



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ANALÝZA HTTP NEZABEZPEČENEJ KOMUNIKÁCIE

AUTOR PRÁCE

AUREL STRIGÁČ

BRNO 2024

Obsah

1	Teoretický úvod	2
1.1	HTTP	2
1.2	Man-in-the-Middle (MitM) útok	2
2	Popis realizácie	3
2.1	Konfigurácia siete z pohľadu útočníka	3
2.2	Povolenie smerovania IP	3
2.3	Sledovanie a manipulácia s paketmi	3
2.4	Preposielanie paketov	4
2.5	Monitorovanie a úpravy prevádzky	4
3	Zhodnotenie výsledkov	5
	Literatúra	6

Kapitola 1

Teoretický úvod

1.1 HTTP

Hypertext Transfer Protocol[1] (HTTP) je základný aplikačný protokol, ktorý sa používa na prenos informácií na webe. HTTP funguje na princípe protokolu požiadaviek a odpovedí medzi klientom (ako je napríklad webový prehliadač) a serverom, ktorý obsahuje požadované zdroje, ako sú webové stránky a obrázky. HTTP neposkytuje šifrovanie dát, čo znamená, že všetky dáta odosielané medzi prehliadačom a webovým serverom sú prenášané vo forme, ktorá je čitateľná pre každého, kto má prístup k sieti. Práve táto vlastnosť z neho robí ideálneho kandidáta na *Man-in-the-Middle* útok.

1.2 Man-in-the-Middle (MitM) útok

Útok typu *Man-in-the-Middle*[4] (MitM) je bezpečnostný útok, kde útočník tajne preberá komunikáciu medzi dvoma stranami, ktoré si myslia, že priamo komunikujú medzi sebou. Útočník môže počas tohto procesu odpočúvať, zaznamenávať alebo dokonca upravovať prenášané dáta.

Tento typ útoku sa môže vyskytnúť v rôznych sieťových vrstvách a je obzvlášť nebezpečný v prostrediach, kde sú dáta prenášané bez šifrovania, ako je to v prípade protokolu HTTP. Úspech MitM útoku závisí od schopnosti útočníka infiltrácie do komunikačného toku, čo môže byť dosiahnuté technikami ako ARP spoofing, DNS spoofing, alebo využitím nezabezpečených Wi-Fi sietí.

Kapitola 2

Popis realizácie

2.1 Konfigurácia siete z pohľadu útočníka

Pri realizácii MITM útoku môže útočník naraziť na výzvy pri prístupe k sieťovej konfigurácii, najmä bez administratívnych práv. Hoci útočník nemôže priamo meniť IP adresy, DHCP nastavenia alebo pravidlá firewallu na cieľových zariadeniach, môže využiť techniky na manipuláciu s týmito konfiguráciami na úrovni siete. Jedným z prístupov je ARP spoofing, ktorý mu umožňuje presmerovať sieťový tok na svoje zariadenie bez nutnosti zmeny konfigurácie na cieľových zariadeniach.

Ďalej, napríklad, útočník môže zneužiť nesprávne nastavenie alebo slabiny v protokole DHCP, čo umožňuje vykonávať DHCP spoofing. Toto môže viesť k tomu, že všetka sieťová komunikácia obete prechádza cez útočníka.

Okrem toho, ak má útočník fyzický prístup k sieťovej infraštruktúre alebo k správcovským nástrojom siete, môže manipulovať s pravidlami smerovania alebo firewallu tak, aby odchytil alebo zmenil smerovanie sieťového toku. Táto úroveň prístupu však zvyčajne vyžaduje vysoký stupeň oprávnení alebo zraniteľnosť v sieťovej infraštruktúre.

2.2 Povolenie smerovania IP

Povolenie IP smerovania je kľúčovým krokom pre konfiguráciu zariadenia, ktoré má fungovať ako smerovač alebo ako prostriedok pre útok typu Man-in-the-Middle (MITM). V systéme Linux je možné povoliť smerovanie IP dočasne zmenou hodnoty v systémovom súbore. Konkrétne, príkazom `echo 1 > /proc/sys/net/ipv4/ip_forward` sa IP smerovanie aktivuje do nasledujúceho reštartu. Pre trvalé zmeny sa odporúča upraviť súbor `/etc/sysctl.conf` a nastaviť `net.ipv4.ip_forward = 1`, čo zabezpečí, že zmena prežije reštart systému. V operačnom systéme Windows je nutné smerovanie povoliť zmenou registra alebo použitím PowerShellu, čo vyžaduje administrátorské práva.

2.3 Sledovanie a manipulácia s paketmi

Sledovanie a manipulácia s paketmi umožňuje nielen pasívne pozorovanie sieťovej komunikácie, ale aj aktívne zasahovanie do prenášaných dát. V tomto prípade, keď sú ARP odpovede falšované, obete a gateway si myslia, že komunikujú priamo medzi sebou, ale v skutočnosti ich pakety prechádzajú cez útočníka. Nástroje ako Ettercap a Bettercap ponúkajú funkcionality pre ARP spoofing, čo mení to, ako zariadenia identifikujú smerovanie v sieti.

Pred vykonaním ARP spoofing útoku je však potrebné zistiť IP adresy zariadení v sieti. Tu prichádza na rad nástroj Nmap[3], ktorý môže byť použitý na vykonanie sieťového skenovania a identifikáciu aktívnych zariadení. Príkazom `nmap -sn 192.168.1.0/24` možno rýchlo zistiť, ktoré zariadenia sú online v danej podsieti. Po identifikácii IP adres gateway a cieľového zariadenia môže byť Ettercap[2] použitý na vytvorenie falošných ARP odpovedí príkazom `ettercap -T -M arp /gateway IP/ /victim IP/ -i interface`, kde Bettercap poskytuje podobnú funkcionality prostredníctvom jednoduchších príkazov v interaktívnej konzole. Toto umožňuje útočníkovi presmerovať sieťovú komunikáciu cez svoje zariadenie a manipulovať s prenášanými dátami.¹

2.4 Preposielanie paketov

Preposielanie paketov je základným mechanizmom v smerovačoch a prostriedkoch pre MITM útoky. Po povolení smerovania IP, operačný systém automaticky začne preposielať pakety medzi sieťovými rozhraniami podľa konfigurácie smerovacej tabuľky. Tento proces je transparentný a nevyžaduje ďalšie zásahy, ak je zabezpečené správne nastavenie siete.

2.5 Monitorovanie a úpravy prevádzky

Pre pokročilé úpravy a analýzu paketov možno použiť nástroj Scapy, ktorý umožňuje programovanie vlastných skriptov pre manipuláciu s paketmi. Skripty môžu zachytávať, analyzovať a modifikovať pakety na úrovni bajtov, čo umožňuje zmeny v obsahu paketov alebo testovanie aplikačných reakcií na modifikované dáta.

208.10.658605	128.103.64.74	10.0.0.9	HTTP	219 HTTP/1.1 304 Not Modified
---------------	---------------	----------	------	-------------------------------

Obr. 2.1: Ukážka zachyteného paketu

```

Transmission Control Protocol, Src Port: 80, Dst Port: 51114, Seq: 167, Ack: 1153, Len: 168
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n
      [HTTP/1.1 304 Not Modified\r\n
        [Severity Level: Chat]
        [Group: Sequence]
        [Response Version: HTTP/1.1]
        [Status Code: 304]
        [Status Code Description: Not Modified]
        [Response Phrase: Not Modified]
        [Date: Wed, 01 May 2024 13:24:40 GMT\r\n
        [Server: Apache\r\n
        [Connection: Keep-Alive\r\n
        [Keep-Alive: timeout=5, max=99\r\n
        [ETag: "309e-583e755d10900"\r\n
        \r\n
        [HTTP response 2/2]
        [Time since request: 0.116474000 seconds]
        [Raw request in frame: 472]
        [Raw response in frame: 170]
        [Request in frame: 202]
        [Request URI: http://access.opennet.net/]
  0000 00 17 ad bb 00 00 4b 54 54 50 27 31 2e 31 20 83 04 Not Modified
  0001 30 34 20 4e 6f 74 20 4d 6f 64 69 65 69 65 64 6d 04 Not Modified
  0002 0a 44 61 74 65 3a 20 57 65 64 2c 20 30 31 20 4d Date: Wed, 01 M
  0003 61 79 20 32 30 32 34 20 31 33 3a 32 34 3a 34 30 ay 2024 13:24:40
  0004 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT Se
  0005 61 63 68 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ache Co
  0006 3a 20 4b 65 65 70 2d 41 6e 69 76 65 6d 0a 4b 65 : Keep-A
  0007 65 70 2d 41 6e 69 76 65 3a 20 74 69 6d 65 6f 75 ep-A
  0008 74 3d 35 2c 20 6d 61 78 3d 39 39 0d 0a 45 54 61 t=5,
  0009 67 3a 20 22 33 30 39 65 2d 35 38 33 65 37 35 35 gi "309e-583e755
  0010 0a 31 30 39 30 22 0d 0a 0d 0a d10900"

```

Obr. 2.2: Viditeľný obsah zachyteného paketu

¹Všetky ukážky použitia jednotlivých príkazov sú iba orientačné. Ich konkrétne použitie sa bude, s najväčšou pravdepodobnosťou, líšiť.

Kapitola 3

Zhodnotenie výsledkov

V rámci tejto práce som úspešne demonštroval praktickú realizáciu *Man-in-the-Middle* (MitM) útoku na nešifrovaný *HTTP* protokol. Mojm hlavným cieľom bolo pasívne monitorovanie komunikácie, čo mi umožnilo získať hlboký vhlad do prenášaných dát medzi klientom a serverom. Tento prístup mi umožnil identifikovať a zaznamenať rôzne typy informácií, čo podčiarkuje zraniteľnosť nešifrovaného *HTTP* spojenia voči odpočúvaniu.

Okrem monitorovania, *MitM* útok poskytuje širšie možnosti zasahovania do prenášanej komunikácie. Medzi ďalšie potenciálne akcie patria:

- **Modifikácia dát:** Útočník môže meniť obsah požiadaviek alebo odpovedí v reálnom čase, čo môže viesť k škodlivým aktivitám ako je šírenie malvéru, falšovanie údajov, alebo manipulácia s transakciami.
- **Redirekcia požiadaviek:** Môžu byť presmerované na škodlivé stránky, čím sa zvyšuje riziko podvodov a phishingu.
- **Odcudzenie osobných údajov:** Odhalenie citlivých údajov ako sú prihlasovacie mená, heslá, čísla kreditných kariet alebo iné osobné informácie.

Táto práca potvrdila, že použitie nešifrovaného *HTTP* v dnešnej dobe predstavuje vážne bezpečnostné riziká. Výsledky naznačujú kritickú, ale aj tak nie nevyhnutnú, potrebu prechodu na *HTTPS*, ktorý cez šifrovanie zabezpečuje ochranu dát prenášaných na internete. Vzhľadom na neustále sa zvyšujúce hrozby v kybernetickom priestore je odporúzané prijímať adekvátne bezpečnostné opatrenia a šíriť povedomie o dôležitosti šifrovania pri zachovaní súkromia a integrity online komunikácie.

Literatúra

- [1] FIELDING, R. T. a RESCHKE, J. F. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. 2014, č. 7231. DOI: 10.17487/RFC7231. Dostupné z: <https://datatracker.ietf.org/doc/html/rfc7231>.
- [2] LINUX, K. *Ettercap* [<https://www.kali.org/tools/ettercap/>]. 2024. Otvorené 01.05.2024.
- [3] LYON, G. a PROJECT, N. *Nmap: the Network Mapper* [<https://nmap.org/>]. 2023. Otvorené 01.05.2024.
- [4] TECHTARGET. Man in the Middle (MitM) Attack. [<https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM>]. 2023. Otvorené 01.05.2024.