«بسمه تعالی»

نکات پیشنهادی در خصوص موضوع همکاری تیم شبکه با معاونت سایبری

1. برگزاری جلسه توجیهی

برگزاری جلسه توجیهی و مطرح کردن موضوعات ذیل در این جلسه:

1.1. ملاحظات امنیتی

1.1.1. استفاده از VPN در تمام شرایط و فعال بودن Kill Switch

1.1.2. تفکیک سیستم کاری شبکه و سیستم نفوذ (هرگونه درج اطلاعات مربوط به موضوعات تیم شبکه بر عهده تیم شبکه می باشد)

1.1.3. صرفا استفاده از VPS برای انجام امور محوله

1.1.4. استفاده از VPN در داخل VPS ها

1.1.5. استفاده از سیستم داخلی، صرفا برای جمع آوری اطلاعات بدون اشکال است

1.1.6. عدم نصب نرم افزارهای ناشناس

1.1.7. رعایت دستورالعمل معاونت سایبری در خصوص امنیت سیستم ها **(بسیار مهم)**

1.2.مستند سازی

1.2.1. تمام اقدامات و روش های استفاده شده باید به صورت قابل بهره برداری توسط سایرین در حین انجام پروژه ثبت گردند و به بعد از پروژه موکول نشود

1.2.2. گزارشات فنی باید در قالب های تعریف شده معاونت نوشته شود (نیاز به توجیه)

1.2.3. با توجه به اینکه قالب های موجود با دید صرفا وب نوشته شده است، در صورتی که قالب ها نیاز به اصلاح بر اساس بر اساس آورده های جدید را داشت، می توانند اصلاحات مورد نظر را اعمال نمایند

1.2.4. گزارش روزانه از اقدامات انجام شده باید به صورت مکتوب و در قالب تحویلی نوشته و به صورت روزانه به تایید آقای هادیان برسد

1.2.5. استفاده از نرم افزار X-mind به پیاده سازی ایده های ذهنی و مشخص کردن مسیر پروژه کمک بسیاری خواهد نمود

1.3.فضای کاری سایبری در گذشته و انتظارات از شبکه

1.3.1. مراحل کار در حال حاضر اکثرا نفوذ از طریق وب بوده که بر اساس مراحل CEH، افراد اقدام به نفوذ می نمایند که در این مسیر از ابزارهایی که ممکن است یک سایت باشد (مثل dnsdumpster) یا ابزار نصبی باشد مثل Nmap استفاده می نمایند که نیازمند توضیح این موارد توسط فرد فنی می باشد

1.3.2. از تیم شبکه انتظار می رود که علاوه بر مسیر هایی که در حال حاضر افراد فنی طی می نمایند درگاه های جدیدی برای نفوذ پیشنهاد دهند که گستره دید افراد فنی اضافه شود تا پروژه ها خروجی بهتری پیدا نمایند.

1.3.3. همچنین یکی از اهداف مجموعه اقدامات، تقویت دانش فنی تیم شبکه در خصوص نفوذ می باشد که در آینده به صورت یک تیم مستقل اقدام به انجام پروژه نمایند.

2. پیشنهاد پروژه

پیشنهاد می شود پروژه ذیل به منظور شروع فعالیت تیم شبکه به عنوان بازوی تیم سایبری در نظر گرفته شود:

2.1. عنوان

2.1.1. نفوذ به شرکت LADPC

2.2. اهداف

2.2.1. ایجاد اخلال گسترده در زیرساخت خدمات الکترونیک دولتی

2.2.2. ارتقاء علمی مجموعه با ارائه درگاه های جدید برای نفوذ به هدف

2.3. فازبندی

2.3.1. دریافت مستندات آماده شده توسط مرکز مطالعات در خصوص معرفی LADPC

2.3.2. جلسه با مرکز مطالعات جهت ارائه مستندات معرفی LADPC

2.3.3. شناخت بیشتر LADPC با هدف راستی آزمایی موارد مطرح شده در جلسه مرکز و اینکه آیا نفوذ به این شرکت ما را به هدف اصلی یعنی "اخلال در زیرساخت خدمات الکترونیک" می رساند یا خیر

2.3.4. جمع آوری اطلاعات از هدف با دید "غیر از وب" (شناسایی روش ها و درگاه های نفوذ علاوه بر وب و اقدام فنی بر اساس آن)

2.3.5. اقدام فنی جهت نفوذ و کسب دسترسی

2.3.6. تصمیم گیری در خصوص دسترسی های گذشته از LADPC و CT به منظور استفاده جهت افزایش دسترسی و نفوذ به شبکه داخلی

2.4. نکات

2.4.1. به منظور پیشرفت سریع تر در ابتدای پروژه دریافت مشاوره از افراد فنی لازم می باشد

2.4.2. پیشنهاد می شود آقای رسولی به عنوان نیروی سایبری به این تیم ملحق شوند

2.4.3. در تمام موضوعات باید دید گذشته تیم سایبری باعث جهت دهی فکری به تیم شبکه شود

2.4.4. جلسه مستمر به منظور ارائه اقدامات انجام شده در طول مسیر پروژه باید برگزار شود