8. IDS i WWW

Uljezi: vanjski, unutarnji

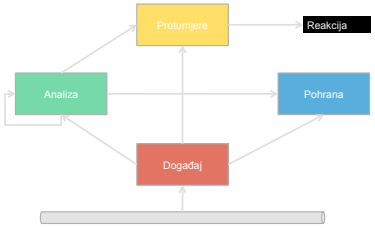
Upadi: fizicki, sistemski(niski racun do admin), udaljeni

Upada se preko:

- **greske u softveru** - preljev spremnika, neocekivane kombinacije, unhandeled input, visenitnost
- **sistemska konfiguracija** - default conf, lazy admin, rupe, veze povjerenja
- **probijanje lozinke** - weak pass, brute force, dictionary
- **sniffing** - shared medium, server ili switch, remote (RMON)
- **greske u dizajnu sustava** -TCP/IP flaws, OS rupe

Upad:

1. promatranje izvana
2. promatranje iznutra
3. iskoristavanje - koriste se rupe, CGI, server, browser, mail itd.
4. upad - skrivanje dokaza
5. unovcavanje



IDS - komplementaran s prevencijom, firewall + anti insajder

•nadzire korisnike i sustav

•nadgledanje ranjivosti i gresaka, prati logove, ispravljanje kofiguracije lose

•pazi na integritet sys files

•identificira sumnjive aktivnosti

•instalacija zamki

- Vrste: NIDS, HostIDS, ProtocolIDS, AppIDS, HibridIDS, SysIntegVer, DeceptionSystem
- Ogranicenja: switched network, resursi, onfly daje premalo podataka,DoS, prikrivanje str

Otkrivanje uljeza: signarure(malo false poz - resursi, update) vs. heuristics(nove-dugo ucenje, puno false poz), lokalno ili mreza

-audit trail - prate se kriticni dogadjaji preko logova, login, fopen itd

-onFly - ids prati informacije s racunala u RT, preusmjerava se mrez prom preko ids

-normal sig - poc profil, prati se ponasanje, prilagodba profila

-dev sig - profili napada, potpisi sumnjivog ponasanja

-param pattern - admin nadgleda sysop i primjecuje sumnjivosti

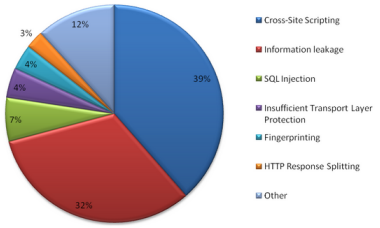
Rootkit:
-upada se i instalira, vrte sniffere, mijenja std programe ls, login, ps, ifconfig, netstat
-otkrivanje: logs, friski ps, rucno ili automatski ako IDS nije kompromitiran

PortSweep - scan portova, lako se otkriva

HTTP - stateless, cookies, session,paremetri, skrivene varijable

Ranjivosti:

1. **umetanje** - SQL injection / whitelist input, procedure, minimizirati ovlasti nad DB
2. **XSS** - napadac salje podatke via cookies itd / whitelist, sanitize
3. **Autentifikacija** - kradja SESSION ID / SSL, provjera certifikata, funkcija itd
4. **Nesigurne reference** - manipulacija preko urla/ hash, temp vrijednosti, provjera prava
5. **cross site forgery** - automatski poslani autent podaci / hidden token, hash fja itd



6.**lose postavke sustava** - backdoor, libraryes itd / patching, provjera sustava

7.**nesigurna pohrana sifriranih pod** - neidentificirani, zaboravljeni / verifikacija arh, sifriranje

8.**nezasitceni URL** - kao i reference, samo za url ne objekte / koristiti autentifikaciju itd.

9.**Transport layer** - sniffing za lozinkama itd / TLS, sifriranje, potpisivanje

10.**redirect** - koristenje redirecta za zaobilazenje logina / provjera parametara, dozvola

9. Mail

4 incidenta:

-klasika - prijetnje, prevare, ucjene, itd

-zli software - virusi, crvi itd.

-zloupotreba - spam, hoax

-gubitak privatnosti - citanje poruka, webbug

SMTP
-obavezne:HELO, MAIL, RCPT, DATA, RSET, VRFY, NOOP, QUIT
-ostale:SEND, SOML, SAML, EXPN, HELP, TURN

-poruke **2xx** - uspjesno izvrsenje poslane naredbe

rijesenja:provjera IP, ogranicenja naredbi,valjanost zaglavlja, logovi, velicina, broj poruka/h

autentifikacija - SMPT-AUTH, ESMPT(SASL), SPA via smpt-auth

MAILvs**MIME** - binarne dat, 998+CRLFz, 7b ASCII, velicina VS svi znakovi, sturktura i vrsta poruke, multimedia attachmenti, objektni oblik, **5 novih zaglavlja**(MIME ver, cont type, **cont-trans-enc**(7/8b(988+), bin, quoted-printable(76+), base64(76+)), cont-ID, cont-dispsition), mulitpart msg

S/MIME - potpis(autent, integritet, neporecivost) i sifriranje(sigurnost podataka, privatnost)
-CMS - kljucevi i certifikati za signature, autent, sazimanje, sifriranje MIME
*signed - autent, neporec, integritet, jedan sadrzaj, jedan potpis
*enveloped - sigurnost i privatnost, priv kljucevima sim kljuc pa salje
*digested - cjelovitost, hash neke vrste
*encripted - samo sifriranje, lokalna pohrana, lozinka, nema kljuceva
*authenitcated - MAC + sif auth key se salje, onda se s key verificira MAC

-ceritficati - class1(dokaz posiljatelja), class2(preko CA, ident i ver posiljatelja)

PGP - autentifikacija, povjerljivost, kompresija, kompatabilnost s mail, segmentacija
-**potpis**(DSS/SHA or RSA/SHA), **sifriranje**(AES, 3DES, IDEA ili CAST (simetrično) VS Diffie-Hellman ili RSA (asimetrično)),**kompresija**(zip), **kompatabilnost**(Radix-64)

kljucevi - web of trust, X.509

LOZINKE - 1. sniff i keylog, 2. cracker
korisnici - ista na vise sys, lako pamtive, tajna pitanja itd.
unix - hash lozinke preko DES, novi MD5,

dictAttack - dict u hash pa onda trazenje, offline. obrana: SALT nekad 12b, danas vise

bolje lozinke - biometrija, graficki uzorci,

pogadjanje - rijecnik, rijeci naopako, imena, registracije itd