BVK – zkouška teorie

1. **Kryptoanalýza se zabývá**
   - Metodami získávání otevřeného textu bez znalosti klíče
   - Zkoumáním odolnosti testovaného algoritmu

2. **Jakou hwashovací funkci používá metoda Digest Autentification**
   - MD5

3. **Která z následujících možností nepatří do fází(řetězců) Netfilter**
   - NAT
   - FILTER

4. **Který protokol definuje bezpečnost u H.323**
   - H.235

5. **Diffie – Hellman algoritmus:**
   - Umožňuje bezpečnou výměnu šifrovacích klíčů

6. **ZRTP protokol je určen pro:**
   - Rozšíření SRTP o mechanismy výměny klíčů
   - Ochranu RTP proti MITM

7. **Jaké jsou parametry Bluetooth zařízení pro zabezpečení přenosu?**
   - PIN
   - BD_ADDR
   - PK

8. **Který z následujících software můžeme označit jako zástupce NIDS?**
   - SNORT

9. **Pro autentizaci se u GSM používá algoritmus:**
   - A3

10. **Vlastnosti protokolu ESP jsou:**
    - Neautentizuje IP hlavičku
    - Šifruje IP data

11. **Kryptografie se zabývá:**
    - Návrhem a konstrukcí kryptografických algoritmů

12. **Který z algoritů GSM je využíván pro generování šifrovacího klíče.**
    - A8

13. **Jaké protokoly využívá architektura IPsec protokolu ?**
    - IP, ESP, AH

14. Pro autentizaci v UMTS se používají algoritmy:

F1, F2

15. SPIT je:

Typ sociálního útoku

Obdoba spam útoku v IP telefonii

Otevřené otázky

16. Co je to Honeypot, definujte

Informační systém sloužící k monitorování neoprávněného využívání systémových zdrojů. Funguje jako návnada lákající útočníka (malware) přičemž po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze, která buď vyloučí, nebo potvrdí, zda se jedná o škodlivý kód. Tento automatizovaný proces umožňuje sběr velkého množství vzorků nákazy, a je tak řádově rychlejší, než je tomu v případě, kdy dochází ke sběru přímo z napadených stanic.
Pro dosažení větší efektivity jsou obvykle jednotlivé honeypoty propojeny do sítí (tzv. honeynets), které sdílí informace o nově detekovaném malwaru a trendech (např. způsobech šíření, použitých kompresních algoritmech apod.).

17. Jaké druhy firewallu můžeme rozlišovat ?

Paketový filtr pracuje jen v ip vrstvě, rozhoduje jen na základě zdrojové a cílové ip adresy, pokročilejší filtry zvládají pracovat i s okolními vrstvami (linkovou a transportní), umožňuje větší možnosti nastavení, lze kontrolovat jednotlivé poskytované služby, větší náročnost.

Stavový firewall udržuje tabulku všech navázaných spojení, slouží pro zjištění, zda pakety náleží do některého otevřeného spojení nebo ne, kvůli paketovému filtru ani stavovému firewallu není nutné měnit stávající aplikace.

Aplikační proxy aplikační proxy funguje v aplikační vrstvě a rozumí daleko lépe obsahu paketů. Umožňuje také identifikaci uživatele, pro každou službu musí být ale samostatné proxy a je potřeba upravit klientské programy.

18. Jaký je rozdíl mezi SRTP a ZRTP

Protocol (RTP) neobsahuje ve svém základu žádné ochranné metody či mechanizmy, proto byl definován protokol SRTP (Secure Real-time Transport Protocol), který již tyto metody má implementovány. V nedávné době byl také uveden nový bezpečnostní protokol ZRTP (Zimmermann Real-time Transport Protocol), který nemá sloužit jako náhrada za SRTP, ale pouze jako nadstavba pro jeho lehčí použití a implementaci.

SRTP rozšiřují o bezpečnostní mechanismy protokol RTP, konkrétně o podporu integrity, ověření autentizace, zaručení důvěrnosti, ochrana proti přeposílání. Má port 5004

ZRTP je nástavba pro SRTP. Rozšiřuje tento protokol o mechanismy pro počáteční výměnu symetrických klíčů a dokáže chránit i proti útokům zvaných jako „man in the middle“
- Používá Diffie- Hellmanův algoritmus

19. Jaký účel má protokol AH v IPsec

- V rámci IPsec existují 2 typy paketů – autentizace a integrita IPsec je zajišťována pomocí tzv. AH a šifrování ESP
  - Protokol poskytuje sekvenční čísla, pro ochranu proti tzv. útokům pomocí zopakování zpráv
  - Autentizace je v IPsec realizována pomocí protokolu Authentication Header (dále také AH)
  - V protokolu AH a ESP se označuje hodnota výstupu autentizačního otisku pod položkou ICV (Integrity Check Value). AH může být použit samostatně nebo spolu s ESP
  - Bližší popisy uvádějí v RFC 2403 a 2404, využívající hashovací funkce HMAC-MD5 a HMAC-SHA1 a RFC 2857 HMAC-RIPEMD-160. Funkce HMAC zajišťuje autentizaci hashovací funkce uživatelským klíčem, takže výše zmíněné funkce jsou považovány za bezpečné. Výstup funkce tedy zajišťuje kromě autentizace také integritu – útočník sice může vypočítat běžný otisk, ale nemůže k tomu navíc podvrhnout klíč vlastníka, který je k výpočtu potřeba.

20. Co je to Milenage ?

Souhrnný název pro algoritmy f1* až f5* (UMTS)– základem je zde symetrická bloková šifra Rijndael

- **f1**– autentizační algoritmus pro ověření sítě
- **f1* a f5*** – také slouží jako resynchronizační algoritmus
- **f2**– autentizační algoritmus pro ověření účastníka
- **f3**– algoritmus pro generování klíče utajení CK (Cipher key)
- **f4**– slouží ke generování klíče integrity IK (Integrity key)
- **f5**– slouží ke generování klíče anonymity AK (Anonymity Key)

21. Stručně a výstižně popište rozdíly mezi proudovou a blokovou šifrou, jejich zástupce a příklady použití

Bloková:
Šifruje se po blocích pevné délky (například 128 bitů) na rozdíl od proudových ifer.. V kryptografii typ symetrické šifry., Pokud je dat více, rozdělí se na více bloků, přičemž do zbylého místa v posledním je umístěna výplň (padding). Při ifrování je každý blok zakódován pomocí šifrovacího algoritmu řízeného utajeným ifrovacím klíčem. Dešifrování probíhá stejným postupem zašifrované bloky stejné délky jsou postupně rozšifrovány stejným šifrovacím algoritmem pomocí stejného utajeného šifrovacího klíče. Slabinou, pomocí které může kryptoanalýza šifru prolomit, je opakované použití

stejné transformace (stejného klíče) na všechny bloky. Proto je nutné použít nějaký druh režimu provozu blokové ifry (modes of operation), který vnese do šifrování další vstup, který způsobí, že zašifrovaná data vypadají jako náhodná sekvence. Tento doplňující náhodný vstup, který je někdy označován za inicializační vektor, může způsobit, že bloková šifra se chová jako proudová (rozdíl mezi těmito druhy šifer není vždy evidentní). Jednou z prvních šifer DES (anglicky Data Encryption Standard) vyvinutá v IBM a standardizována v roce 1977. Její nástupce AES (anglicky Advanced Encryption Standard) byl přijat v roce 2001. Blowfish, Twofish, GOST

Proudová

Šifruje se po jednotlivých znacích. Proudová šifra je v kryptografii typ symetrické šifry, kde vstupní datový tok je kombinován (typicky pomocí funkce XOR) s pseudonáhodným proudem bitů (keystream) vytvořeným z šifrovacího klíče a šifrovacího algoritmu. Výsledkem je zašifrovaný datový tok (proud), který je kódován neustále se měnící transformací (na rozdíl od blokové šifry, kde je transformace konstantní). Proudové šifry jsou typicky rychlejší než blokové šifry a pro implementaci potřebují jednodušší hardware. Jsou náchylnější ke kryptoanalytickým útokům, pokud jsou nevhodně implementovány (počáteční stav nesmí být použit dvakrát). FISH, RC4

22. Stručně a výstižně popište metody symetrického a asymetrického šifrování, rozdíly mezi nimi a příklady použití

Sym: velmi rychlé, výpočetně nenáročné, náchylnější na útoky než Asym, obě strany mají stejný klíč pro šif a dešif.

DES - bloková šifra slovo má pevnou délku (pro DES 64 bitů, z nich využito jen 56), 3DES

Asym: pro **šifrování** a dešifrování používají odlišné klíče. To je základní rozdíl oproti symetrické kryptografii, která používá k **šifrování** i dešifrování jediný klíč.

- RSA(Asym.) je 1000x pomalejší než DES (SK)
-

23. Stručně a výstižně popište způsob přenosu master klíče při vytváření relace pomocí SRTP

Pro distribuci se používá protokol SDP, ten ale není, tak jako většina dalších protokolů, chráněn proti případným útokům, proto se ještě navíc k němu využívá bezpečnostních
protokolů TLS (Transport Layer Security) nebo IPsec.

24. Uveďte a popište tabulky používané v IPtables

IPtables pracuje se třemi základnimi tabulkami:

filter - Výchozí tabulka, určená k filtrování procházejících paketů. Jsou v ní pří- stupné řetězce INPUT, OUTPUT a FORWARD.

nat - Tabulka používaná pro překlad adres v řetězcích PREROUTING, POSTROUTING a méně často i v OUTPUT.

mangle - V této tabulce lze měnit některé další hodnoty v IP hlavičce (TOS, TTL) a označit pakety. Značka není součástí paketu a zaniká s odchodem paketu. Pracuje se všemi pěti definovanými řetězci.tracking)

25. Co je to Kasumi ?

Kasumi je jádrem obou šifrovacích algoritmů f8 a f9 je to tzv. bloková šifra, kdy délka bloku je 64 bitů a délka klíče 128 bitů. Z šifry KASUMI vychází šifra MISTY1, která je povinná pro šifrování dat v W-CDMA sítích.

26. Definujte podstatu Kerckhoffova principu?

Bezpečnost šifrovacího systému nesmí záviset na utajení algoritmu, ale pouze na utajení klíče.

Základní Axiómy:
1. pouze klíč je tajný
2. kryptografické algoritmy nejsou tajné
3. musím předpokládat, že útočník zná princip šifrovacího systému.

27. Jak můžeme definovat útok DOS? (Denial of service)

Znepřístupnění služeb jakýmkoliv způsobem. Docílit lze: obsazením přenosové kapacity(DDoS), přivlastnění systémových zdrojů, zneužití chyb v programech, napadením DNS. Motivací k této činností je konkurenční boj, forma demonstrace, kyber terorismus, skrytí sekundárního útoku.
DDoS - distribuovaný DoS je prováděn ze 2 a více stanic současně. Služby které poskytují ochranu před DDoS útoky jsou například Incapsula, Cloud Flare, SUCURI. http://www.digitalattackmap.com

28. Definujte pravidlo pro IPtables, které provede následující: Povolení UDP trafficu na porty 5060 až 5070 z IP adresy 192.168.0.1. Ostatní příchozí data budou zahozena

iptables -P INPUT DROP
iptables -A INPUT -i eth0 -s 192.168.0.1 -j ACCEPT
iptables -A INPUT -p udp --dport 5060:5070 -s 192.168.0.1 -j ACCEPT (tohle ještě není asi OK)

29. Uveďte stručně a výstižně, jaký je účel IPS a IDS systémů, rozdíl mezi nimi a příklady implementace.(Intrusion Detection Systems, Intrusion Protection Systems)

IDS/IPS jsou systémy detekce či protekce neoprávněného vniknutí do počítačové sítě
IPS - slouží k zabezpečení sítě, analyzuje chování v síti (podezřelé aktivity) pokouší se blokovat útoky a následně je hlásit správci
IDS - může být zařízení nebo softwarová aplikace - podle jeho nastavení a po zjištění nebezpečí v síti je schopný ho zablokovat
implementace pomocí Snort (Cisco) nebo Suricata (OISF)

30. Uveďte stručně a výstižně, jaký je rozdíl mezi protokoly AH a ESP v IPsec

AH (authentication header) - autentizační hlavička může být použita samostatně nebo s ESP.
Autentizace a integrita IPsec je zajišťována pomocí tzv. AH a šifrování ESP
ESP - je protokol určený pro poskytnutí především pro zabezpečení přenášených dat.

Caesarova šifra?

Znaky otevřeného textu jsou nahrazovány jinými znaky dle dohodnutých pravidel. Každý znak se nahradil znakem, který je v abecedě o 3 pozice před ním. Později byla Caesarova šifra zdokonalena proměnlivou hodnotou posunutí v abecedě.

Steganografie?

Utajuje existenci zprávy, respektive existenci komunikace.
Steganografie využívá metody utajení komunikace ukrytím zpráv. Utajený přenos zprávy probíhá v pozadí neutajené zprávy. Jedná se o techniku ukrytí zprávy v zprávě, resp. ukrytí tajné informace ve zprávě.

Praktická zkouška z předmětu BvK

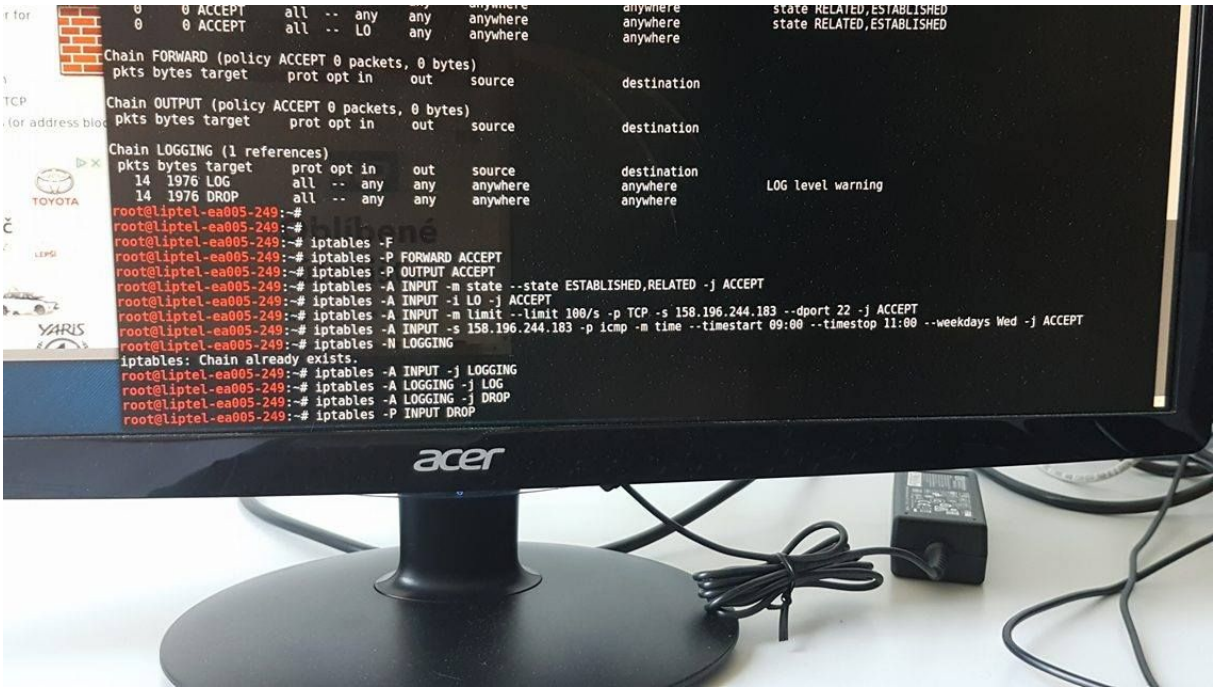
Virtuální PC jsou dostupné přes SSH na IP: **158.196.244.178-179**

158.196.244.181-190

Login: **student** Heslo: **k440**

dání 3:

- Definujte firewall pomocí nástroje iptables.
- Použijte jedno PC jako útočníka a druhé jako server, který je nutno ochránit.
- Zakažte veškerý provoz na rozhraní, kromě sestavených session a provozu na loopback.
- Povolte z IP adresy útočníka provoz pouze na protokol TCP a port 22 a omezte jej pouze na 100 paketů za sekundu.
- Povolte z IP adresy útočníka ICMP ping pouze v čase a dni konání zkoušky (Středa 9:00 – 11:00).
- Veškerý další provoz bude zahozen a bude logován do syslogu.



```
iptables - F
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i Lo -j ACCEPT
iptables -A INPUT -m limit --limit 100/s -p TCP -s 158.196.244.184  --dport  22 -j ACCEPT
iptables -A INPUT -s 158.196.244.184 -p icmp -m time --timestart 09:00 --timestop 11:00 --weekdays
Thu -j ACCEPT
iptables -N LOGGING
iptables -A INPUT -j LOGGING
iptables -A LOGGING -j LOGGING
iptables -A LOGGING -j DROP
iptables -P INPUT DROP
```

Praktická zkouška z předmětu BVK

Virtuální PC jsou dostupné přes SSH na IP: **158.196.244.181-18**

Login: **student** Heslo: **k440**

Zadání 1:

- Vytvořte CA pomocí nástroje openssl.
- Pro uložení certifikátů a klíčů vytvořte adresář firma s příslušnou adresářovou strukturou a nastavte příslušná přístupová práva.
- Vytvořte také soubor s indexací podepsaných certifikátů a jejich počítadlo.
- Upravte konfigurační soubor openssl.cnf pro Vaše potřeby.
- Doba platnosti certifikátu CA bude 10 let.
- Vytvořte certifikát a klíč CA, který bude šifrován rsa 4096 bit klíčem a bude zabezpečen PEM frází: labn211.
- Na stejném lokálním PC vytvořte požadavek na podepsaný certifikát s platno a šifrovaním rsa 2048 bitů. Požadavek bude obsahovat stejnou PEM frázi jak
- Nechte požadavek podepsat CA.

Zadání 2:

- Vytvořte šifrované VPN spojení s využitím TLS/SSL certifikátů mezi serverer klientem pomocí OpenVPN nástroje.
- Použijte vzdálené PC jako klient a lokální jako server.
- Certifikační autoritu, certifikát DH, certifikáty i klíče vygenerujte buď pomo nebo pomocí openssl. Pro distirbuci klíčů a cert. použijte SSH spojení.
- Vytvořte konfigurační soubory server.conf a klient.conf.
- Šifrované spojení pojede přes tun rozhraní, bude využívat lzo kompresi, D algoritmus, port 5000, verbosity bude nastavena na úroveň 5 a IP adresy rozhraní budou 192.168.2.1 pro server a 192.168.2.2 pro klienta.