VOIP Security and Asterisk

Peter Šuľaj

ZLÉ ZABEZPEČENIE STÁLO MAJITEĽKU MILIÓNY ČESKÝCH KORÚN

pre študentov TUKE

- Za 3 dni 2 milióny korún
- Blanka Pribylová – prevádzkarka hotela vo Valašskom Meziříčí

AKO OKRÁDAŤ CEZ VOIP ?

- „Prémiové čísla“ 1 – 2 Eur/min

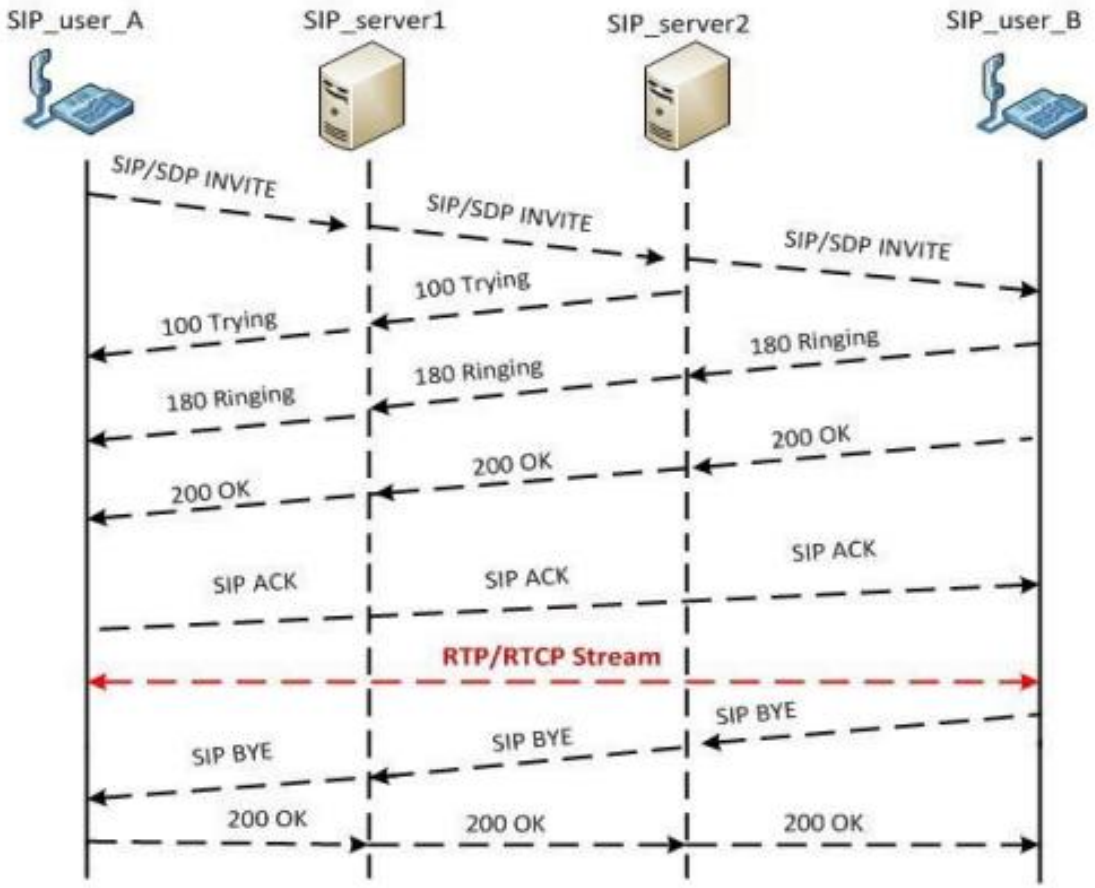
IDENTIFIKÁCIA ÚČASTNÍKOV V SIETI SIP

Telefónna „adresa“ môže teda vyzerať nasledovnými spôsobmi:

- SIP: jano@frima.sk – ako FQDN (Fully Qualified Domain Name) mená
- SIP: 123456@gateway.com; user=phone, ako E.164 (PSTN) adresy
- SIP: 123456; password=zmen@192.100.1.4 , SIP: jano@192.100.1.4 ako kombinácia IP adresy a mena

IDENTIFIKÁCIA ÚČASTNÍKOV V SIETI SIP

Dvaja SIP klienti môžu navzájom komunikovať priamo ak poznajú svoje URL adresy.



ÚTOKY NA SIP

Najčastejšie útoky na SIP

Záplava SIP Invite

- typ DDoS proti aplikačnej vrstve, na ktorej SIP pôsobí.
- záplava SIP serverov správami od neregistrovaných účastníkov.
- začne vysielať množstvo INVITE správ v krátkom časovom rozpätí a v rôznych dávkach, tak aby nebolo možné rozoznať pravdivé dáta od tých, ktoré spadajú pod DDoS útok.

Záplava SIP REGISTER

- modifikovaná správa REGISTER s neplatným prihlasovacím menom a heslo.
- Po obdržaní správy UNAUTHORIZED zo strany servera útočník vygeneruje tzv. MD5 digest,
- SIP server sa pritom preťažuje tým, že musí porovnávať prijatý MD5 hash zo záznamami o užívateľoch na serveri

DoS pomocou správ BYE

- správou BYE zvyčajne UA ukončuje spojenie z iným UA.
- Ak dokáže útočník podvrhnúť túto správu na základe údajov získaných z prebiehajúcej komunikácie, tak ju dokáže prerušiť počas jej priebehu a predčasne ukončiť spojenie medzi komunikujúcimi stranami

Preťažená ústredňa

Inter-Asterisk eXchange (IAX)

- signalizačný protokol - alternatíva k protokolom SIP a H.323..
- je open source,
- prenos signálového aj médiového toku používa UDP port 4569, čo prináša niekoľko výhod,
- IAX2.
- „trunk", povoľuje viacerým dátovým tokom spojenia do jedného spoločného dátového toku – trunku, pričom výsledný datagram je reprezentovaný jedným spoločným záhlavím, čo znižuje preťaženie spojené s prideľovaním a distribúciou individuálnych kanálov.

Bezpečnosť v protokole IAX

Ponúka na výber z 3 možností autentizácie: plain text, MD5 (hash), RSA šifrovacie kľúče.

Tie však samozrejme nemajú vplyv na samotný tok dát, ktorý je zabezpečený pomocou šifrovania a prenosu cez VPN siete a riešený na iných vrstvách sieťovej hierarchie.

Vo verzii IAX2 bola pridaná možnosť šifrovania dátového toku medzi koncovými bodmi za použitia dynamickej výmeny kľúčov pri zostavovaní hovoru

(pre Asterisk príkaz encription = aes128).

Ako ďalšie obranné mechanizmy uvádzam protokoly IPsec a DTLS.

ÚTOKY NA IAX

Najčastejšie útoky na IAX

Odhalenie užívateľských mien

- môžeme zistiť tieto prihlasovacie údaje buď metódou postupného odhadu užívateľských mien alebo slovníkovým útokom

Slovníkové útoky

- Rozdelujeme na offline a online

IAX Man-in-the-Middle

- Musi zabezpečiť komunikáciu medzi IAX a Asterisk ústrednou

Preťažená ústredňa

For internal use only !!

Komplexné zabezpečenie IP PBX Siemens

ÚTOKY NA IP PBX ASTERISK

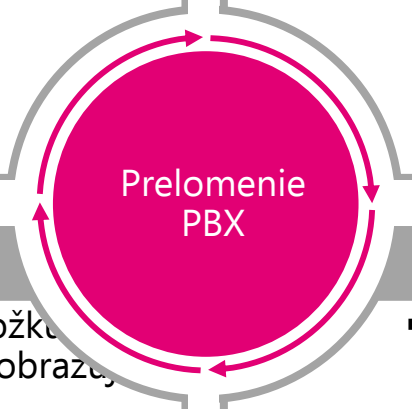
4 Hlavné útoky na IP PBX Asterisk

Slovníkové útoky

- obísť šifrovací alebo autentifikačný mechanizmus pomocou určenia kľúča alebo frázy skúšaním najčastejších kombinácií rôznych slov

Brute force SIP útoky

- Tieto útoky majú tiež za úlohu prelomiť užívateľské prípadne serverové heslá.



Odhalenie a podvrhnutie Caller ID

- Tieto dva útoky sa zameriavajú na položku ID alebo inak ID volajúceho, ktoré sa zobrazuj na displeji prijímajúcej strany

Dialstring injection a SQL injection

- Je podobný útoku SQL injection proti databáze, v ktorých nie je vykonané dostatočné filtrovanie vstupných reťazcov.

SLOVNÍKOVÉ ÚTOKY

- predstavujú mechanizmus ako obísť šifrovací alebo autentifikačný mechanizmus pomocou určenia kľúča alebo frázy skúšaním najčastejších kombinácií rôznych slov.
- Asterisk odpovedá len “invalid peer” alebo “invalid password”.
- Útočník však potrebuje zistiť identitu aspoň jedného účastníka, aby mohol útok začať.
- Ako obranu je možné zablokovať útočníkovú IP adresu špecifikovaním príkazu iptables a nastavením pravidla Fail2ban [], ktorý skenuje logovacie súbory a zamietne IP adresu, z ktorej bolo generovaných príliš veľa pokusov.

- Ďalšou možnosťou obrany je používanie silných hesiel.

Brute force SIP útoky

využívajú hlavne nasledovné trhliny:

- Otvorené/nezabezpečené porty (napr. SSH port 22, SIP port 5060)
- Rovnaké alebo podobné názvy klapiek a užívateľských mien
- Zle navrhnuté heslo
- Tieto útoky spôsobujú pomerne veľkú množstvo pamäte počas priebehu útoku.
- Napadnutá môže byť aj len určitá časť spojenia.

Odhalenie a podvrhnutie Caller ID

- odcudzenie Caller ID užívateľa treťou stranou
- Mnoho systémov zvykne využívať Caller ID pre účely autentifikácie užívateľov..
- Pri odhalení Caller ID útočník zistí túto hodnotu a následne ju dokáže zmeniť na požadovanú.
- Pomocou telefónneho čísla dokáže útočník vyhľadať a zistiť rôzne Caller ID potenciálnych obetí týchto útokov

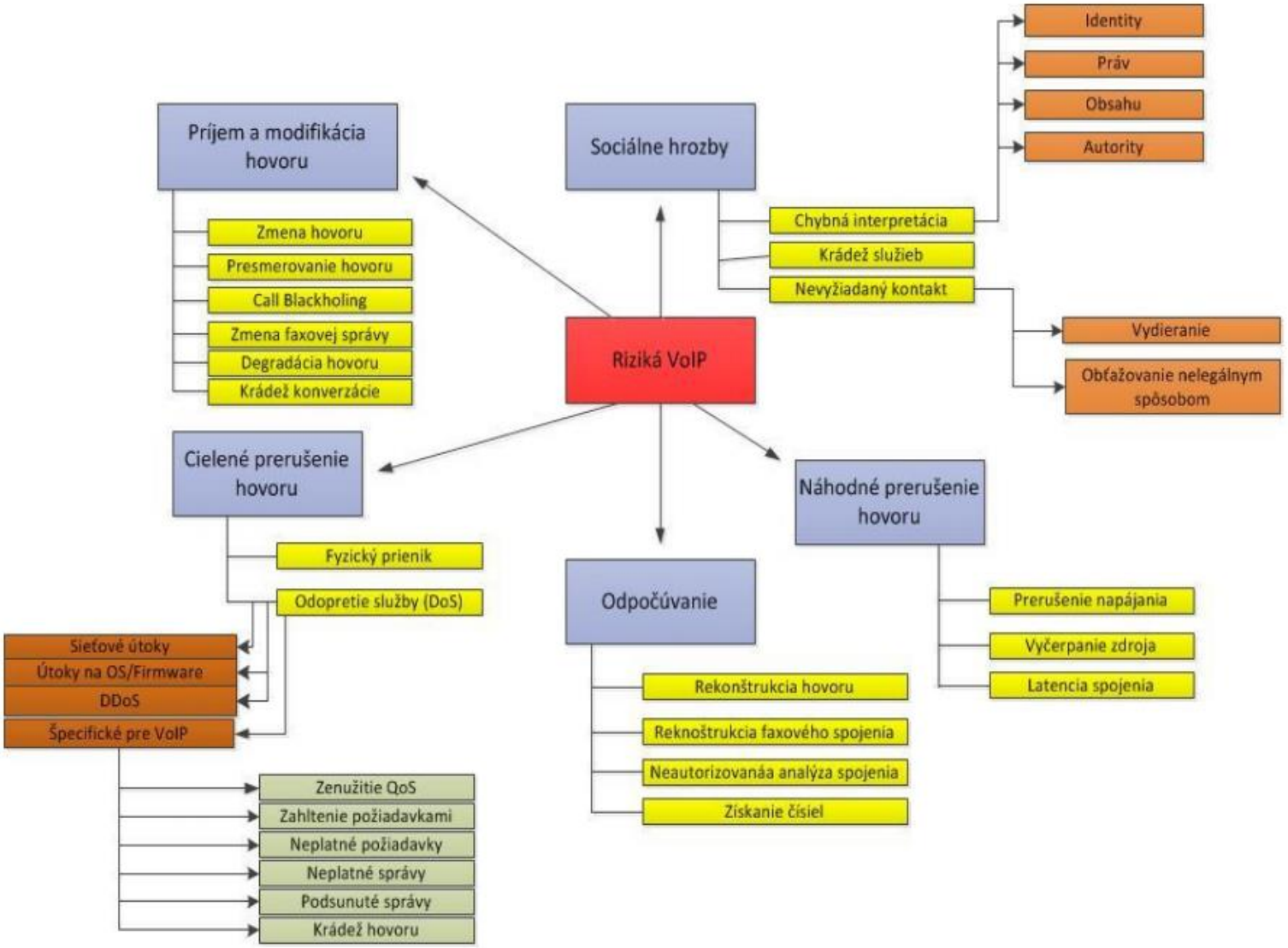
Dialstring injection a SQL injection

- publikoval v roku 2010 Olle Johansson.
- Obdoba SQL injection proti databáze, v ktorých nie je vykonané dostatočné filtrovanie vstupných reťazcov.
- Asterisk povoľuje veľkú znakovú sadu pri vytáčaní klapiek.
- Obrana -- > môže poslúžiť filtrovanie volacích reťazcov (dialstrings) zo všetkých VoIP kanálov predtým, ako sú poslané do volacieho plánu (dialplan).
- Na systém Asterisk ako aj na iné voľne dostupné IP PBX systémy ako napríklad FreePBX, Elastix existuje množstvo ďalších útokov,

For academy test only !!

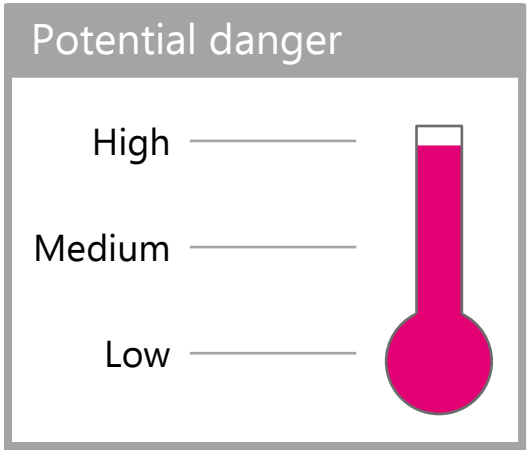
Hrozby a útoky v sieťach VoIP

Klasifikácia hrozieb a útokov podľa VOIPSA



Útoky na odoprenie služby - DoS

- Sposobuje dočasnú degradáciu služby alebo jej úplne odopretie.
- útok DoS môže spočívať v zahltení užívateľských staníc v rámci vnútornej siete veľkým počtom paketov rôznych veľkostí.
- IP telefóny môžu prestať pracovať ak napríklad prijmú UDP paket väčší ako 65534 bajtov na porte 5060 (štandardný UDP VoIP port).
- V protokole SIP sa môže jednať o útoky na proxy server za účelom jeho preťaženia.

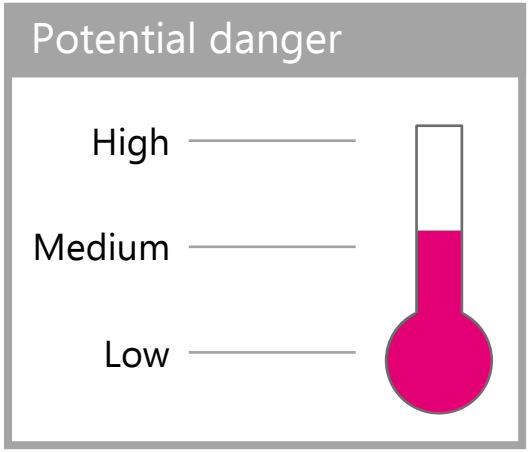


Niektoré z DoS útokov

- Modifikácia QoS – VLAN tag, ToS (Type of Service)
- Záplava volaním (Call Flooding) – DoS útok spočívajúci v posielaní veľkého počtu platných alebo neplatných správ/požiadaviek (napr. SIP INVITE, SIP REGISTER) pre zostavovanie hovoru na server. Prípade sa môže jednať o zaplavenie SIP servera po zostavení spojenia (ak už prebehla registrácia) požiadavkami typu SIP INFO, SIP NOTIFY.
- Záplava UDP – tento typ útoku je zameraný na záplavu a obmedzenie prenosovej kapacity spojenia.
- Pozmenené pakety (Malformed packets, protocol fuzzing) – ide o vytváranie rôznych typov paketov pre ten istý protokol, obsahujúce dáta, ktoré postupne tlačia špecifikáciu protokolu k zlomovému bodu. Táto metóda je známa ako tzv. fuzzing. Príklad modulu pre testovanie stability rôznych protokolov touto metódou je program ISIC. Odoslanie "fuzzing" paketu proti IP telefónu môže napríklad zapríčiniť to, že telefón prestane prijímať prichádzajúce hovory.
- Útoky proti infraštruktúre (DHCP, DNS, TFTP atď.) - v tomto prípade sa jedná o útoky proti infraštruktúrnym jednotkám ako DHCP server alebo DNS server, ktorých odstavenie resp. uvedenie do režimu offline znemožní komunikáciu takmer všetkým užívateľom, ktorý využívajú tieto služby.

Zachytenie a krádež spojenia

- útoky typu MiTM (Man in the Middle),voľne preložené “muž v strede” postavené protokole ARP, ktorý z IP adresy dokáže zistiť fyzickú MAC adresu zariadenia v sieti.
- Najčastejšie ARP poisoning , ktorý predstavuje jeden z najpopulárnejších spôsobov na odpočúvanie hovoru.
- V rámci tohoto útoku sa vykonáva aj útok MiTM, ktorý je jednou z možných súčastí.



Nástroje pre útok na ústredňu Asterisk

- Cain a Abel - silný nástroj pre ARP poisoning a VoIP špehovanie. Jeho účinnosť spočíva v tom, že automaticky vykonáva jednotlivé ARP požiadavky a vytvára ucelené správy o tom, aké data zachytil. Je určený pre OS Windows.
- ettercap – je ďalším silným MiTM nástrojom určeným hlavne pre distribúcie OS Linux ale aj pre Windows či Solaris. Ettercap však nedokáže pokryť toľko modelových situácií ako Cain a Abel, ako napríklad nahrávanie RTP streamov.
- dsniff – predstavuje Linuxovú aplikáciu pre útoky ARP poisoning programom, ktorý sa nazýva arpspoof. Dsniff nie až taký plnohodnotný program ako Cain a Abel alebo ettercap a na zabezpečenie IP smerovania a VoIP špehovania je potrebné využiť iné dostupné aplikácie.

Nástroje pre útok na ústredňu Asterisk

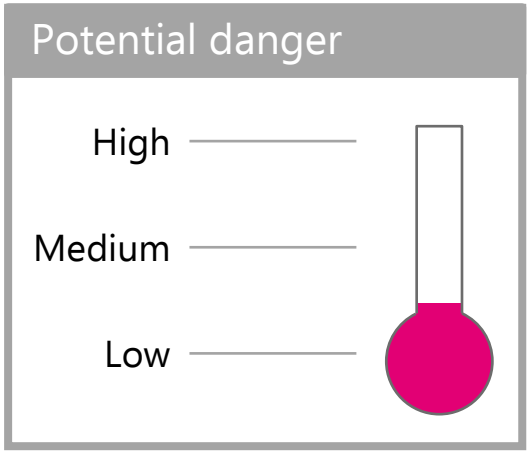
- Man in The Middle (MiTM) Tento útok nazývaný aj únosom registrácie môžeme napríklad odvodiť z toho, že pole „From" v prostredí protokolu SIP, ktoré je súčasťou záhlavia SIP žiadosti o spojenie je možné ľubovoľne modifikovať.

For academy test only !!

Manipulovanie signalizácie a médiového toku

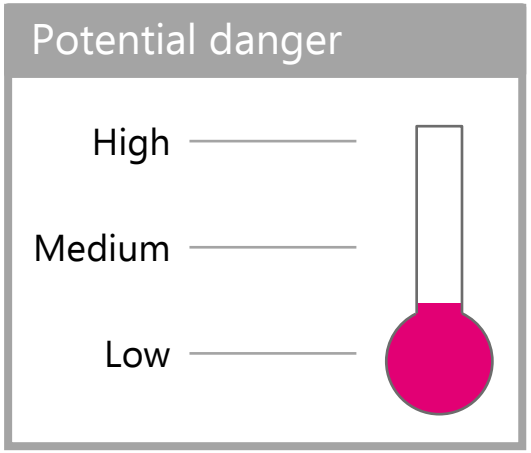
Odstránenie registrácie (Registration removal)

- IP telefóny sa zvyčajne registrujú cez proxy server, ktorý vie kam má smerovať hovory.
- SIP môže proxy server zmeniť registračný interval v správe 200 OK.
- IP telefón nedokáže prijímať hovory.
- vymazať všetky registrácie vhodným modifikovaním správy REGISTER.
- Na tento účel je možne použiť napríklad program SiVuS, ktorý je voľne dostupný.



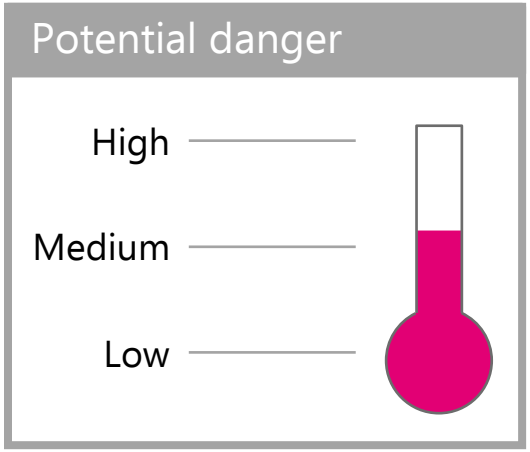
Útoky presmerovaním (Redirection Attacks)

- útočník monitoruje správu INVITE, konkrétne správy 301 a 302, ktoré dokáže využiť na presmerovanie odpovede smerom ku sebe a tak vlastne zamietnuť službu pre druhú stranu a vydávať sa za správnu komunikujúcu stranu



Zmena toku RTP (RTP Mixing)

- spočíva v pridaní nového audio toku do už existujúcej konverzácie, čím sa naruší jej plynulosť.
- Vloženie tohto zvuku môže mať za následok prepísanie toho existujúceho. Zmiešanie audio tokov spôsobí, že nové zvuky sa buď pridajú alebo splynú s tými ostatnými v závislosti ako hlasitosti, počtu slov a podobne.



For academy test only ☺

PROGRAMOVÉ PROSTRIEDKY PRE NAPADNUTIE PBX

Wireshark

- Wireshark je protokolový analyzátor, pôvodne nazývaný Ethereal, ktorý predstavuje užitočný nástroj pre zachytávanie a filtrovanie sieťovej komunikácie v počítačových sieťach.
- podieľa sa na zachytávaní signalizačných (SIP, IAX2) a transportných dát (RTP/UDP), ktoré následne analyzujeme.

Tshark

- terminálová forma programu Wireshark so všetkými možnosťami, ktorými Wireshark disponuje.
- Disponuje rozšírenými možnosťami nastavenia filtrácie podľa špecifických požiadaviek, ďalej možnosťami nastavenia časového intervalu alebo funkcionalitou dekódovania dát (napr. RTP pri VoIP).

Nmap

- vytvorená za účelom získavania dôležitých parametrov ako sú otvorené porty, IP adresy či rôzne sieťové a aplikačné služby.
- Na základe vstupných parametrov IP adresy a masky siete dokáže za pomerne krátku dobu zobraziť výsledky jednotlivo pre každú skenovaná IP adresu.

BYE Teardown

- využíva správu BYE protokolu SIP na ukončenie aktívnej relácie medzi volajúcimi účastníkmi.
- Na svoje fungovanie vyžaduje aby účastník zozbieral niekoľko potrebných údajov ako: Call ID, From Tag a To Tag.
- Všetky tieto parametre môžeme nájsť v odpovedi SIP 200 OK.
- Vyžaduje teda spoluprácu so sieťovými analyzátormi,

INVITE flooder

- princípom tejto aplikácie je zahltenie koncovej stanice alebo proxy servera veľkým počtom užívateľom definovaných správ INVITE, ktoré majú za následok degradáciu a významné zhoršenie kvality prebiehajúceho hovoru.
- Na svoje fungovanie potrebuje 4 základné povinné parametre: extension (klapka), target proxy IP (ip proxy servera), target source IP (zdrojová IP účastníka), počet paketov.

For academy test only !!

Experimentálne generovanie útokov

Analýza útokov odpočúvaním

- Hlavným účelom tohoto útoku je zachytiť jeden prípadne viac hovorov medzi úžívateľmi, ktoré sa uložia vo forme súboru .pcap -- > analýza a dekódovanie zvukového záznamu do formátu .raw
- Protokol SIP využíva na prenos hlasového toku transportný porotokol RTP pracujúci na UDP.
- Signalizácia a dátový tok sú v prípade SIPu oddelené, tak existujú aj dve skupiny portov, ktorými sú odlíšené. Pri volaní cez SIP sa na signalizáciu obvykle užívateľovi prideľuje port 5060 (prípadne 5061 SIP-TLS).
- Na dátový tok je pre RTP vygenerovaná hodnota portu od 10 000 po 15 000 v prípade IP 79XX na strane užívateľa. Ústredňa ma spravidla iný port.
- Protokol IAX2 používa na rozdiel od SIPu jeden štandardizovaný port 4569, ktorý sa využíva na signalizáciu aj prenos dátového obsahu. Ako transportný protokol je využitý UDP.

Útok odpočúvaním pre jeden SIP hovor

- Jednoduchý PHP skript, ktorý následne vykoná požadované operácie. Tie v tomto prípade použijú program Tshark a funkciu display_call, ktorej obdoba je využitá aj pri ostatných útokoch a má nasledujúcu formu:

```
function display_call($command) {
 $c = $command . " 2>&1";
 echo "<br /><pre>$c</pre><br />";
 flush();
 $output = shell_exec($c);
 echo "<pre>$output</pre>";
}
```

Útok odpočúvaním pre jeden SIP hovor

- Zachytený súbor je následne uložený do zvoleného priečinka odkiaľ k nemu môžeme pristupovať a čítať z neho potrebné údaje.
- Pomocou PHP príkazu echo sa do prehliadača zobrazia hlásenia o úspechu alebo neúspechu daného zachytávania a ďalšie prípadné pokyny pre užívateľa.
- Všetky parametre skriptu sú spracovávané metódou POST, ktorá sa stará o odoslanie dát na server a interpretovanie ich návratovej hodnoty.
- Celý proces sa užívateľovi zobrazí v tom istom okne odkiaľ spustil zachytávanie a to pomocou vnoreného rámca tzv. iframe, ktorý sa do okna prehliadača načíta po spustení zachytávania.

Prerušenie hovoru – Call drop attack

- útok je vykonávaný programom Teardown BYE, ktorý bol napísaný v jazyku Python a má pomerne jednoduchú príkazovú syntax
- Má povinné polia:
  - Interface - sieťové rozhranie (napr. eth0, ppp0), ktoré si užívateľ volí z ponuky
  - Extension – klapka, ktorú používa účastník v danom kontexte Asterisku
  - SIP proxy – IP adresa servera proxy, obvykle v paketoch uvedená aj ako zdrojová IP adresa účastníka
  - Target IP – cieľová IP adresa účatníka (v tomto prípade rovnaká ako SIP proxy)
  - Call ID – identifikátor hovoru, hodnota býva uvedená napríklad v správe INVITE
  - From Tag – hodnota tagu prichádzajúceho hovoru (zachytená v SIP 200 OK)
  - To tag – hodnota tagu volanej strany, ktorá sa vygeneruje po prevzatí hovoru volanou stranou
- zachytávanie prichádzajúcich SIP paketov, z ktorých sú najdôležitejšie správy INVITE a 200 OK.

Záplava volaním – INVITE flood attack

- Využívame INVITE flooder.
- Potrebujeme zachytiť niektorú zo správ INVITE, TRYING, RINGING, OK alebo ACK.
- Zahltenie cieľového uzla je možné aj v prípade ak komunikujúce strany aktuálne spolu nevolajú..

Skenovanie portov a IP adries

- Zisťovanie dostupných (aktívnych) IP adries a portov. K tomuto účelu je v práci využitý program nmap, ktorý na základe zvolených kritérií zisťuje dostupnosť a stav sieťových zariadení a uzlov.
- Ako hlavný a zároveň povinný parameter slúži cieľová IP adresa, prípadne aj celá sieť alebo podsieť, ktorých skenovaním sa získavajú užitočné informácie.
- vstupné parametre port, IP adresa a maska siete, na základe ktorých program nmap zaháji skenovanie siete.

ZABEZPEČENIE KOMUNIKÁCIE

Zabezpečenie komunikácie proti odposluchu

- šifrovanie pomocou protokolu SRTP, ktorý dnes už štandardne podporuje väčšina ústrední (napr. Asterisk, Cisco, Avaya),
- zabezpečí šifrovanie prenášaných RTP paketov, ale pred jeho samotným použitím musí medzi účastníkmi prebehnúť výmena šifrovacích kľúčov, najčastejšie použitím protokolu SDES, ktorý je súčasťou správy SIP.
- Kombinácia SRTP+SDES zvyčajne funguje s protokolom TLS, ktorý sa stará o bezpečné overenie učastníkov a doručenie kľúčov oprávnenej strane.
- Nie je rozšírený do korporátnej či firemnej sféry a podporuje ho len časť VoIP zariadení (SFLphone, Linphone).
- Náhrada --- > použitie tunelovacieho protokolu IPsec, ktorý kompletne znemožní potencionálnemu útočníkovi čo i len zachytiť prenášané hovorové dáta. Pri jeho implementácii však treba rátať s vyššími nárokmi na oneskorenie či prenosovú kapacitu, pretože využíva výpočetne zložité algoritmy (AES-CBC, AES-CTR), na zostavenie bezpečného a šifrovaného kanálu v rámci VPN siete.

Zabezpečenie proti útokom DoS

- Útok INVITE flood realizovaný a opísaný v prezentácii patrí medzi DoS.
- Sieťové zariadenia z kateorie NIPS (Network Intrusion Prevention Systems), ktoré detekujú a blokujú potencinálne aj reálne útoky tým, že sledujú všetky prechádzajúce (prípadne len vybrané) pakety a v prípade podozrenia zablokujú príslušný prenosový kanál.
- Používanie protokolov TCP s TLS namiesto UDP pri signalizácii k eliminái útokov typu INVITE flood či UDP flood, oddelenie hlasových tokov pomocou tzv. voice VLANs s filtrovaním MAC adries
- Odporúča sa používať iné hodnoty portov ako sú tie štandardné (SIP 5060, IAX2 4569).
- Vhodné je do siete implementovať napríklad SIP firewall, ktorý by sledoval signalizáciu prichádzajúcu od VoIP telefónov, prípadne ich softvérových ekvivalentov.

Ochrana pred manipuláciou signalizácie

- Vhodné použiť kombináciu protokolov TCP a TLS, aby bolo útočníkovi znemožnené správne odhadnúť parametre správ.
- Overením správy SIP BYE je možné zabrániť ukončeniu hovoru zo strany útočníka, pretože neoverená podvrhnutá správa BYE nebude príjemcom akceptovaná.
- V praxi sa však BYE správy overujú len málokedy.
- Na zvýšenie ochrany pre manipuláciou signalizácie je vhodné využívať funkcionalitu proxy serveru a vyhnúť sa tak priamemu nadviazaniu spojenia.

ĎAKUJEM ZA POZORNOSŤ !