Varnost na internetu in računalniških omrežjih

Nevarnosti na spletu

- V kolikšnem času napadalci odkrijejo nezaščiten računalnik?
- Je vaš računalnik lonček z medom (“honeypot”)?
- Kdo so beli klobuki (“white hats”)?
- Kdo so črni klobuki (“black hats”)?
- Lahko se vas loti že “script kiddie”!
- Kaj pomeni “own”, “0wn3d”, “rooted”, “got root”?

Napadi na dan 0

- zero-day (0-day) je dan, ko je objavljena do sedaj neznana ranljivost
- sodobne komunikacije omogočajo, da so zlonamerni programi včasih razviti še isti dan - 0-day napad

Dostopnost / Razpoložljivost (Availability)

OPIS	DELOVANJE	IZPAD NA LETO
	99,0 %	87 ur 36 min
komercialna (nižja)		
komercialna (višja)	99,7 %	27 ur 17 min
visoka	99,9%	8ur 46 min
'fault-tolerant'	99,99%, 99,999	53min, 5 min
neprekinjena	100%	0 min

Škodljiva programska oprema (Malware)

Malware

- škodljiva programska koda, namerno razvita za povzročanje škode:
  - virusi
  - črvi
  - trojanski konji
  - vohunski programi (spyware in Adware)
  - hoax
  - jedrni kompleti (root kits)

Virus

- škodljiva koda, ki okuži datoteke računalnika
- koda, ki je izdelana tako, da okuži datoteke in povzroči:
  - škodo
  - izgubo podatkov
  - odpoved sistema
- vrste:
  - virusi zagonskega sektorja
  - datotečni virusi
  - makro virusi
  - miltipartitni (zagonski + datotečni)
  - polimorfični virusi (kombinirani, mutirajo)

Virusi za mobilne naprave

- se že pojavljajo
- trenutno je poznanih dobrih deset virusov za Symbian OS
  - večina ne predstavlja večjega tveganja
- samo vprašanje časa je, kdaj bo tveganje postalo kritično

Črv

- avtonomna programska koda, ki se brez nadzora širi po omrežju
- lahko se samo množi in zaseda vire računalnikov v omrežju
- lahko vsebuje škodljivo kodo
- primeri
  - Code Red
  - Nimda

Trojanski konji (Trojan Horses)

- oblika škodljive kode, ki lahko povzroči večjo škodo sistemu ali omrežju
- večinoma delujejo skrito in so zamaskirani
- se pojavijo kot oblike drugih, koristnih programov
- se običajno ne replicirajo sami (tako kot npr. virusi in črvi)
- različice:
  - kraja gesel
  - beleženje pritiskov tipk
  - orodja za oddaljeno administracijo
  - Zombiji (za distribuirane DoS napade, SPAM)

Trojanski konji (Trojan Horses)

- omogočajo dostop do uporabnikovega računalnika
- odprejo “zadnja vrata” (backdoor)
- upravljanje in/ali zloraba računalnika brez privolitve ali/in vednosti uporabnika
- pridobivanje informacij – gesla, številke kreditnih kartic,….
- širjenje:
  - el. pošta
  - spletne strani
  - jedrni kompleti in ostali škodljivi programi

Trojanski konji (Trojan Horses)

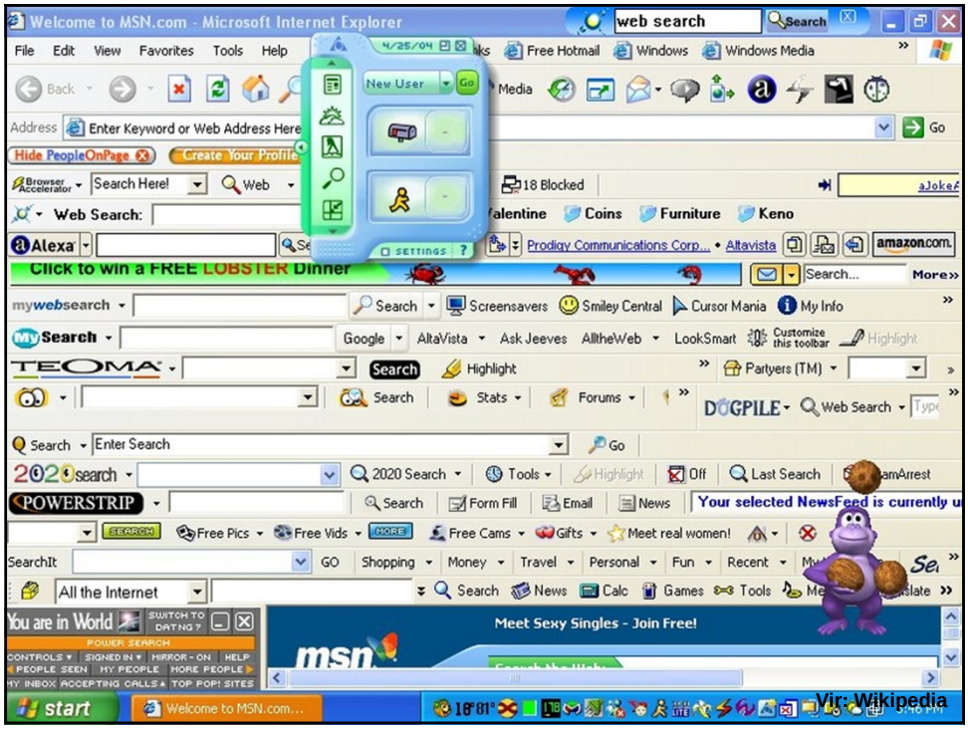
- Zloraba okuženih računalnikov (Zombijev) :
  - Dostop do okuženega računalnika na daljavo
  - Pošiljanje E-mail sporočil (SPAM)
  - Uničevanje podatkov (brisanje, formatiranje,…)
  - “Downloader”
  - FTP dostop: dodajanje ali kopiranje podatkov na/z okuženega računalnika
  - Onemogočijo varnostno programsko opremo (protivirusnih program, požarni zid,…)
  - Denial-of-service napad (DoS)

Vohunski programi (spyware)

- Oblika kode, ki se namesti z namenom, “puščanja” informacij
- običajno v obliki “adware” - programov, ki ob deskanju po spletu prikazujejo reklame
- sporoča zbrane podatke v izvorni strežnik (običajno podatke o navadah uporabnika - deskanju)
- Spyware kazniv v ZDA
  - “Spy Act”, oktober 2004
  - hkrati prva tožba proti posamezniku (New Hampshire)

Vohunski programi (spyware)

- pridobivanja informacij o osebi ali organizaciji, brez njihove vednosti
  - obiskovane spletne strani, številke kreditnih kartic, gesla,...
- Prenesejo se na uporabnikov računalnik brez njegove vednosti
- Skrito pridobivanje informacij o uporabniku in njegovih navadah
- Viri:
  - spletne strani s piratskimi programi, pornografijo ipd
  - redkeje preko el. pošte
- Ogrožanje uporabnikove zasebnosti
- Povzročanje premoženjske škode



Vir: Wikipedia

Vohunski programi (Adware)

- pogosto jih obravnavamo skupaj s vohunskimi programi
- programerji, jih vidijo kot vir prihodtkov brezplačnih programov
- nekatere programi adware so hkrati tudi shareware programi
- razlika:
  - adware prikazuje oglase (reklame)
  - shareware uporabnika poziva k registraciji ali ga opozarja na iztekajočo se preizkusno dobo

Vohunski programi (Adware)

- prikazujejo reklamna sporočila, pop-up okna, vsiljujejo uporabniku oglase
- niso tako nevarni kot so **nadležni**
- vir:
  - brezplačni in shareware programi
  - P2P programi
  - ppletne strani

Vir: Wikipedia

Jedrni kompleti (Root Kits)

- namestijo na uporabnikov računalnik brez da le-ta kaj opazi
- poskušajo ubraniti odkritja
- zlonamerni - imajo podobno vlogo kot drugi nadležni programi (npr. črvi, virusi)
- znan predstavnik je Sonyjev jedrni komplet - na CD-jih z glasbo
- zelo težko jih je odkriti in odstraniti
- manipulirajo z jedrom operacijskega sistema
- omogočajo namestitev in skrivanje drugih zlonamernih programov

Jedrni kompleti (Root Kits)

- **Strojna programska oprema (Firmware)** - programi se namestijo v strojno programsko opremo, npr. v "flash" grafične kartice
- **Virtualizirano (Virtualized)** - jedrni kompletu spremenijo zagonsko zaporedje, nato se naloži opercijski sistem v virtualni stroj
- **Na nivoju jedra (Kernel level)** - programi spreminjajo dele OS, imajo obliko gonilnikov in nalagljivih modulov, nudijo neomejen dostop do funkcij OS
- **Na nivoju knjižnice (Library level)** - krpajo (patch) ali spreminjajo klicev OS, kar jim omogoča skrivanje določenih datotek, imenikov procesov,...
- **Na aplikacijskem nivoju (Application level)** - zamenjava regularnih izvršljivih datotek s kompromitiranimi (npr. Trojanski konji), izvedejo s pomočjo krpanja, vstavljanja programske kode,…

Nezaželena pošta - SPAM

Nezaželena pošta - SPAM

- vključuje:
  - komercialni oglasi
  - potegavščine povezane z delnicami
  - odrasle vsebine
  - finančne potegavščine (hoaxes)
- 93% vse elektronske pošte je SPAM
  (okoli 180 milijard sporočil na mesec)
- 1 milijon sporočil stane $20 na črnem trgu

Nezaželena pošta - SPAM

- v preteklosti:
  - lastni poštni strežniki
- sedaj:
  - botneti

Nova generacija SPAM

- novi zombiji so bolj zmogljivi:
  - spremljajo elektronsko pošto na okuženem računalniku
  - izvajajo rudarjenje podatkov
- rezultat:
  - pošiljanje vsebinsko izpopolnjenih sporočil, ki pretentajo filtre
- prihodnost:
  - vsebinsko izpopolnjena sporočila, ki pretentajo tudi bralce (omejitev na angleško govoreč prostor)

Primeri SPAM-a

Ask yourself, if you want to be a Lion in your bed.

If the answer is Yes, visit us.

We will help!

Totally Satisfied to me show details 7:48 PM (14 hours ago) Reply

Replica Rolex models of the latest Baselworld 2009 designs have just been launched on our replica sites.

These are the first run of the 2009 models with inner Rolex inscriptions and better bands and cases. Only limited to 1000 pieces worldwide, they are expected to sell out within a month.

Browse our shop

eply Forward

GET YOUR DIPLOMA TODAY!

If you are looking for a fast and cheap way to get a diploma, this is the best way out for you. Choose the desired field and degree and call us right now

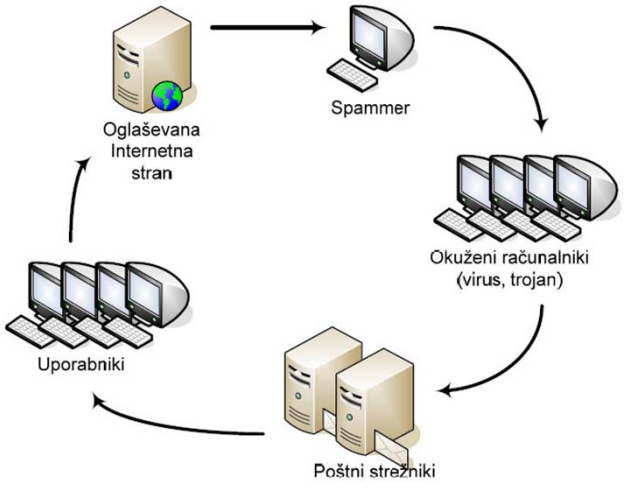
Bachelors, Masters or even a Doctorate.

For US: 1.845.709.8044
Outside US: +1.845.709.8044

"Just leave your NAME & PHONE NO. (with CountryCode)" in the voicemail.

Our staff will get back to you in next few days!

Začaran krog



BotNet

- gospodar in zombie računalniki
- zombie – računalniki uporabnikov
- pošiljanje (velikih) količin SPAM-a
- DOS oz. DDOS napadi

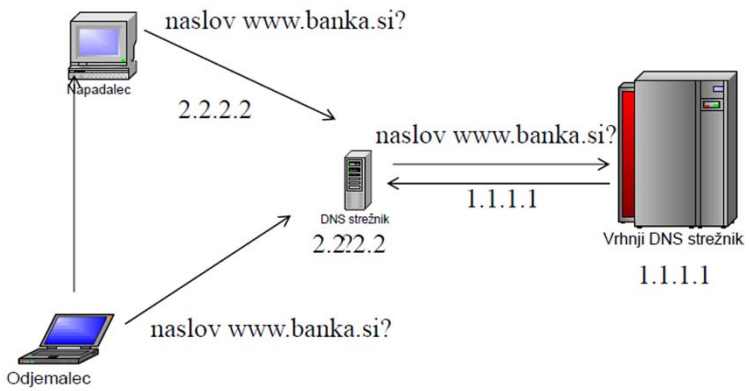
BotNet

- botnet omrežja s 100.000 do 200.000 računalniki niso več redkost
- rekorder je dansko omrežje:
  - 1.5 milijona računalnikov pod nadzorom treh posameznikov (starosti 19, 22 in 27 let)
- mutacije programov v enem omrežju se merijo v tisočih
  - preveč, da bi lahko programe našli z iskanjem specifičnih podpisov, kot to dela večina protivirusnih programov

Varnost interneta

- s pretvorbo besedila v IP je možno manipulirati (DNS spoofing)
- preprečitev storitve (Denial of Service): več različnih metod, napadalec pošilja veliko količino prometa na IP naslov napadene naprave, kar preprečuje normalno delovanje
- implementacije TCP/IP imajo napake – dodatne varnostne luknje

DNS spoofing



Napadi, specifični za internet

- IP Spoofing
  - izdelava IP paketa z napačnim IP naslovom
  - IP ne vsebuje kontrole naslovov - trivialen postopek
- mail Spoofing
  - pošljemo sporočilo z lažnim imenom pošiljatelja
  - veliko načinov, zelo prefinjeni s postavitvijo lastnega poštnega strežnika
- web Spoofing
  - URL rewriting - http://www.nevarno.si/http://www.najdi.si
  - skrivanje imena v drugi obliki zapisa (problemi poimenovanja)
  - manjša odstopanja v črkovanju za nepazljive bralce

DNS spoofing

- preusmerjanje prometa na “napačne” spletne strani
- kadar DNS ne pozna IP naslova:
  - napadalec pošlje zahtevo po naslovu na DNS
  - DNS povpraša po naslovu drugi DNS strežnik (DNS_2)
  - napadalec pošlje odgovor na zahtevo še pred strežnikom DNS_2

Ribarjenje (Phishing)

Ribarjenje (Phishing)

- "ribarjenje" za gesli, številkami kreditnih kartic, …
- beseda se prvič pojavi v novičarski skupini alt.2600, januar 1996
- fishing - F se pogosto zamenja s "Ph"
- zavajajoča elektronska pošta, spletne strani
- uporabnik sporoči osebne finančne podatke
  - številka kreditne kartice
  - uporabniško ime, geslo
- s simuliranjem uveljavljenih znamk (bank, zavarovalnic, …)

Ribarjenje (Phishing)

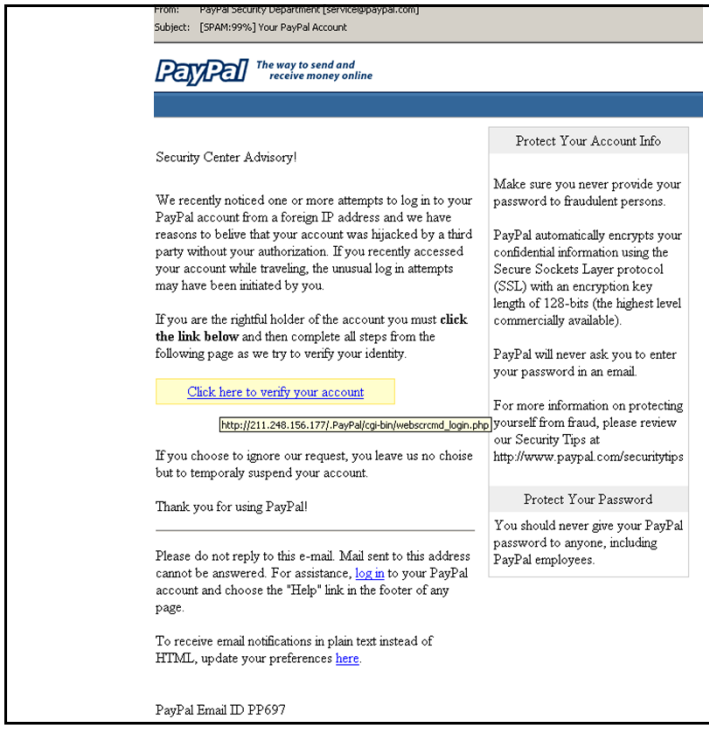
- uporabniku posnemajo resnično spletno stran z namenom se dokopati do podatkov – banke, eBay, Amazon,…
- prepričajo uporabnika, da so nekaj kar niso
- širijo se preko spletnih strani ali el. pošta
- primer: elektronska sporočila od bank, eBaya,…
- včasih preusmerijo uporabnika na spletne strani s nadležnimi programi
- beležijo precejšnje uspehe

Ribarjenje (Phishing): tehnike

- manipulacija spletnih povezav:
  - premetavanje črk v spletnih naslovih
  - uporaba posebnih znakov
  - uporaba @ (http://www.google.com@members.tripod.com)
- uporaba slik namesto besedila:
  - ribarjenje preko el. pošte
  - težko zaznavanje - zaščitni programi

Ribarjenje (Phishing) - tehnike

- zloraba spletnih tehnologij:
  - uporaba JavaScripta za spreminjanje spletnih strani
  - moderni pristopi zlorabljajo tudi druge Web 2.0 tehnologije razen JavaScripta
  - uporaba Cross-Site Scriptinga (XSS) – vstavljanje vsebin na legalne in korektne spletne strani; uporabnik tega pogosto niti ne opazi



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

Vir: Wikipedia

Avtomatizacija phishing ukan

- hitrost nastajanja phishing spletnih strani je posledica avtomatizacije
  - vnaprej pripravljeni kompleti spletnih strani
  - zbirke sporočil podjetij
  - zbirke logotipov podjetij
  - zbirke predlog spletnih strani podjetij
  - …

Phishing napadi

- statistika v ZDA
  - dosegli so 57 milijonov ljudi
  - oškodovali so vsaj 122 dobro poznanih blagovnih znamk
  - že konec leta 2004 je skoraj polovica napadov vsebovala tudi neko obliko nevarne kode
- že s spremembo hosts datoteke lahko spremenimo ciljni ip naslov domene
- napadi na domenske strežnike z namenom, da jih napadalci onesposobijo in zamenjajo z lastnimi

Primer phishinga v Sloveniji

- **Uporabnike NLB Klika posebej opozarjamo, da smo v teh dneh ugotovili pojav nove škodljive programske opreme, ki simulira lažni vstopni ekran NLB Klika. Od uporabnika zahteva izvoz kvalificiranega digitalnega potrdila ter vnos različnih gesel.**
  Da boste znali razločiti med pravo in ponarejeno vstopno stranjo v NLB Klik, smo za vas pripravili kratke opise in prikaze razlik ter varnostnih opozoril, če tako stran zaznate.

- http://www.nlb.si/cgi-bin/nlbweb.exe?doc=16038

Prevare po e-pošti

- nigerijska prevara
- prejemnik pošlje “transferne stroške” za prenos milijonov usd v pomoč pošiljatelju…
- pretvorba valute v x1000 “legalne valute” …

Spletni napadi

Najpogostejše varnostne luknje

- prekoračitev izravnalnika
- zaščita aritmetičnih operacij
- zaščita skript in spletnih strani
- vpis SQL ukazov
- slabosti kriptografskih algoritmov
- napadi DoS (Denial of Service)

Seznam CVE

- Common Vulnerabilities and Exposures
  - Seznam skupnih imen za ranljivosti programske opreme
- http://cve.mitre.org/cve/downloads/

Prekoračitev izravnalnika

- se pojavi, ko podatki presegajo pričakovano velikost in prepišejo druge vrednosti
- primarno se pojavlja v nenadzorovani C/C++ kodi
- vključuje štiri vrste:
  - prekoračitev sklada
  - prekoračitev kopice
  - prekoračitev v-tabele in funkcijskih kazalcev
  - prekoračitev upravljavca izjem
- lahko izkoristijo napadalci in škodljivi programi

Možni rezultati prekoračitve izravnalnika

MOŽEN REZULTAT	CILJ HEKERJA
Kršitev dostopa	DoS napadi na strežnike
Nestabilnost	Motenje normalnega delovanja PO
Vključevanje programske kode	-Pridobitev pravic za izvajanja lastne programske kode -Dostopa in izkoriščanje pomembnih podatkov -Izvajanje uničujočih akcij

Primer prekoračitve sklada

```
void nevarna(const char* podatki)
{
char lokalnaSpremenljivka[4];
int seEnaLokalnaSpremenljivka;
strcpy (lokalnaSpremenljivka, podatki);
}
```

Obramba pred prekoračitvijo izravnalnika

- posebna previdnost pri uporabi:
  - strcpy
  - strncpy
  - CopyMemory
  - MultiByteToWideChar
- uporaba/GS opcije prevajalnika v Visual C++ za zaznavanje prekoračitev
- Uporaba strsafe.h za varnejšo uporabo izravnalnika

Obramba pred prekoračitvijo izravnalnika

- preverimo vse indekse polj
- uporabimo obstoječe ovojne razrede za varno delo s polji
- preverimo dolžino poti z uporabo_MAX_PATH
- uporabimo preizkušene metode za delo s potmi kot npr. splitpath
- uporabimo nadzorovano kodo, pozornost pri uporabi PInvoke in COM interoperabilnosti

SQL injection

- je postopek dodajanja SQL ukazov v uporabniški vnos
- uporabljajo hekerji za:
  - izpis podatkov o podatkovni bazi
  - spremembo podatkov v podatkovni bazi
  - izogibanje avtorizaciji
  - izvajanje več SQL stavkov
  - izvajanje vgrajenih shranjenih procedur

SQL injection: primer

```
sqlString = "SELECT JePoslanoFROM"+ " NarocilaWHERE
   IDNarocila='"+ ID + "'";
```

- če je vrednost ID vpisana neposredno iz uporabniškega vnosa (splet ali Windows), lahko uporabnik vnese:
  - 1001
  - 1001' or 1=1 –
  - 1001„;DROP TABLE Narocila—
  - 1001„;exec xp_cmdshell('fdisk.exe') --

SQL injection: obramba

- prečistimo vhodne podatke
  - vsi vhodni podatki so škodljivi razen če dokažemo nasprotno
  - poiščemo veljavne podatke, ovržemo vse ostalo
  - odstranimo neželene znake (regularni izrazi?)
- zaganjamo z najnižjimi privilegiji
  - nikoli ne izvajamo kot “administrator”
  - omejimo dostop do vgrajenih shranjenih procedur
- uporabimo shranjene procedure ali sql parametrizirana povpraševanja za dostop do podatkov
- ne izpisujemo napak, ki jih javlja baza!

Vstavljanje skript

- SQL Injection je le ena od različic
- podobne ranljivosti se uporabijo vedno, ko se en programski jezik izvaja v drugem
- dobro poznavanje in ločevanje:
  - ukaznega toka in
  - toka podatkov

Vstavljanje skript: primer

- ukazni tok:
  - dir
- običajni podatkovni tok:
  - c:
- zloraba podatkovnega toka:
  - c: | format c: /y
  - -> dir c: | format c: /y
- pozor pri vsakem združevanju tokov!

Cross-site scripting

- tehnika, ki omogoča hekerju:
  - izvajanje škodljive kode v brskalniku odjemalca
  - vstavljanje<script>, <object>, <applet>, <form>, in<embed> oznak
  - krajo informacij seje in avtentikacijskih piškotkov
  - dostop do računalnika odjemalca
- katerakoli spletna stran, ki prikazuje HTML z uporabniško vsebino je ranljiva!

XSS: Običajni obliki napada

- napad na spletne e-poštne aplikacije in forume
- uporaba <form> oznake za redirekcijo osebnih podatkov

Obramba

- ne zaupamo vnosu uporabnikov
- ne izpisujemo uporabniških vnosov brez predhodne validacije
- ne shranjujemo skrivnih informacij v piškotkih
- uporabimo opcijo HttpOnly za piškotke v IE 6.0 SP1
- uporabimo<frame> varnostne atribute za določanje varnosti
- uporabimo ASP .NET varnostne funkcije

Napadi “Denial of Service”

- izstradanje CPU
- izstradanje pomnilnika
- izstradanje virov
- izstradanje omrežja

Napadi “Denial of Service”: obramba

- varnost naj bo del načrtovanja
- ne zaupamo vnosu uporabnikov
- inteligentna odpoved
- testiranje varnosti

Zaščitna prog. oprema

Požarni zid

- je naprava ali programska oprema za varovanje omrežja ali strežnika pred nevarnim mrežnim prometom
- delovanje
  - opazovanje prometa med omrežji
  - nadzor prometa med omrežji
- običajno postavljeni na točko povezave med omrežji - “vratarji”

Filtriranje paketov

- dovolijo ali prepovejo IP pakete glede na postavljena pravila:
  - naslov pošiljatelja
  - vrata
- delujejo na nivoju omrežja
- zelo hitri
- prvi nivo obrambe

Vrata na nivoju povezave

- "poslušajo" TCP povezovanje iz zunanjih naslovov
- dovolijo ali prepovejo povezavo glede na številko vrat
- v primeru dovoljene povezave:
  - TCP seja je vzpostavljena med zunanjim naslovom in požarnim zidom
  - ločena seja je vzpostavljena z internim naslovom
  - posreduje podatke med omrežji na nivoju seje
- dodatna varnost, običajno skupaj s filtriranjem paketov

Vrata na nivoju aplikacije

- filtrirajo promet glede na uporabljen aplikacijski protokol
- HTTP, FTP, …
- dovolijo samo npr. HTTP protokol na vratih 80
- vrata na nivoju povezave dovolijo vse protokole na vratih 80…

- beleženje prometa, avtentikacija, pretvorba protokolov, …
- počasnejši

Demilitarizirana cona (DMZ)

- je cona med internim in zunanjim omrežjem - “ni v omrežju in ni zunaj omrežja”
- delno ščiti strežnike z zunanjimi storitvami, vendar omogoča dostop do njih
- primer: omogočimo samo dostop do vrat 80 - ker ponujamo samo storitve na teh vratih
- nekateri strojni požarni zidovi imajo priključek ”DMZ”
- včasih je primerno postaviti več DMZ con

Pametna omrežna oprema

- računalnik se lahko priključi v omrežje šele, ko izpolni določene pogoje
  - nameščeni zadnji popravki
  - nameščen protivirusni program
  - nazadnje pregledan celoten računalnik pred največ 7 dnevi
  - vključen požarni zid
  - …

Protivirusna zaščita

- Namenska programska oprema
- Zaznava zlonamerno prog. Opremo
  - Na podlagi vzorcev
  - Na podlagi vedenje (hevristika)

Varnost brezžičnih omrežij

Brezžične dostopne točke

- v letu 2005 je bilo 70% brezžičnih dostopnih točk v ZDA popolnoma nezaščitenih
- večina ostalih za zaščito uporablja WEP (Wired Equivalent Privacy) protokol, ki ni varen
- le redke uporabljajo WPA (Wi-Fi Protected Access)

Wardriving

- iskanje brezžičnih omrežij
- prevozno sredstvo, prenosnik, kartica za brezžično omrežje, GPS, programska oprema
- iskanje SSID, omrežij z nešifriranim prometom