/فرمت اصلی رو حفظ کنید برای پرسش که خوندش راحت‌تر باشه:

1.اقای مهندس وقتی که اکسز میگرید سیسمان روپاک میکنید؟
خیر، باید دسترسی سطح بالا داشته باشیم برای اینکار

2.فرایند رد تیم معمولا چقدر طول میکشه ؟؟
استاندارد 8 ماهه و بیشتر بر اساس **TIBER-EU**

3. دسترسی از طریق DMZ بگیریم بهتره یا از مثلا از فیشینگ و دسترسی بگیریم بهتره ؟
خیلی سوال کلیه بستگی داره از کجا میتونی یه موقع وب سازمان میزنی تو dmz یه موقع نمیخوره با فیشینگ میزنی تو یک zone دیگه است بعد باز خیلی سوال مطرح هست کدوم vlan راهی پیدا میشه برسیم به هدفمون مثلا دیتابیس یا نه !

4. استاندارد ردتیم تو ایران همون چک لیست و روال کلی و جهانی هست یا روشها خیلی فرق دارن و محلی سازی میشه؟.
بر اساس **TIBER,AASE,CBEST**
بعد دقت کنید ما داریم یک سری تکنیک که مربوط به یک گروه شبیه سازی میکنیم دیگه چک لیست همون تکنیک ها هست
من باید TTP همه رو شبیه سازی کنم وضعیت مشخص کنم که شناسایی شد نشد

5. بنظرتون برای شروع رد تیم مثل اون ریپازیتوری که توی گیت هابتون گذاشتید اول توی وب و شبکه اکسپرت بشینم بعدش بریم سراغ بقیه یا نه فرایندش فرق داره .
بستگی به سطح تجربه و دانش فنی فعلی شما وجود داره تو همین شبیه سازی یک سری جاها کامند ویندوزیزدیم یک سری تو شبکه اپپی میدونستیم چیه چه رنجی بیسیک شبکه سیستم عامل ویندوز و لینوکس برای کار پیدا کردن تو ایران الزامی خارج mac هم هست توسعه بدافزار هم هست و ...

6. مهندس جان این فایلی که روش جلو رفتید رو هم میشه لطف کنید و قرار بدین؟(obsidian)
بله همش پابلیک هست و فایل قرار میدم

7. برای api های نیتیو منبع خوبی دارید که بخونیم ؟؟
بهترین منبع داکیومنت ماکروسافت
و اینترنالز آقای پاول و کتاب هاش

8. منابعی رو میشه معرفی کنید واسه مباحث فیشینگ، inforamtion gathering ،osint که aptها استفاده کردن؟ چون بیشترشون فقط کلیت رو گفتن
ببینید تنها منبع ما گزارش های هوش تهدید که مثلا mandiant میده بیرون
ولی اوسینت خودش یادگیری فقط کتاب بزل

9. میشه پروژه رد تیم مثلا رزومه مون خوب باشه ریموت هم بگیریم ؟؟
من نتونستم، فقط ریموت پن تست گرفتم بیشتر نه

10. درباره رد تیم نظامی کم توضیح دادید توی ویدیو های یوتویب میشه یکم درموردش توضیح بدید ؟

ردتیم نظامی منظورم نفهمیدم بیشتر APT گروه های دنیا وابسته به نهاد نظامی و دولتی هستند مثلا TAO که تیمی هست که تو NSA امریکاست و توسعه دهنده استاکسنت بودند

11.پیشنهاد میدید بریم یکم بلو تیم بخونیم که ردتیمیر بهتری بشیم ؟؟
برای درک بهتر که چطور میشناسنت بلوتیم خوبه میتونه آنتی فارنزیک یادبگیری شناسایی سخت بشه

12.مهندس فایل obsidian رو ممکنه در اختیارمون قرار بدید؟← **تکراری**
13. اقای مهندس بنظرتون اندروید اینترنال و اینها هم بخونیم فایده ای داره برای ردتیم ؟؟
من دانشی روی اینترنالز اندرویید ندارم

14.پیشنیاز های رد تیم رو از پایه ترین حالت میتونین بگین ؟ مثلا تست نفوذ اندروید خوبه یاد بگیریم یا از شبکه چه دوره هایی رو بگذرونیم و ...
تست نفوذ یادمیگیریم که غیر از فیشینگ روش بلد باشیم باهاش نفوذ کنیم مثلا وب ، شبکه اگر پروژه بر اساس assume breach نباشه باید دسترسی اولیه بگیریم

15. چقدر Cpp نیاز داریم؟ برای یادگیری و کار کردن
توسعه ابزار
توسعه بدافزار

16. مهاجرت در ردتیم چجوریه؟ چه کشورایی راحت تر و بهترن؟ و اصلا حوزه خوبی هست برای مهاجرت؟
آلمان ، امریکا، هلند

17. مهندس چطوری بفهمیم مثلا اومدیم یک exe تولید کردیم دادیم به طرف اکسز گرفتیم طرف میره تو ویروس توتال اپلودش میکنه چطوری اطلاعات اونو داشته باشیم ؟ مثل APT ها که اینکارو میکنن که بفهمیم شناسایی شدیم یا نه
هش باید سرچ کنی

18. چطوری بفهمیم که تو سیستمی که بهش رسیدیم ایزوله نشده ؟

Honey pot
Deception
Decoy

Ipconfig
Scan ip range

19. روش های کردنشیال دامپینگی که خودتون استفاده میکنید چیه بیشتر ؟ اگر ممکنه توضیح بدید ممنون ازتون

Mimikatz

Change the sourcecode

20.چقدر CVE ها تاثیر داره برای جلو برد اهداف ؟

Cve - poc ?

cobalt strike - > payload
Proxy socks 4

Metasploit socks 4
Ip range

22. مثلا اقای مهندس یک جا ssrf زدید بعدش تونستید gopher زدید رفتید داخل رو اسکن کردید رسیدید به یک روتر چیکار میکنید ؟ مثلا اگر بروت فورس کنید چطوری اینکارو میکنید که soc ها نفهمن

Slow password spray
Brute force
Run as

23.مثلا اقای مهندس اکسز گرفتیم مثلا میایم fltmc میزنیم سریع میان بالا سرمون چیکار کنیم ؟

@soheilsec

24. مهندس درآمد رد تیمینگ توی ایران ممکنه بفرمایید برای تکنسین و... حدودی، هر پروژه چقدر، نرمالش قیمت گذاری چطوریه ؟

2 3 میلیارد

25.مهندس خودتون برای رد تیمینگ از کبالت استفاده نمیکنید؟ از کجا کرکش رو دانلود کنیم بهتره؟

Pwnzer
Zero day lab

Caldera

26چه سودی داره پاک کردن event viewer وقتی لاگ رفته برای soc ؟.

Anti forensic

27. نمیشه جلوی ارسال لاگ به SIEM رو گرفت؟ یعنی agent splunk مثلا غیرفعال بشه یا کلا شبکه ای نتونه لاگی بفرسته؟ ممکنه در سیم alert برای قطع لاگ تولید بشه برای همین لاگ فیک یا از پیش تولید شده بفرسته (مثل فرایند اکستاکس نت که 13 روز لاگ ضبط کرده بود و از روز 14 ام لاگ روز اول رکورد رو میفرستاد) (seyed mojtaba)

Dashboard agent

28. کردنشیال گارد چقدر میتونه جلوی این داستان دامپ رو بگیره؟ راه بایپسی داره یا نه؟(seyed mojtaba)

@soheilsec

29. برای دامپ پسورد ها فرمودید خود استفاده از mimkatz باعث نمیشه EDR و... سریع مشکوک بشن؟

FUD mimikatz
Nanodump

IOA -> systeminfo

30. طی تجربه ای که در RedTeam داشتید، بین برند های مختلف برای EDR چه پیشنهادی برای یه سازمان با اسکوپ 2000 سرور ویندوزی میتونید داشته باشید؟(seyed mojtaba)

Multi brand
Firewall
Antivirus
EDR

31. مهندس نوت obsidian خودتون رو از چه منابعی درستش کردید ؟

Cs conti leak
Mitre attack
Github

32. گروه APT آیا میتونه این همه تست های مختلف انجام بده؟ منظورم این هست هرکدوم از این ها میتونن یه alert مثلا SLEM رو Fire کنن یا آنتی ویروس واکنشی نشون بده بهشون، چجوری ارزیابی میکنن که چه روش یا ابزاری رو برای هر تکنیک یا تاکتیک پیاده سازی کنن. از طرفی هم APT ها نمیتونن کاملا دیوایس های امنیتی سازمان رو شبیه سازی کنن تو لابراتوارشون. در کل چجوری ریسک زدن یه دستور و از بین رفتن دسترسی و شناسایی شدنشون رو بعد از دسترسی اولیه قبول میکنن. (seyed mojtaba)

Conti leak [carbon black]
Cobalt strike

34. اگر شبکه هدف کلا لینوکسی باشه باز هم دست مهاجم اینقدرباز هست یا سخت تر میشه؟(seyed mojtaba)

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/Indexes/Indexes-CSV/linux-index.csv

35. خودت تو فکر مهاجرت هستی؟ چون مصاحبه داشتی با اونور، گفتم رفتنی شدی شاید (seyed mojtaba)
آفر نگرفتم

36. با دسترسی File Write و فایل File Read روی یه سیستم Centos بدون هیچ دسترسی سرور به اینترنت یا DNS چه سناریویی میشه پیاده سازی کرد؟ فقط از طریق sqli روی وب سرور دسترسی دارم به اون سرور (توش موندم) (seyed mojtaba) سرور خودش دیتابیس هست و لینوکسیه. وب سرور رو میبینه nginx هست.
.bat base64 file mimikatz registry
.sh local

.bat net use web server public_html shell

37. مهندس laZagne برای استخراج پسورد استفاده میشه؟

https://github.com/AlessandroZ/LaZagne

Nirsoft

38. دوره اوسینتون رو از کجا بگیریم؟

peneter.com

39. مهندس میگن هش سرچ کنید بجای آپلود داخل ویروس توتال، این فرقش چیه توضیح میدید

Search

40. مهندس منطقی وقتی همه apt ها میان از فیشینگ اینیشیال اکسس میگیرن بریم وب یاد بگیریم؟

Email ->
Sms -> email check kon
Isolate network

41. مهندس شما از چه سورس‌هایی برای آپدیت نگه داشتن خودتون استفاده می‌کنید؟؟ آیا عضو فوروم‌ها شدن میتونه مفید باشه؟؟ میتونید درباره فوروم‌های دارک وب بیشتر توضیح بدید؟

Haveibeenpwned
exploit.in
Breach datbase IRAN

MITRE att&ck
Bleepingcomputers

42. مهندس بهترین منبع برای خرید سرورهای Bullet proof کجاست؟

Warez VPS iran
Netherland

43. مهندس با اومدن تکنولوژی های جدید مثل nsx و ai ,... کار آفنسیو ها سخت نشده؟ یه جورایی انگار دیگه فقط زیرودی به درد میخوره تو آینده، توی ایران فعلا نه ولی در جهان همه شرکت ها میرن سمتش
سمت آفنسیو چطور

Micro segmentation

UBEA

44. یکسری آنتی چیت های بازی ها هستن که دسترسی کرنل دارند ولی به عنوان malware شناخته نمیشن، از signature اینا نمیشه سوا استفاده کرد؟

@soheilsec

45-مهندس پنتست وب برای شروع رد تیم خوبه یا نه هم برای درامد تا بتونم رد تیم را به سطح مناسب برسونم؟
Pentest web -> taghaza balas
Pentest android -> kame

46-مهندس برای رد تیم توی دانشگاه توی گرایش ارشد رایانش امن برم یا شبکه؟

47- مهندس شبکه ایزوله رو چطوری وارد بشیم ؟
100$
1000$

IAB
exploit.in
xss.is

48-مهندس برای رسیدن به سطح قابل قبول برای وارد شدن به کار چه مدت طول میکشه؟
همش بستگی به سطح دانش فعلیتون

Pen200 PWK
PEN300

خسته نباشید مهندس واقعا عالی بود