال درخواست با هدرهای حجم بالا به این session های در حال انتظار باعث از کار افتادن وب سرور می شود.

حملات syn flood : هدف آن ، پروسه hand_shake پروتکل tcp است. در این حمله، پروسه سه مرحله ای ایجاد ارتباط tcp از سمت مهاجم نیمه کاره، رها می شود. این کار باعث می شود سرور سرویس دهنده برای باقی مراحل در انتظار باقی بماند و زمانی که تعداد اینگونه درخواست‌ها زیاد می شود ، سرور قادر به برقراری ارتباط و درخواست جدید نخواهد بود.

حملات dos در سطح تجهیزات شبکه : پسورد طولانی در سیسکو و باگ buffer overflow

حملات در سطح سیستم عامل : (ping of death) و استفاده از پروتکل icmp ،

حملات مبتنی بر application : وادار به استفاده از تمام منابع در دسترس سرور و خارج از دسترس نمودن آن (finger bomb)

حملات از طریق سیل داده ها : flood pinging و استفاده از تمام پهنای باند سیستم قربانی

فایروال WAF :

کار آن شناسایی حملات , sql injection . xss , buferoverflow , information leakage
web server and dos attack , parameter tampering است.

انواع waf :

۱. مبتنی بر شبکه NW WAF
۲. مبتنی بر میزبان Host Based WAF

Waf ها می تواند تحت مدل مختلفی از جمله لیست سیاه، لیست سفید و مدل های امنیتی ترکیبی کار کنند .

انواع اسکن:

۱. اسکن پورت
۲. اسکن آسب پذیری
۳. اسکن شبکه port scanning - nmap

پورت شناخته شده ۱۰۲۳ – ۰

پورت های رجیستر شده ۴۹۱۵۱ – ۱۰۲۴

پورت های دینامیک ۶۵۵۳۵ – ۴۹۱۵۲

مانیتور اتصالات tcp/ip با ابزار currports

لیست پورت های باز و در حال استفاده tcp , udp را نشان می دهد:

www. Hirsoft.net/utils/cports.html

three-way-handshake :

۱. ارسال flag syn و در خواست ارتباط
۲. پاسخ و ack به درخواست و آمادگی برای ارتباط
۳. ack flag و برقراری ارتباط
۴. نهایتا برقراری ارتباط tcp

flag های tcp :

۱. syn (آغاز ارتباط)
۲. ack (تصدیق رسیدن بسته

۳. psh ارسال بلافاصله داده های بافر شده
۴. RST (راه اندازی ارتباط)
۵. FIN (دیگر انتقال انجام نشود)
۶. urg (داده های داخل بسته بلافاصله پردازش شوند).

اقدامات امنیتی در اکتیو دایرکتوری :

۱. پاک کردن domain admins
۲. استفاده از دو اکانت

سناریو ۱ : نیروی IT با دسترسی Domain – سناریوی ۲: نیروی IT با دسترسی عادی

استفاده از laps : local administrator password solution

مدیریت رمز عبور:

۱. پاک کردن اکانت های قدیمی کاربران
۲. عدم نصب نرم افزاراضافی یا روال های اضافی

مدیریت آسیب پذیری :

۱. اولویت بندی
۲. بروز رسانی سیستم عامل
۳. بروز رسانی نرم افزار
۴. بروز رسانی نرم افزارهای تاریخ مصرف گذشته

انواع وضعیت ها:

time-wait ، syn send ، sys received ، listening ،established، closed wait ،closed

Endpoint : device هایی که نقطه پایانی شبکه هستند و به شبکه متصل

EPP : **endpoint protection platform** (آنتی ویروس ، ضد تروجان ، رمزنگاری دیتا، فایروال، ips , DLP)

برای جلوگیری از نشت اطلاعات و شامل ابزارهای , Kaspersky , mcafee , windefender, atp ..... sentine که به عنوان مکانیزم دفاعی خط اول مقابله با تهدیدات شناخته شده اند.

Symantic endpoint protection , trend micro officescan

EDR : یک پلتفرم و سیستم امنیتی شناسایی و پاسخ endpoint detection and response

دفاع لایه ای (آنتی ویروس و فایروال) . بعد از حمله crowdstrke falcon, carbon black, fireEye endpoint security(HX) , RSA, ebdgame

Windows security : account protection , virus & threat protection, Device security , app & browser control , firewall & protection family option , device performance & head

مکانیزم DEF : data execution prevention یک گزینه امنیتی است که در جلوگیری از اسیب رسیدن به شما از جانب ویروس ها و دیگر تهدیدات امنیتی می توند جلوگیری کند.

MY COMPUTER->SYSEM PROGRAM-> advanced->visual effects -> let windows choose whats best for my computer -> turn on DEP for essential windows program and services only

دفاع در برابر DDOS :

دفاع قبل از حمله: استفاده از فایروال و anti ddos

دفاع در زمان حمله DDOS:

۱. فیلترینگ ورودی (ingress filtering) : راه اندازی یک روتر که اجازه ورود بسته هایی با منبع غیرمجاز را به شبکه نمی دهد.
۲. فیلترینگ بر اساس تاریخچه (history based ip filtering) : بر این اساس روتر لبه شبکه صرفا بسته های ورودی را که از قبل در پایگاه داده آدرس های ip وجود دارد را می پذیرد.
۳. تغییر آدرس IP : تغییر آدرس IP کامپیوتر قربانی با ادرس جدید که باعث می شود که آدرس قبلی غیر معتبر شود.
۴. Load balancing : افزایش پهنای باند در زمان وقوع حمله تا از قطع سرویس جلوگیری شود.
۵. تحلیل الگوهای گرافیکی حمله DOS : نگهداری مولفه های ترافیکی در زمان حمله و سپس تحلیل آنها جهت بروز رسانی تکنیک های توزیع بار (load balancing) و مکانیزم های جدید فیلترینگ و جلوگیری از حملات بعدی DDos

تفاوت dos , ddos :

Ddos : مبداء چندین سیستم هماهنگ، سریع، شدت حمله، دشواری در شناسایی، شامل volumetric , application layer , fragmentation , و حملات پروتکل

Ping www.anat.ir -f -l 1500 پاسخ ، حجم پاکت بالا است و باید fragment شود.

سامانه ای که می خواهیم حمله کنیم، چه میزان حجم بسته هایی را از ما قبول می کند و به ما پاسخ می دهد (این همان mtu می شود) یعنی میزان حجمی که سرور می تواند به ما پاسخ دهد.

نرم افزار currports یک ابزار مانیتور شبکه است.. لحظه ای که مرورگر را اجراء می کنیم به کجا وصل می شویم.

DOS : مبداء یک سیستم واحد، شدت کم، کند، راحتی تشخیص رایانه ip مهاجم، رایج ترین آنها buffer overflow ، پینگ(icmp flood) ، حمله قطره اشکیflooding , teardrop

حمله IGMP flood : در دسته حمله های dos قرار دارد.

وب سایت www.fakemailgenerator.com برای ایجاد ایمیل های یک بار مصرف .

تهدیدات لایه OSI :

Layer 7: malware injection , phishing attacks , app level os attack

Layer 6 : format string attack , malicious code injection , data encoding /decode vulnerability

Layer 5: session hijacking , broute force attack , session fixation

Layer 4: man in the middle , sys/ack flooding , tcp/ip vulnerabilities , hes

Layer 3: ip spoofing , routing table manipulation , ddos attack

Layer 2 : mac address spoofing , arp spoofing , vlan hopping

layer 1: physical temering , wiretapping , electromagnetic interference

فایروال:

فایروال UTM :

UTM (firewall , ips , ids , app control , vpn concentrator , anti virus , dlp , email security , content/web filtering)

مثل fortigate , syberoam , Sophos , kerio در محیط smb استفاده می شود.

NGFW: firewall , ips , app control , vpn concentrator

در محیط enterprise استفاده می شود و با throughput بیشتر از utm و در edge قرار می گیرند.

فایروال ISFW : internal segmentation : اعمال امنیت و در سطح لایه access بین سگمنت های داخلی ، جایی بین core/distribute و access switch ها در شبکه قرار می گیرند. دارای پورت بیشتری نسبت به سایر فایروال ها. (firewall , ips , atp , application control)

فایروال DCFW : امنیت را برای دیتا سنتر ها فراهم می کنند و در لایه core , gateway قرار میگیرد. (firewall , ddos protection) و قوی هستند.

فایروال CCFW : cloud computing firewall برای شرکت های ارائه دهنده سرویس ابری

فایروال های ng,utm, dc, cc از لحاظ operation mode به صورت nat , route (mode) عمل می کنند ولی isfw ها transparent mode هستند

ویژگی های فایروال:

۱. امضای دیجیتال، Application authentication
۲. Inbound and outbound packet filtering
۳. فیلتر سایت ها بر اساس پروتکل
۴. فیلتر بر مبنای آدرس مبداء و مقصد
۵. فیلتر بر اساس پورت مبداء و مقصد
۶. Internet connection sharing (ISC) support
۷. غیر قابل مشاهده شدن نقاط آسیب پذیر و نفوذ پذیر سیستم فایروال stealth mode : سیستم هایمان مثلا نتواند با پورت اسکن اطلاعات پشت فایروال را بدست آورد.
۸. قابلیت پشتیبانی از قوانینی که کاربر تعیین می کند مانند support custom rules
۹. مسدود کردن بسته هایی با یک آدرس IP مشخص و با تعریف پورت های خاص برای کاربر خاص
۱۰. فیلترسایت ها بر اساس محتوی (نام سایت و کلمات کلیدی)content filtering
۱۱. مسدود سازی کوکی ها وآدرس و نام و تلفن و پسورد و ..... cookie control

/ AD blocking /mobile code protection سه میلیون کاربر دارد و مسدودسازی انواع ناخواسته تبلیغاتی و سرعت اینترنت هم بالا می رود.

Intrusion detection tracking - و /logging/email checking

توپولوژی پیاده سازی فایروال یا طراحی فایروال:

Dual homed: فاقد DMZ و با خط dial up , isdn به اینترنت متصل می شود.

Two legged : با یک ناحیه DMZ،روتر متصل به اینترنت به سوئیچ شبکه داخلی متصل

می شود.

Three – legged : یک کارت شبکه دیگر برای DMZ استفاده می شود. روتینگ بسته های اطلاعاتی بین اینترنت و DMZ با روشی متفاوت از اینترنت و شبکه داخلی انجام

می شود.

استفاده از session Hijacking برای انجام حمله man in the middle

در حالت طبیعی ،حمله dos شامل سه بخش است:

۱. Master/handler شروع کننده حمله
۲. Slave/seconaryvictim/zombie/agent/bot/botnet دستگاهی که توسط master به خط افتاده است.
۳. Victim primary victim سیستم هدف

عامل های agents or Zambies : سیستم هایی هستند که برنامه خاصی روی آن نصب شده است.

Cpu hog ابزاری برای حمله dos جهت استفاده از منابع cpu روی سیستم هدف

Winnuke به دنبال پورت ۱۳۹ باز و ترافیک ip ناخواسته به سیستم هدف روی آن و باعث buffer overflow می شود و سیستم از کار می افتد.

Targa برنامه ای که برای حملات dos استفاده می شود.

RPC locator : سرویسی که به برنامه های توزیع شده اجازه اجرا بر روی شبکه را می دهد و مستعد حملات DOS هستند و بسیاری از حملات DOS از این آسیب پذیری استفاده می کنند.

حمله smurf : ارسال تعداد زیادی ترافیک icmp تا آدرس ip با آدرس جعلی شده قربانی را broadcast کند.

نحوه شناسایی و سپس جلوگیری از حمله dos :

۱. کند شدن سرور
۲. دریافت ارور(Error) های عدم اتصال به پایگاه داده - too many comnnection یا internal server error است.

نحوه جلوگیری از حمله DDOS :

کنترل و مدیریت حمله DDOS با اعمال فیلترینگ network-ingress , rate _ limiting ترافیک شبکه

تشخیص نفوذ، برای شناسایی هکرهایی که با master , slave یا agent ارتباط برقرار می کنند

host_auditing (شناسایی ابزارهای کلاینتی و سروری DDOS با اسکن) ، network auditing (شناسایی agent های ddos در ماشین ها یا در شبکه)

ابزارهای ردیابی شبکه (جریان بسته ها با آدرس جعلی)

https:// www.host_tracker.com

مزایای استفاده از CDN :

۱. سرعت بیشتر وب سایت
۲. افزایش رضایت بازدیدکنندگان
۳. بهبود CEO برای موتورهای جستجو
۴. کسب رتبه بالاتر در نتایج جستجو گوگل
۵. کاهش مصرف پهنای باند و ترافیک Host , server
۶. لود Load بهتر تصاویر
۷. افزایش امنیت وب سایت با مخفی سازی اطلاعات سرور اصلی

مشکل استفاده از cdn : پرداخت هزینه ماهیانه و معروف ترین cdn ها : maxcdn , amazon cloud front , cloudflare

در cdn آی پی سرور به دلیل قرارگیری پشت شبکه cdn قابل دسترس نبوده و حملات هکر به سمت ای پی cdn برای هکر هیچ دستاوردی ندارد.

بررسی امنیت لینک ها و ادرس های اینترنتی:

https://unmask.sucuri.net , https://safeweb.norton.com, https://onlinelinkscan.com ,https://urlvoid.com

استفاده از openvpn بجای vpn و استفاده از l2tp , ipsec , و عدم استفاده از ptp

آیا vpn مشکل نشت dns دارد؟ dnsleaktest.com .

اگر نشت dns داشته باشد ممکن است ip اصلی کاربر فاش شود و نباید اطلاعات واقعی ما را نشان دهد.

تست آدرس ip بعد از اتصال از طریق vpn : سایت whatismyipaddress.com

Whoer.net/extended از flash و jave در صورت نشت dns حفاظت می شود؟

تست آدرس ipleak,net:p2p torrent ip ، اگر اطلاعات واقعی ما آمد یعنی امن نیستیم.

برای جلوگیری از نشت اطلاعات خود می توان webrtc را در مرورگر متوقف کرد.

سطح رمزنگاری بیشنرف سرعت vpn کمتر و قدرت پردازشی بیشتری هم نیاز خواهد بود.

تست سرعت :vpn : سایت speedof.me

حملات ddos می تواند تا ۳۰۰ گیگابایت ترافیک در ثانیه را به سمت سایت ارسال کند.

مراکز scrubbing : سیستم متمرکز پاک سازی دیتا است و ترافیک بد (مثل sql injection , xss , ddos و هر عمل شناخته شده) را پاک می کند و توسط isp ها استفاده می شود.

ارئه دهندگان امنیت ابری مثل prolexic, f5 , serverius دارای چندین scrubbing در جهان هستند.

مهمترین تکنیک های حملات dos :

حملات بر مبنای پهنای باند

جریان سیل آسای درخواست سرویس

حملات بر مبنای جریانی از sys

حملات بر مبنای جریانی از icmp

حملات نظیر به نظیر

حملات dos دائمی

حملات بر مبنای جریانی از اپلیکیشن ها

سه چک لیست ساده برای شناسایی dos :

نظارت و تحلیل ترافیک وب سایت

بررسی تاخیروب سایت و تاخیرهای طولانی مدت

Start -> local group policy editor -> administrator templates -> windows components -> windows power shell

فعال سازی لاگ pwer shell **:**

که شامل turn on کردن , module logging , power shell script block logging powershell transcription که توصیه می شود powershell transcription را فعال کنید زیرا تمامی لاگ های مربوط به پاور شل توسط این گزینه ثبت می شود و برای فعال کردن گزینه مورد نشر gpupdate/force را در cmd اجراء می کنیم.

ابزار فارنزیکی foye tracker بجای دستورات netstat یا wmic

Netstat -na قدیمی‌ترین و بهترین دستور مایکروسافت برای تحلیل ارتباطات با اینترنت است. اینکه چه IP از چه پروتکلی به کجا وصل شده است و الان در چه وضعیتی هست.

ESTABLISHED : هنگامی که سیگنال SYN از سمت کلاینت به سرور ارسال شده و ارتباط به صورت کامل برقرار شده است.

نرم افزار opensavefileview برای بررسی اینکه چه فایل هایی باز شدن یا ذخیره شدن بر روی یک سیستم برای ردگیری رد پاها .

ابزار فارنزیک antimeter : SCAN MEMORY را انجام می دهد.

امن ترین سرویس های ایمیل رمز گذاری شده :

Protonmail (رمزنگای مبداء به مقصد) و tutanota (استفاده از aes, rsa) mailfence , رمزنگاری end to end و پشتیبانی از openpgp

من الله التوفیق