دانشگاه صنعتی اصفهان
مبانی رایانش امن (نیمسال دوم ۱۳۹۹)

تکلیف اول

مریم سعیدمهر
شماره دانشجویی : ۹۶۲۹۳۷۳

I. سوال تئوری

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

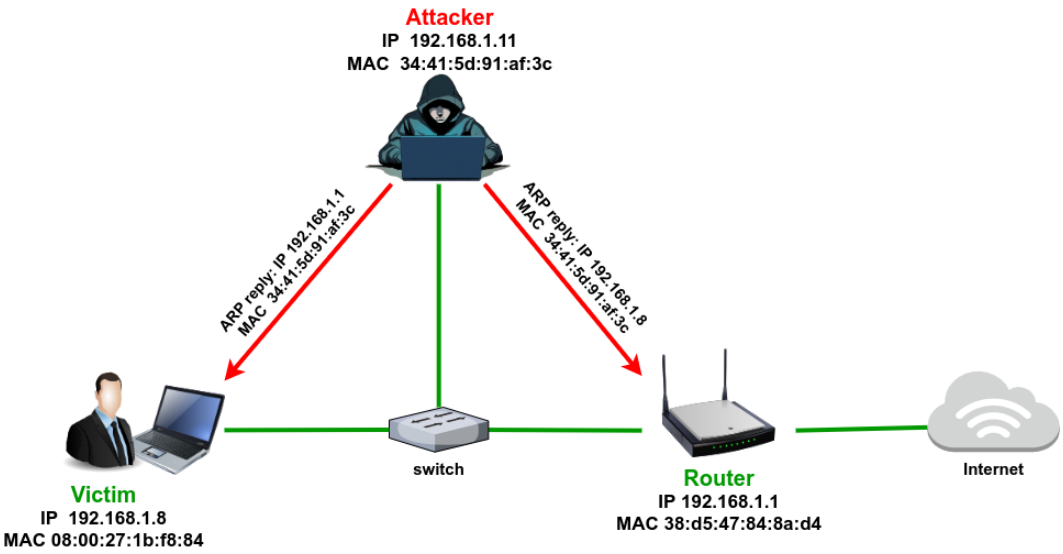
پروتکل Address resolution protocol (ARP) عمل تبدیل IP به MAC را برای ما انجام می دهد. نحوه کارکرد آن بدین صورت است که درخواست هایی در شبکه پخش می شود که آیا IP شما ***.***.***.*** است؟ اگر درست است مک خود را ارسال کنید.در همین حین تمامی کلاینت های شبکه IP خود را چک می کنند که در صورت درست بودن یک پاسخ همراه مک به فرستنده ارسال می کنند.

برای این که این درخواست پیوسته در شبکه ارسال نشود و ترافیک بیهوده ایجاد نشود.هر کلاینت یکبار این درخواست را ارسال کرده و سپس جواب‌های ارسالی را بصورت یک جدول در Cache ARP نگه داری می کند. این جدول شامل Mapping بین IP و MAC می باشد. هر زمان که بسته ای به یک کلاینت در یک شبکه داخلی ارسال می شود، باید از Gateway عبور کند سپس Gateway با استفاده از ARP، آدرس MAC کلاینتی که بسته به آن مربوط می شود را با استفاده از IP موجود در بسته پیدا کرده و آن بسته را به کلاینت مورد نظر ارسال می کند.
دو ویژگی این پروتکل که منجر به اشکالات امنیتی میشود و نوعی آسیب پذیری است که در این حمله از آن سواستفاده میشود به شرح زیر است :

۱. تمام پکت های این پروتکل چه از نوع request و چه response در این پروتکل Trusted تلقی میشوند یعنی اگر کسی به دروغ بگه MAC معادل IP من فلان مقدار است این پروتکل به حرف او اعتماد میکند و این زوج را در خود cache میکند.

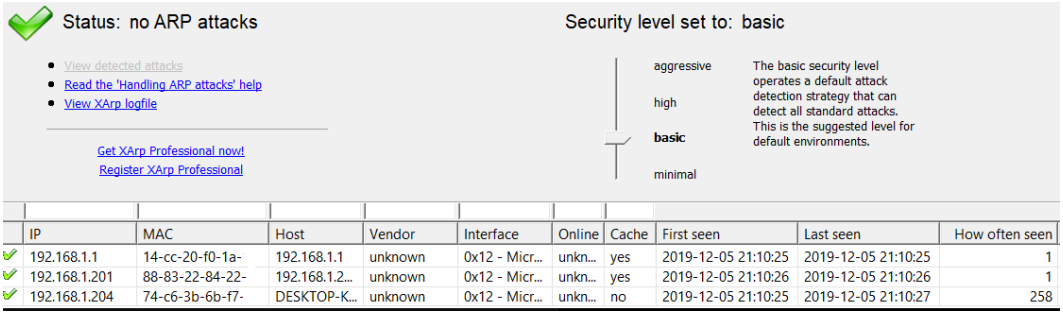
۲. کلاینت ها تمام ARP Reply ها را در ARP Table ذخیره میکنند حتی اگر قبل از آن هیچ ARP Request نفرستاده باشند.

در نهایت با استفاده از همین دو ویژگی (در اینجا آسیب پذیری هم واژه مناسبی هست!) میتوان حمله ARP Spoofing را انجام داد. روند آن در شکل ۱. آورده شده است (همراه با ذکر جزییات)



شکل ۱: ARP Spoofing

همانطور که در شکل ۱. پیداست در حمله ARP Spoofing یک Attacker با ارسال دو ARP Reply این حمله را انجام میدهد.
یک ARP Reply به Victim میفرستد و به او میگوید که "من Router هستم."
یک ARP Reply به Router میفرستد و به او میگوید که "من Victim هستم."
به این ترتیب ارتباط قربانی و روتر که قبلا از طریق سوییچ (در شکل) انجام میشد الان از طریق سیستم حمله‌کننده انجام میشود و لذا حمله‌کننده تسلط کامل در ارتباط قربانی و شبکه اینترنت دارد(مگر اینکه رمزنگاری انجام شود و به این ترتیب محتوای plaintext را از حمله‌کننده پنهان کرد)
روش های مختلفی برای شناسایی حمله ARP Poisoning وجود دارد. Command Prompt ویندوز، برنامه هایی مانند Snort ، ArpWatch ، XArp ArpAlert، و ... قابلیت شناسایی این نوع حملات را دارند.
اگر به اینکه کامپیوتر شما مورد حمله ARP Poisoning قرار گرفته یا خیر مشکوک هستید، یک راه ساده استفاده از Command Prompt است. با استفاده از دستور arp -a می توانید ARP Table خود را مشاهده کنید.
در این جدول اگر دو دستگاه با آدرس IP های مختلف دارای آدرس MAC یکسانی باشند آنگاه احتمالا کامپیوتر شما مورد حمله ARP Poisoning قرار گرفته است. البته این موضوع را نمی توان با قطعیت بیان کرد زیرا در بعضی مواقع در برخی روترها آدرس IP ابتدا و انتهای آن با یک آدرس MAC در ARP Table ذخیره می شود. این مورد یکی از استثناها می باشد.مشابه این سناریو در دستگاه های لینوکسی و مک نیز قابل اجراست اما برای دستگاه های اندرویدی نیاز به دسترسی روت خواهید داشت.
یا مثلا ابزار قدرتمند XArp : این ابزار پیشرفته برای لینوکس و ویندوز منتشر شده است که در Background اجرا شده و حملات را به طور آنی شناسایی می کند.



شکل ۲: برنامه XArp

با تنظیم Security Level به minimal یا basic یا high و یا aggressive می توانید حساسیت برنامه را تنظیم کنید

II. سوالات عملی

به طور کلی ، کلیه مستندات مربوط به تکلیف اول از طریق این لینک در دسترس است.

۱. vsftpd 2.3.4 Backdoor vulnerability in Metasploitable 2.0

تمامی قسمت های این سوال (ازجمله بخش اختیاری) در ویدیو توضیحاتم پوشش داده شده است.
ویدیو از طریق این لینک قابل دسترس است.

۲. Bob

تمامی قسمت های این سوال در ویدیو توضیحاتم پوشش داده شده است.
ویدیو از طریق این لینک قابل دسترس است.

۳. Trojan using BeEF and DNS spoofing

تمامی قسمت های این سوال (ازجمله بخش اختیاری) در ویدیو توضیحاتم پوشش داده شده است.
ویدیو از طریق این لینک قابل دسترس است.

۴. Arp Spoofer using python (scapy library)

تمامی قسمت های این سوال در ویدیو توضیحاتم پوشش داده شده است.
ویدیو از طریق این لینک قابل دسترس است.
اسکریپت نوشته شده به زبان پایتون نیز در فایل آپلود شده در سامانه ضمیمه شده است. همچنین از طریق این لینک نیز در دسترس است.