1.2 Uvod u slabosti mreže, prijetnje i napade

1.2.1 Slabosti mreže

Kada govorimo o mrežnoj sigurnosti, spominju se tri uobičajena termina, slabost mreže, prijetnja i napad.

Slabost mreže je slabost koja je sastavni dio i ugrađena je u svaku mrežu i mrežni uređaj. To uključuje router-e, switch-eve, stolna računala, servere pa sve do samih sigurnosnih uređaja.

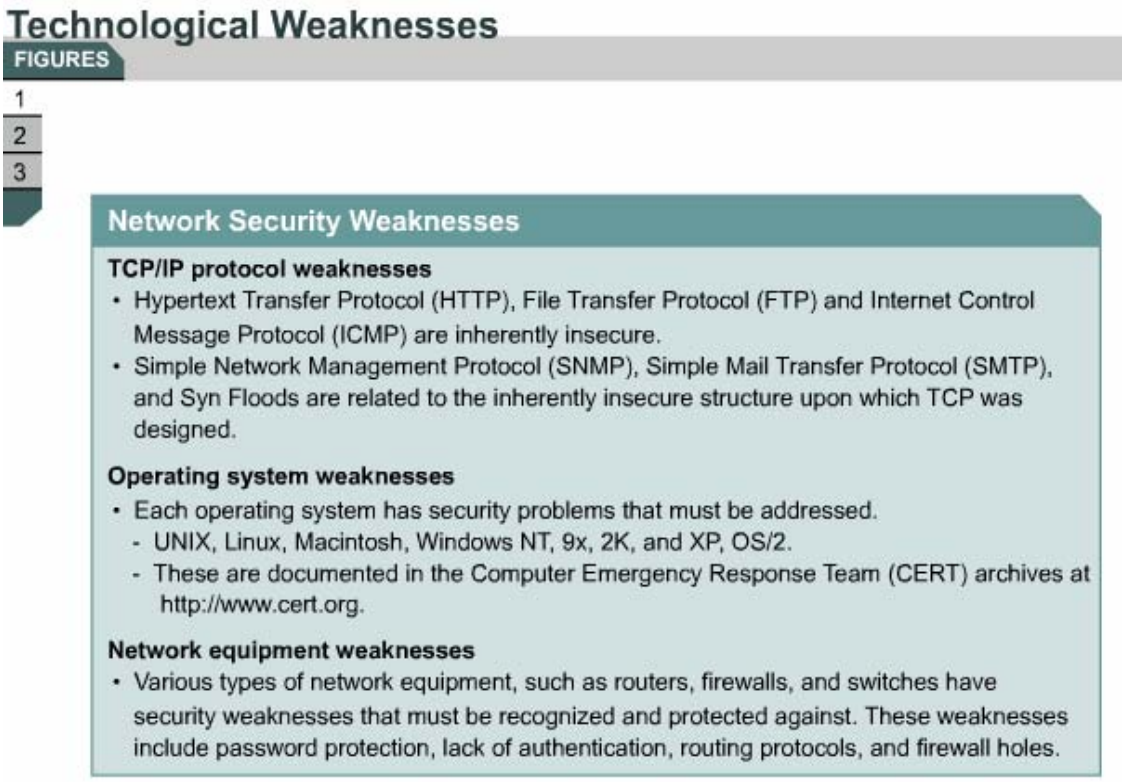
Prijetnje su ljudi zlonamjerni, spremni i kvalificirani  da iskoriste te slabosti meže. Oni kontinuirano traže, otkrivaju i iskorišavaju nove slabosti mreže.

Na kraju, prijetnje koriste različite alate, skripte i programe i napadaju mreže i mrežne uređaje. Tipično, mrežni uređaju koji se najčešće napadaju su krajnje točke kao npr. serveri ili stolna racunala.

Tri najčešće slabosti mreže su:

- Tehnološka slabost mreže
- Konfiguracijska slabost mreže
- Slabost sigurnosnih pravila i procedura

Tehnološka slabost mreže
Kompjuteri i mrežne tehnologije imaju suštinske sigurnosne slabosti. To uključuje TCP/IP protocol




Slabost konfiguracije
Mrežni administratori ili mrežni inženjeri moraju naučiti što je slabost konfiguracije i korektno konfigurirati kompjutere i mrežne uređaje da bi maksimalno kompenzirali te slabosti.
Neke najčešće slabosti konfiguracije dane su u listi na slici 2.

## Configuration Weaknesses

FIGURES

1
2
3

| Weakness | How the Weakness is Exploited |
|---|---|
| Unsecured user accounts | User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers. |
| System accounts with easily guessed passwords | This common problem is the result of poorly selected and easily guessed user passwords. |
| Misconfigured Internet services | A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems. |
| Unsecured default settings within products | Many products have default settings that enable security holes. |
| Misconfigured network equipment | Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes. |

Slabosti sigurnosnih procedura
Slabost sigurnosnih procedura može prouzročiti nepredvidive prijetnje sigurnosti. Mreža se može naći u situaciji velikog sigurnosnog rizika ako korisnici mreže ne poštuju sigurnosne procedure. Neke uobičajene slabosti sigurnosnih procedura i kako se te slabosti zlorabe dane su u tablici na slici 3.

## Security Policy Weaknesses

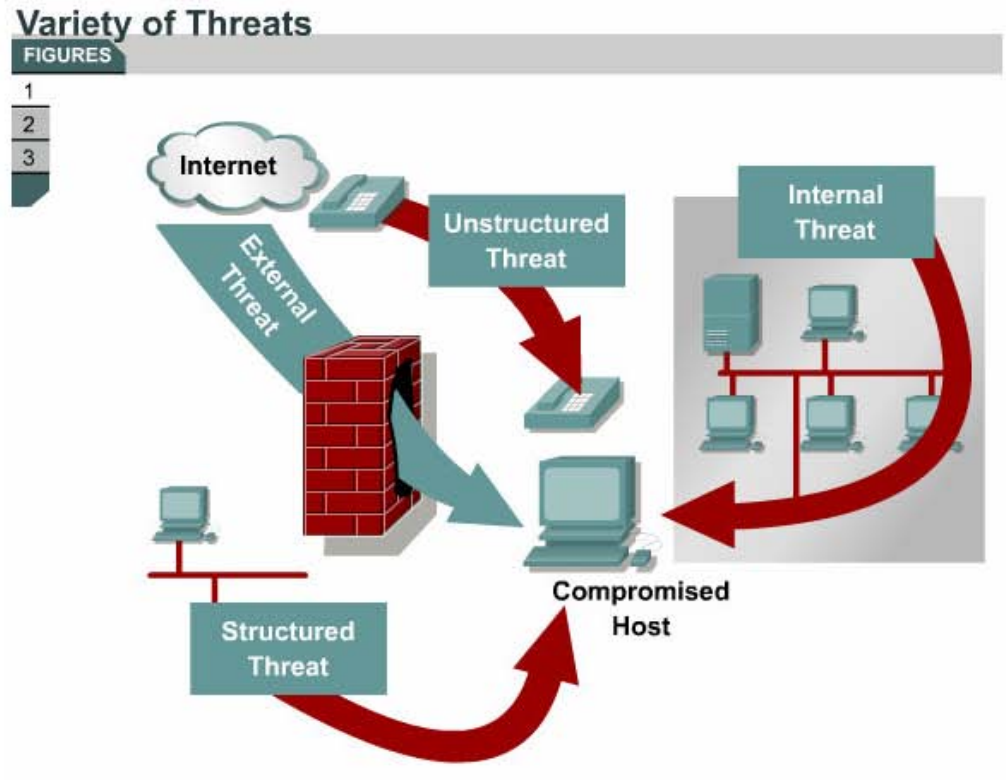
FIGURES

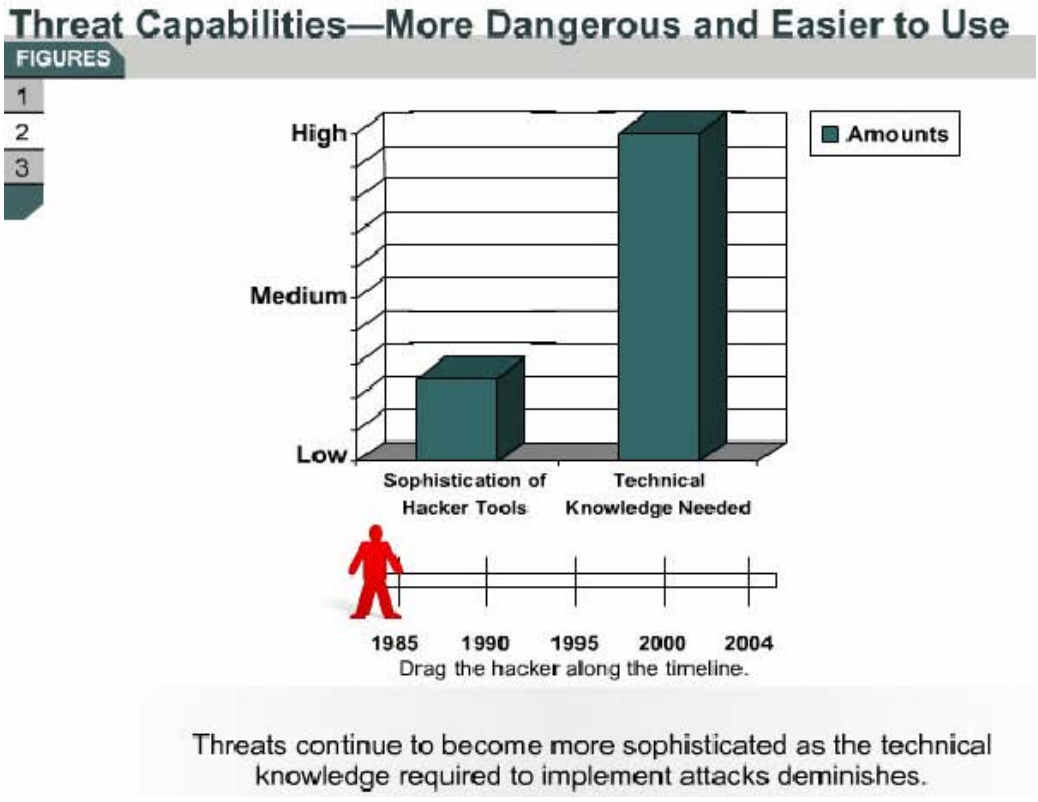
1
2
3

| Weakness | How the Weakness is Exploited |
|---|---|
| Lack of written security policy | An unwritten policy cannot be consistently applied or enforced. |
| Politics | Political battles and turf wars can make it difficult to implement a consistent security policy. |
| Lack of continuity | Frequent replacement of personnel can lead to an erratic approach to security. |
| Logical access controls not applied | Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network. |
| Logical access controls not applied | Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist. |
| Software and hardware installation and changes do not follow policy | Unauthorized changes to the network topology or installation of unapproved applications create security holes. |
| Disaster recovery plan is nonexistent | The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise. |

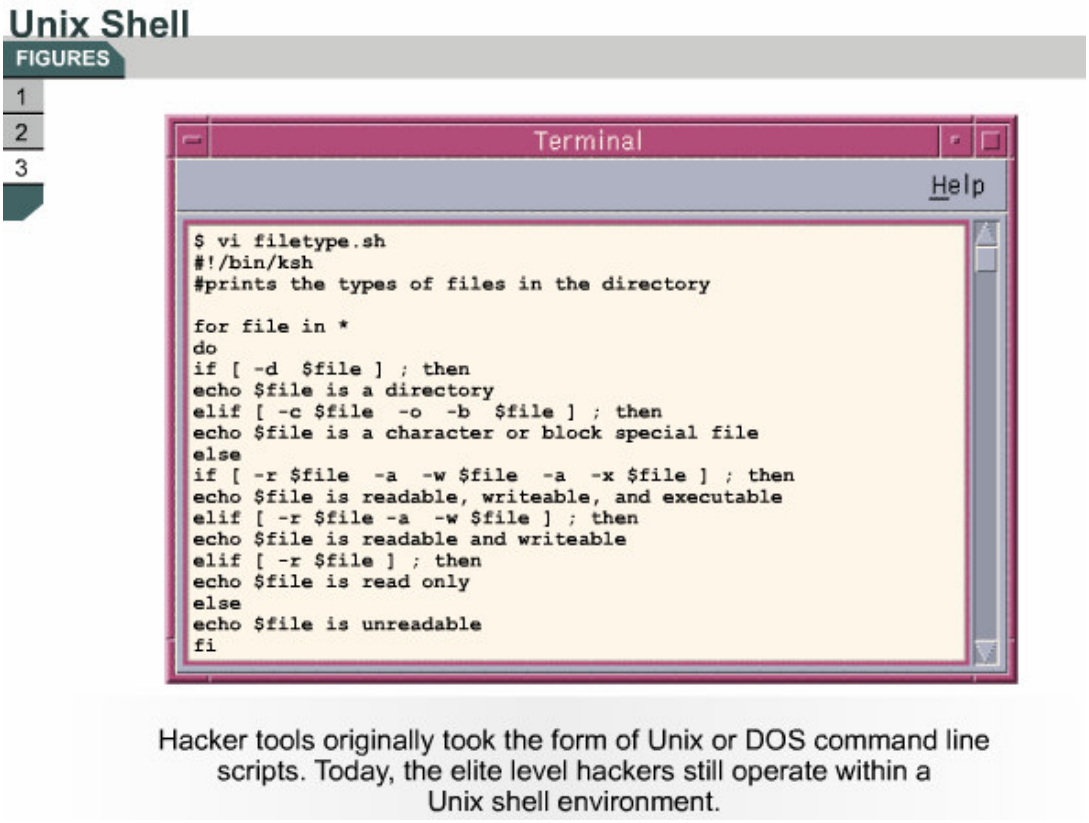
1.2 Uvod u slabosti mreže, prijetnje i napade
1.2.2 Prijetnje

Postoje četiri primarne grupe prijetnji mrežnoj sigurnosti:




Prijetnje koje dolaze izvan mrežne strukture dolaze najviše od neiskusnih pojedinaca koji koriste jednostavne, lako dostupne alate za „hacking“ kao shell skripte i programe za probijanje lozinki.




Hacker tools originally took the form of Unix or DOS command line scripts. Today, the elite level hackers still operate within a Unix shell environment.

Čak i prijetnje koje doaze izvan mrežne strukture koje se izvršavaju s namjerom testiranja i provjere hacker-ovih sposobnosti mogu nanijeti ozbiljnu štetu poduzeću. Na primjer, ako je vanjska WEB stranica poduzeća napadnuta, integritet cijelog poduzeća je narušen. Čak i ako je vanjska WEB stranica odvojena od pristupa internim informacijama koje su zaštićene firewall-om, okolina to ne prepoznaje. Sve što okolina, odnosno ostali korisnici, vide je stranica koja nije sigurna što bitno utječe na poslovanje.

Prijetnje unutar mrežne strukture

Prijetnje unutar mrežne strukture dolaze od strane hacker-a koji su posebno motivirani i tehnološki kompetentni. Te osobe dobro poznaju slabosti mreže i mogu razumjeti i razviti zlonamjeran kod i skripte. Oni razumiju, razvijaju i koriste sofisticirane hakerske tehnike da bi prodrli u tvrtke koje ništa ne sumnjaju. Ove grupe ljudi vrlo često su uključene u slučajeve velikih prevara i krađa koje se nalaze u izvještajima institucija koje se bave praćenjem kompjuterskog kriminala.

Vanjske prijetnje

Vanjske prijetnje se mogu pojaviti od strane pojedinaca ili organizacija koje rade izvan poduzeća. One ne moraju imati autorizirani pristup kompjuterskom sistemu ili mreži. Oni pronalaze svoj put u mrežu uglavnom preko inerneta ili dialup pristupnih servera.

Interne prijetnje

Interne prijetnje se pojavljuju kada netko ima autorizirani pristup preko otvorenog računa na serveru ili direktan, fizički pristup mreži. Prema istraživanjima FBI-a interni pristup i zlonamjerno i krivo korišten računi uzrokuju 60-80% incidenata.

Kako su se vrste prijetnji, napada i zlonamjernog iskorištavanja razvijale, pojavila se različita terminologija opisa tih pojedinaca ili grupa. Neki najčešći pojmovi su:

Hacker

Hacker je općenit pojam koji se u prošlosti koristio za opis kompjuterskog experta. U zadnje vrijeme, ovaj termin ima negativne konotacije i koristi se za opisivanje pojedinaca koji nastoje neautorizirano i zlonamjerno pristupati mrežnim resursima.

Cracker
Cracker je pojam koji generalno bolje opisuje pojedince koji nastoje neautorizirano i zlonamjerno pristupati mrežnim resursima.

Phreaker
Phreaker je pojedinac koji manipulira telefonskom mrežom s ciljem izvršavanja funkcija koje standardno nisu dozvoljene. Uobičajeni cilj phreaker-a je upad u telefonsku mrežu, obično preko prepaid telefona, i obavljanje besplatnih razgovora.

Spammer
Spammer je pojedinac koji šalje velike količine neželjenih mail poruka. Spammer-i obično koriste viruse da bi preuzeli kontrolu nad kućnim kompjuterom s ciljem korištenja tog kompjutera za slanje velike količine poruka.

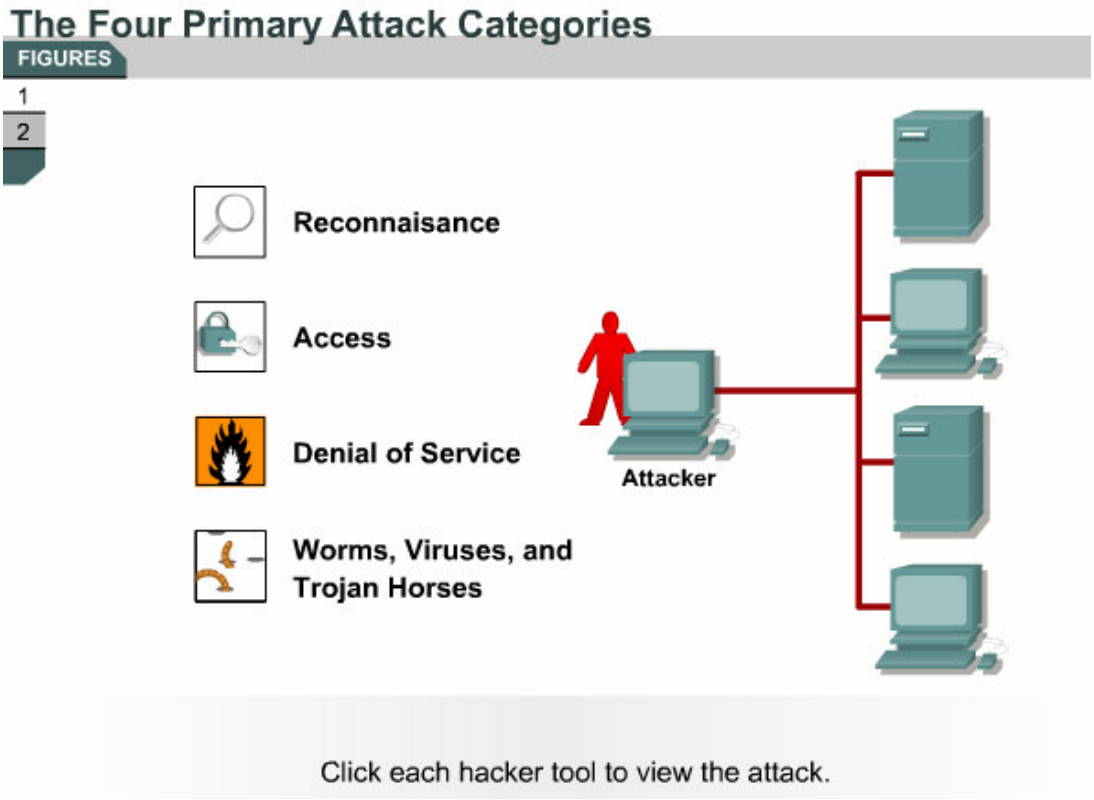
Phisher
Phisher koristi mail ili druge načine s ciljem prevare i dobivanja privatnih, osjetljivih informacija kao na primjer broj kreditne kartice ili razne lozinke. Phisher će se zamaskirati kao povjerljivi sugovornik koji ima legitimno pravo pristupa takvim informacijama.

White hat
White hat je pojam koji opisuje pojedince koji koriste svoje sposobnosti da otkriju slabosti sistema ili mreže i da obavijeste vlasnike mreže o tim slabostima kako bi one mogle biti sređene.

Black hat
Black hat je drugi termin za pojedince koji koriste svoje znanje kompjuterskih sistema za upad u sustav ili mrežu za čije korištenje nisu autorizirani.

1.2 Uvod u slabosti mreže, prijetnje i napade
1.2.3 Napadi

Postoje četiri glavne klase napada kako je prikazano na slici 1.



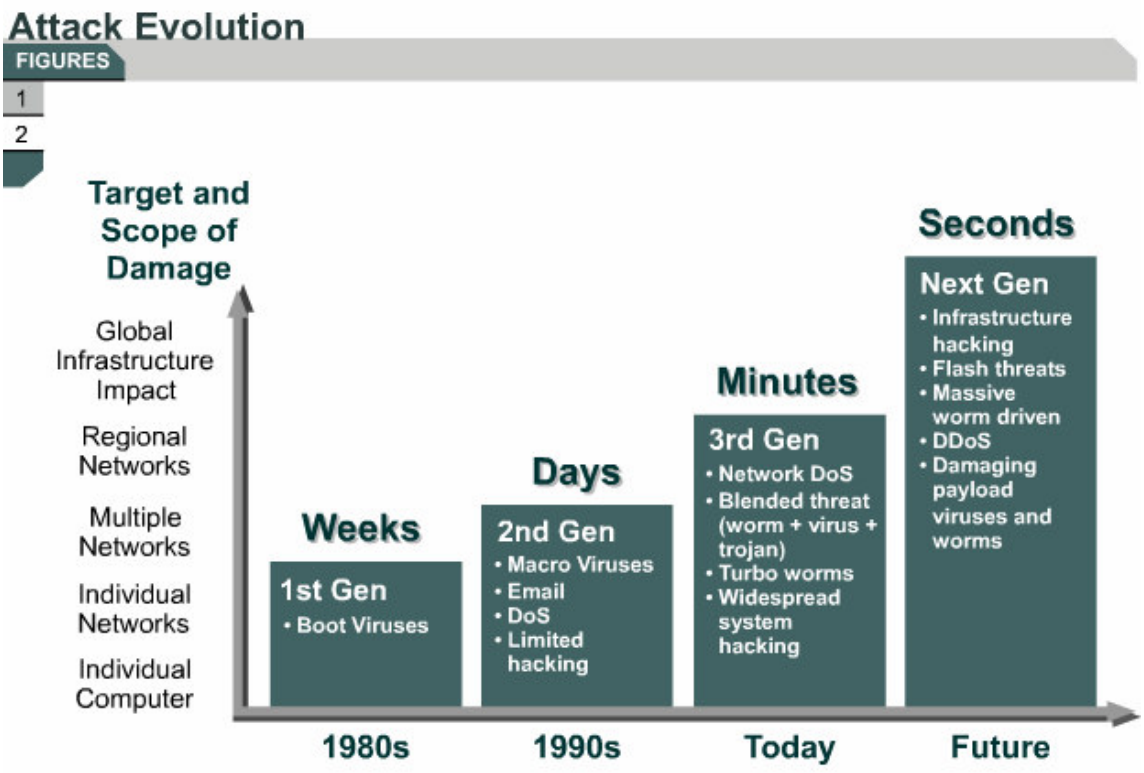
Upit (Reconnaissance)
Upit je neautorizirano otkrivanje i mapiranje sustava, servisa ili slabosti mreže. Još je poznato kao i skupljanje informacija  i u većini slučajeva, prethodi stvarnom pristupu ili napadu Denial of Service (DoS). Upit je nekako analogan ponašanju lopova koji promatra susjedstvo i slabe točke prije provale u kuću kao npr. prazne kuće, slaba vrata ili prozori i sl.

Pristup (Access)
Pristup sustavu je sposobnost neautoriziranog upada kod kojega pojedinac nema autorizirani račun niti lozinku. Upad ili pristup sustavu za koji se nema službeni pristup uključuje pokretanje skripti ili alata koji provjeravaju poznate slabosti sustava ili aplikacija koje su napadnute.

Odbijanje servisa (Denial of Service (DoS))
Odbijanje servisa temelji se na tome da napadač onesposobi ili korumpira mrežu, sustav ili servis s ciljem da ovlašteni korisnici ne mogu pristupiti tom servisu. DoS uključuje bilo rušenje sustava ili njegovo usporavanje do stupnja da je neupotrebljiv. DoS može isto tako biti jednostavan i samo uništavati ili korumpirati podatke. U većini slučajeva, izvođenje napada jednostavno uključuje izvođenje skripte. Napadač ne mora prethodno pristupiti cilju jer način pristupa je sve što se obično traži. Iz tog razloga DoS napad je najopasniji.

Crvi, virusi i Trojanski konji (Worms, Viruses, and Trojan Horses)
Zlonamjerni software se ubacuje u host s ciljem nanošenja štete, korumpiranja sustava, dupliciranja, odbijanja servisa ili pristupa mreži, sustavu ili servisima.

Što je najgore, priroda svih tih napada se stalno mijenja. Od relativno jednostavnih virusa 80-ih do znatno kompleksnijih i zahtjevnijih virusa, DoS napada i zlonamjernih alata koji se danas pojavljuju.
Danas alati za „hakiranje“ su vrlo moćni i široko rasprostranjeni. Pojavljuju se opasnosti samoširećih crva. Također su prošli dani kada je trebalo dani i tjedni da se neki virus proširi po mreži. Sada je širenje prijetnje po mreži na nivou cijelog svijeta samo pitanje minuta. SLAMMER je primjer crva koji se proširio po cijelom svijetu za manje od 10 minuta.




Slijedeće generacije napada širiti će se brzinom sekunde. Ti crvi ili virusi mogu napraviti mnogo više nego samo propteretiti resurse sustava nego s količinom prometa koji su u mogućnosi generirati, mogu značajno utjecati na troškove poduzeća, ukrasti vitalne informacije ili čak obrisati diskove.
Također, postoje bojazni da bi prijetnje sutrašnjice mogle ugroziti samu strukturu interneta.