به نام خدا

مبانی رایانش امن

دکتر موزرانی

تکلیف اول

مهلت تحویل: جمعه ۱۳ فروردین ساعت ۲۳:۵۹

۱) حمله Arp Spoofing را همراه با ذکر جزئیات (MAC and IP address) توضیح دهید، سپس دو مورد از دلایل ایجاد این حمله و یک روش برای تشخیص آن را ذکر کنید.

- **سوالات عملی:**

۲) قصد داریم به ماشینی با سیستم عامل عمدا آسیب پذیر Metasploitable 2.0 نفوذ کنیم. این ماشین را می توانید از این قسمت دانلود نمایید.

در ابتدا این سیستم عامل را بر روی ماشین مجازی نصب و اجرا کنید به علاوه سیستمی به عنوان مهاجم (ترجیحا Kali linux) انتخاب کرده و مراحل زیر را به صورت گام به گام انجام دهید.

۱- گام اول برای حمله یافتن IP address سیستم قربانی می باشد اینکار را بدون مراجعه به ماشین قربانی و صرفا از طریق سیستم مهاجم انجام دهید. (می توانید از ابزار nmap استفاده کنید)

۲- سیستم عامل آسیب پذیر Metasploitable دارای اپلیکیشنی با نام Vsftpd است که از نوعی آسیب پذیری تحت عنوان Back Door (درب پشتی) برخوردار است. exploit این آسیب پذیری در ابزار Metasploit موجود می باشد. (این ابزار به طور پیش فرض بر روی kali linux نصب بوده و قابلیت نصب بر روی سایر سیستم عامل ها همچون windows, ubuntu را نیز دارد) به کمک این exploit به سیستم قربانی نفوذ کرده و یک دسترسی shell به سیستم قربانی بگیرید.

۳- پس از گرفتن دسترسی به shell با استفاده از دستور whoami تعیین کنید به عنوان چه کاربری در سیستم قربانی دسترسی دارید. سپس تلاش کنید پسورد آن را تغییر دهید. آیا می توانید پسورد را تغییر دهید ؟ چرا ؟

۴- تلاش کنید منشاء آسیب پذیری این برنامه را بیابید. (این قسمت اختیاری و حاوی نمره اضافه است.)

۳) سیستم Bob آسیب‌پذیر است. در یک دایرکتوری محتوای فایل flag.txt وجود دارد که برای یافتن آن، سطح دسترسی کاربر باید به سطح دسترسی root افزایش پیدا کند. از VulnHub سیستم Bob را دانلود کرده و با استفاده از ابزارهای virtualization همچون vmware player آن را اجرا کنید.

- کاربرد فایل robots.txt در وب سایت ها را توضیح دهید. تحت چه شرایطی منجر به آسیب پذیری می‌شود؟

(راهنمایی: می‌توانید از سیستم عامل kali linux استفاده کنید و برای رسیدن به سطح دسترسی root ابتدا باید از ماشین Bob یک shell موفق گرفته و سپس سعی کنید password حساب Bob را بدست آورید.)

۴) با استفاده از ابزار BeEF و hook مرورگر قربانی می‌خواهیم یک trojan در سیستم هدف نصب کنیم و آن را persistent قرار دهیم.

برای این کار ابتدا یک trojan ساخته سپس به روشی دلخواه (ex : fake notification) باعث نصب trojan شوید.

- درصورت ایجاد DNS spoofing نمره اضافه محسوب می‌شود:

با توجه به آنکه فایل های وب سرور در دایرکتوری /var/www/html ذخیره می‌شود، پس یک سایت دلخواه را انتخاب کنید (ex: google.com)، محتویات آن را در index.html قرار دهید و سپس با ابزاری مانند Ettercap به محض آنکه قربانی وارد سایت مذکور شد به IP وب سرور حمله کننده redirect شود. (به هر web server مناسبی می‌توان redirect کرد اما در این تمرین از local web server استفاده می‌کنیم).

۵) در این سوال قصد داریم یک نوع از حملات MITM معروف به Arp Spoofing را که در سوال ۱ از شما خواسته شده بود ، پیاده سازی و عملیاتی نماییم. برای این امر لازم است شما یک اسکریپت به زبان پایتون بنویسید که به عنوان Arp Spoofer عمل کند.

(اسکریپ نوشته شده را علاوه بر توضیح و تست در ویدئو در فایلی تحت عنوان arp_spoofer.py ضمیمه تکلیف کرده و در سامانه بارگذاری کنید)

(راهنمایی : می توانید از کتابخانه scapy برای نوشتن ماژول Arp Spoofer استفاده نمایید.)

لطفًا به نکات زیر توجه نمایید:

- در صورت وجود سوال و یا ابهام، میتوانید به ایمیل های زیر پیام دهید:

Sara.br1378@gmail.com (سارا برادران)

ae.naderi@gmail.com (عاطفه نادری)

- برای هر یک از سوالات عملی به صورت جداگانه حتماً مستند تهیه نمائید؛ از مراحل حل و اجرای آن، یک ویدیو با صدای خودتان تهیه نمایید. انجام تمام مراحل را به شکل دقیق توضیح دهید و در حین انجام کار چرایی و چگونگی هر مرحله را بیان نمایید.
- تکالیف را در سامانه تحویل دهید.

سلامت و موفق باشید.