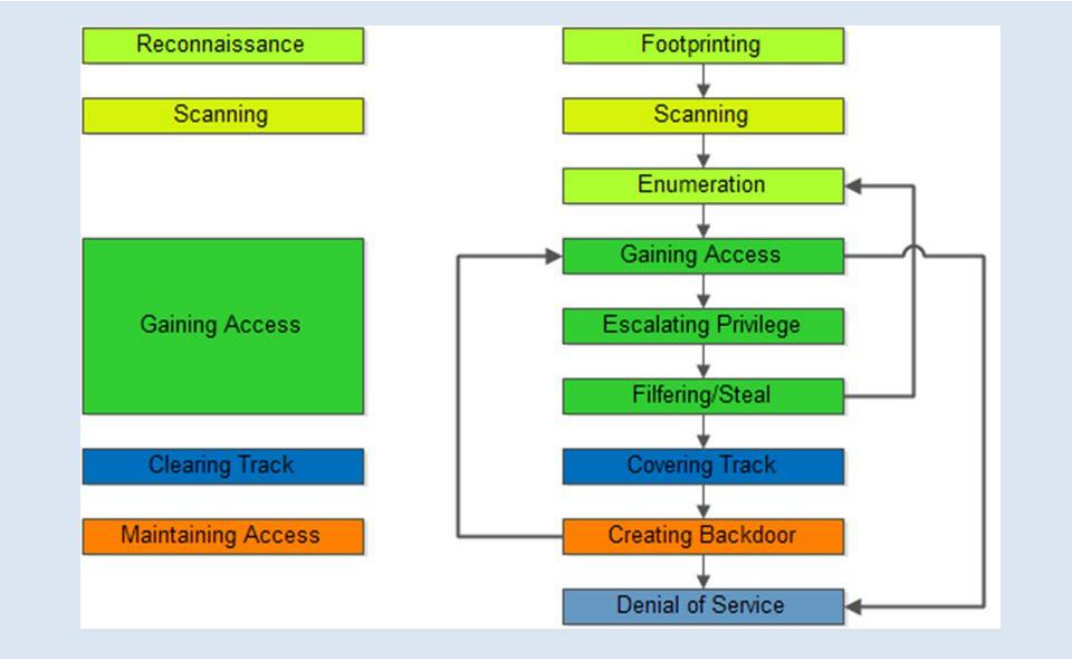
Copyright © September 2023

PERTEMUAN 13

EKSPLOITASI KEAMANAN

A. Anatomi Suatu Serangan Hacking

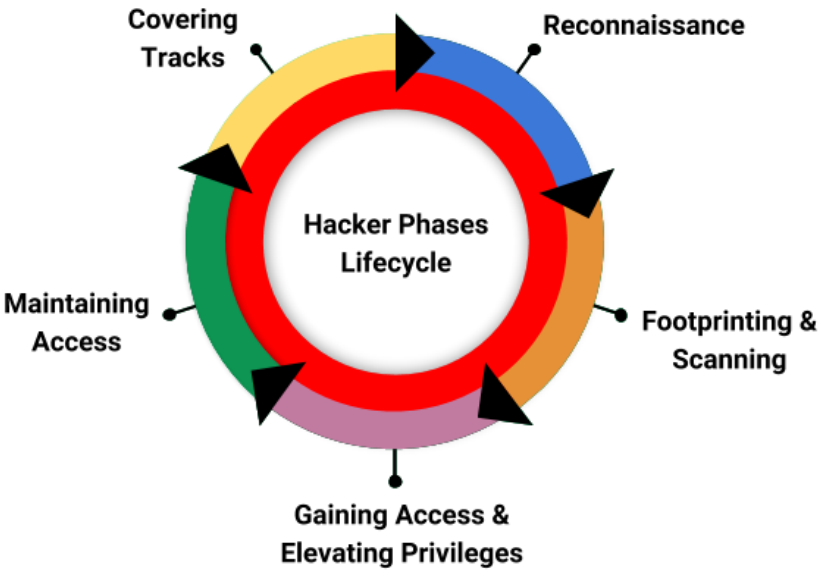


- Footprinting
  i. Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer.

Copyright © September 2023

- Hacking Tools
  i. whois, host, nslookup, dig (tools di sistem UNIX)
  ii. Sam Spade (tools di sistem Windows) http://www.samspade.org.
  iii. ARIN, Traceroute, NeoTrace, VisualRoute, Trace, SmartWhois, Visual Lookout, VisualRoute Mail Tracker, eMailTrackerPro

Copyright © September 2023



B. Scanning
- Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan port scan.
- Mencari informasi mengenai suatu alamat IP dapat menggunakan beberapa software seperti:
    i. WinSuperKit - http://www.mjksoft.com
    ii. Ping Plotter – http://www.pingplotter.com
    iii. SuperScan
    iv. UltraScan
    v. Lain-lain

C. Enumeration
- Telaah intensif terhadap sasaran, yang mencari user account absah, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.

Copyright © September 2023

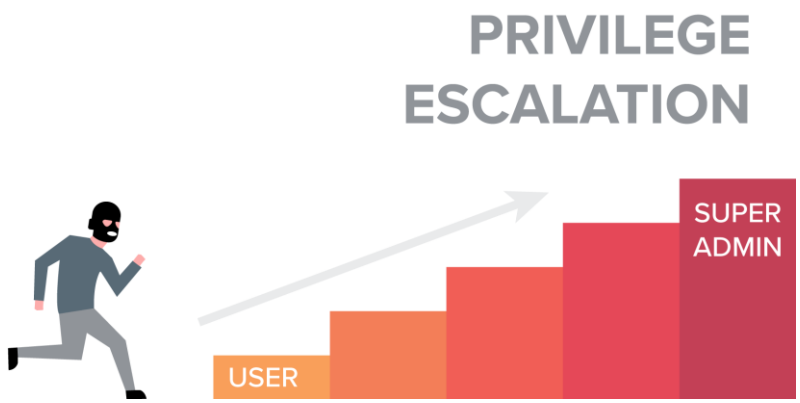
```
sukumar@sukumar-VBox: ~/Desktop/cprog/enum
sukumar@sukumar-VBox:~/Desktop/cprog/enum$ gcc example3.c -o example3
sukumar@sukumar-VBox:~/Desktop/cprog/enum$ ./example3
Setting Hw_Error to IO_ERROR
Value of Hw_Error = 11

Setting Hw_Error to DISK_ERROR
Value of Hw_Error = 12

Setting Hw_Error to NETWORK_ERROR
Value of Hw_Error = 1

Setting Hw_Error to PRINT_ERROR
Value of Hw_Error = 2
sukumar@sukumar-VBox:~/Desktop/cprog/enum$
```

D. Gaining Access

- Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, serta melakukan buffer overflow.

E. Escalating Privilege

- Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc_messages.



F. Pilfering

Copyright © September 2023

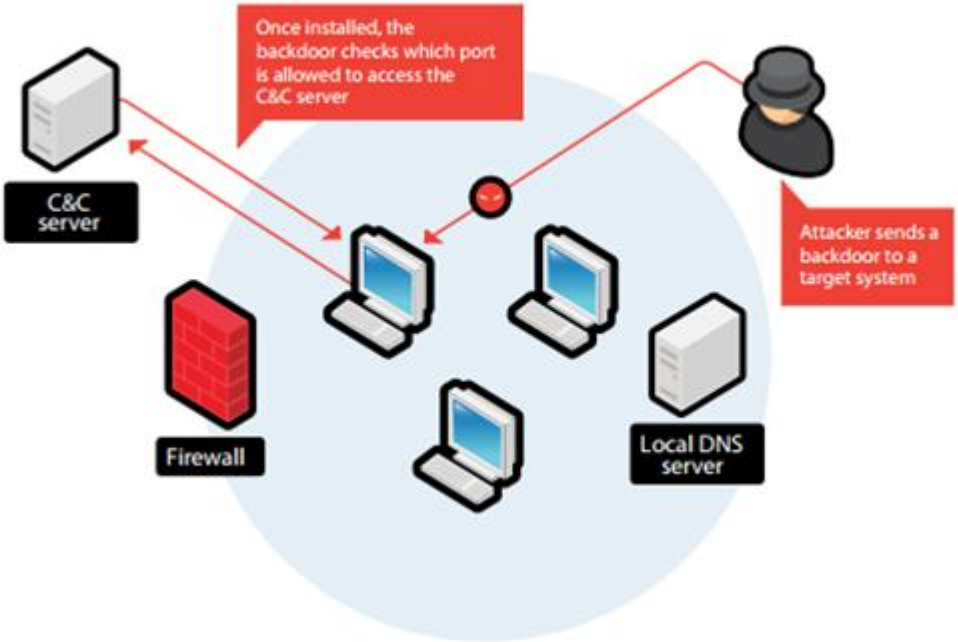
- Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file, dan user data.

G. Covering Tracks

- Begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas.Meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming.
- Dump Event Log, elsave.exe, WinZapper, Evidence Eliminator

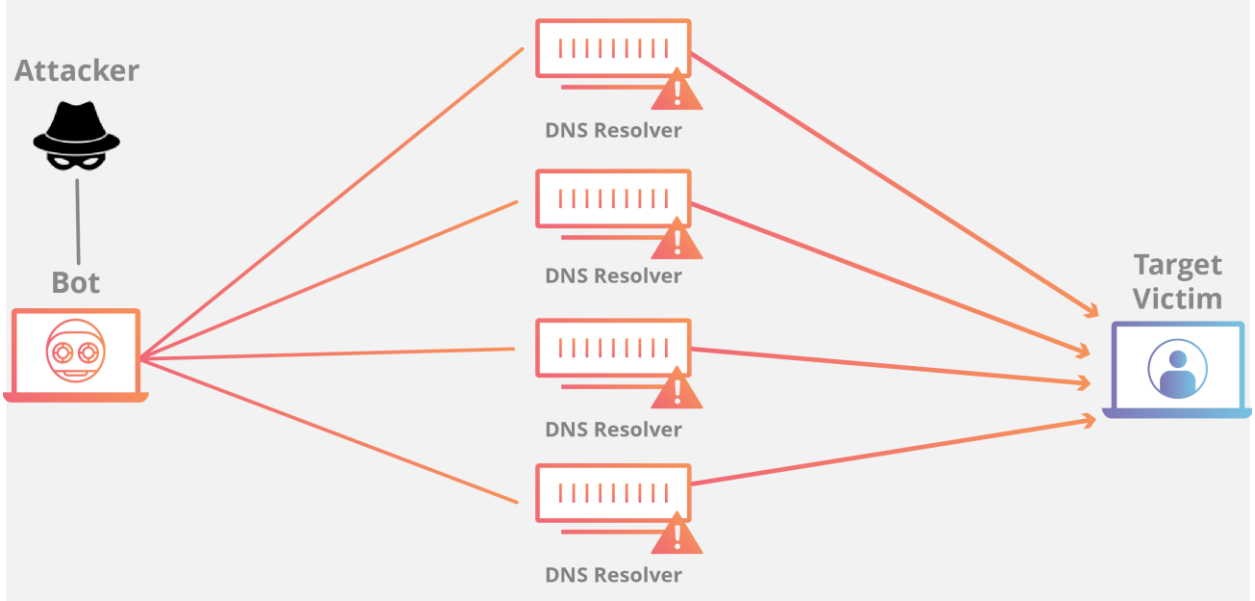
H. Creating Backdoors

- Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk *user account* palsu, menjadwalkan *batch job*, mengubah *startup file*, menanamkan servis pengendali jarak jauh serta *monitoring tool*, dan menggantikan aplikasi dengan trojan.



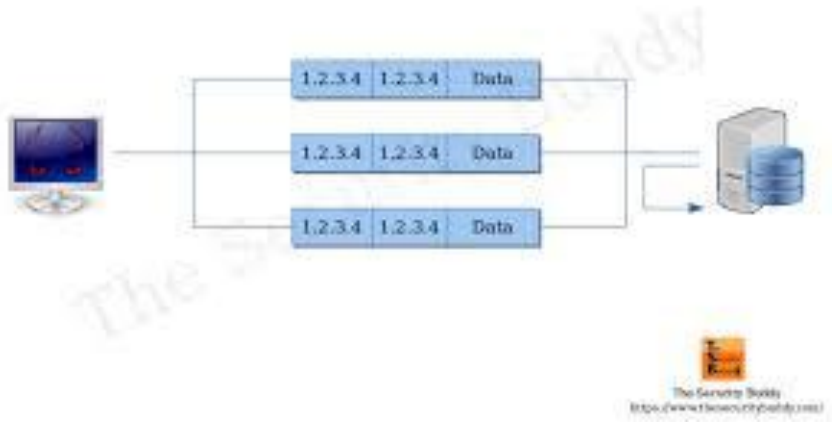
Copyright © September 2023

I. Denial Of Service
- Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir.
- Berusaha mencegah pemakai yang sah untuk mengakses sebuah sumber daya atau informasi
- Biasanya ditujukan kepada pihak-pihak yang memiliki pengaruh luas dan kuat (mis: perusahaan besar, tokoh-tokoh politik, dsb)
- Teknik DoS:
  i. Mengganggu aplikasi (mis: membuat webserver down)
  ii. Mengganggu sistem (mis: membuat sistem operasi down)
  iii. Mengganggu jaringan (mis: dengan TCP SYN flood)
- Contoh: MyDoom worm email (berita dari F-Secure, 28 Januari 2004) http://www.f-secure.com/news/items/news_2004012800.shtml
  i. Ditemukan pertama kali 26 Januari 2004
  ii. Menginfeksi komputer yang diserangnya. Komputer yang terinfeksi diperintahkan untuk melakukan DoS ke www.sco.com pada tanggal 1 Februari 2004 jam 16:09:18
  iii. Pada saat itu, diperkirakan 20-30% dari total lalulintas e-mail di seluruh dunia disebabkan oleh pergerakan worm ini
  iv. Penyebaran yang cepat disebabkan karena:
    - "Penyamaran" yang baik (tidak terlihat berbahaya bagi user)
    - Penyebaran terjadi saat jam kantor
    - Koleksi alamat email sasaran yang agresif (selain mengambil dari address book di komputer korban, juga membuat alamat email sendiri)



Copyright © September 2023

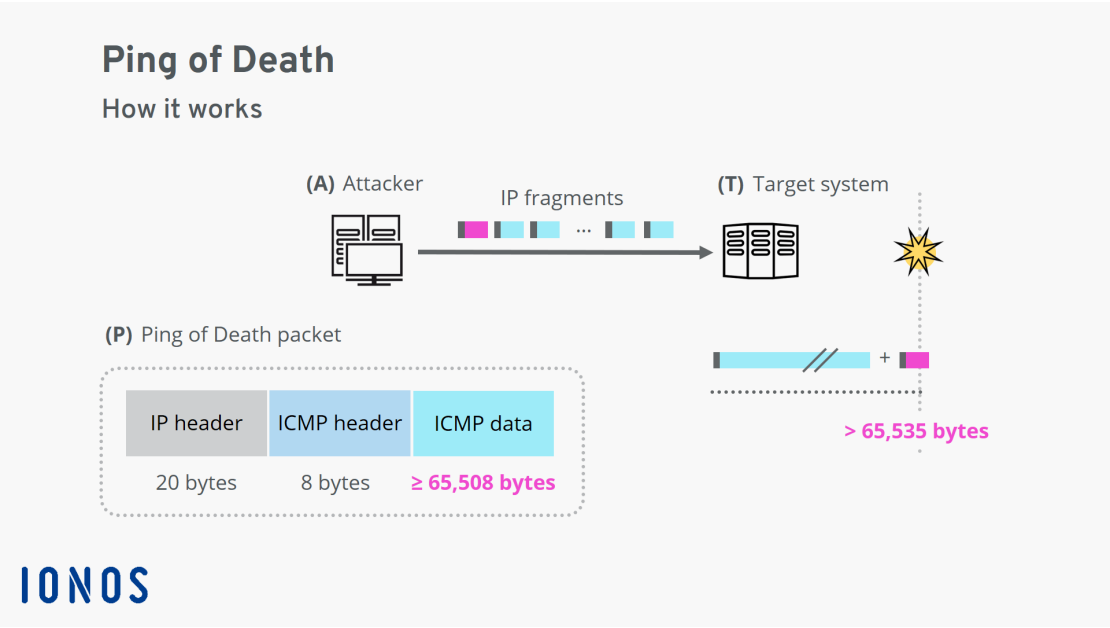
- Klasifikasi DoS Attack
  i. LAND Attacks, Smurf, Buffer Overflow Attacks
    - LAND attack : serangan terhadap suatu server/komputer yang terhubung dalam suatu jaringan yang bertujuan untuk menghentikan layanan yang diberikan oleh server tersebut.
    - Tipe serangan disebut sebagai Denial of Service (DoS) attack.
    - LAND attack dikategorikan sebagai serangan SYN (SYN attack) karena menggunakan packet SYN (synchronization) pada waktu melakukan 3-way handshake untuk membentuk suatu hubungan antara client dengan server berbasis TCP/IP.



Copyright © September 2023

ii. Ping Of death

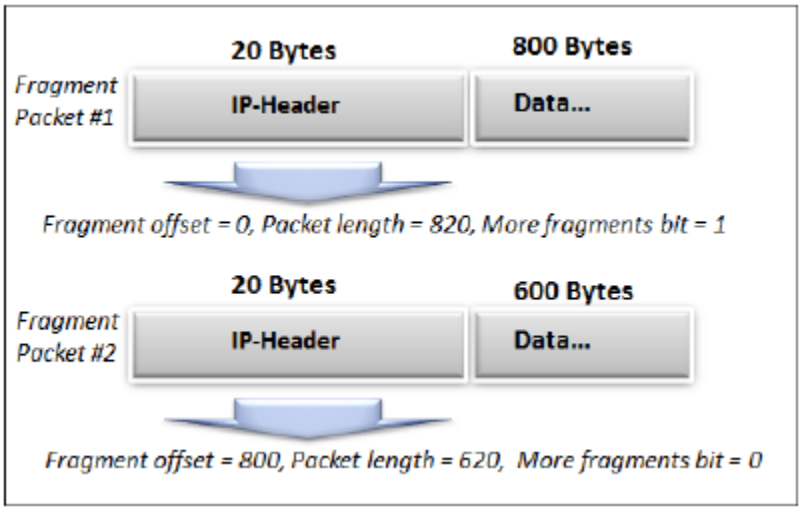
- Ping of Death merupakan suatu serangan DoS terhadap suatu server/komputer yang terhubung dalam suatu jaringan.
- Serangan ini memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau pemecahan paket, dan juga kenyataan bahwa batas ukuran paket di protokol IP adalah 65536 byte atau 64 kilobyte.
- Penyerang dapat mengirimkan berbagai paket ICMP (digunakan untuk melakukan ping) yang terfragmentasi sehingga waktu paket-paket tersebut disatukan kembali, maka ukuran paket seluruhnya melebihi batas 65536 byte



Copyright © September 2023

iii. Teardrop

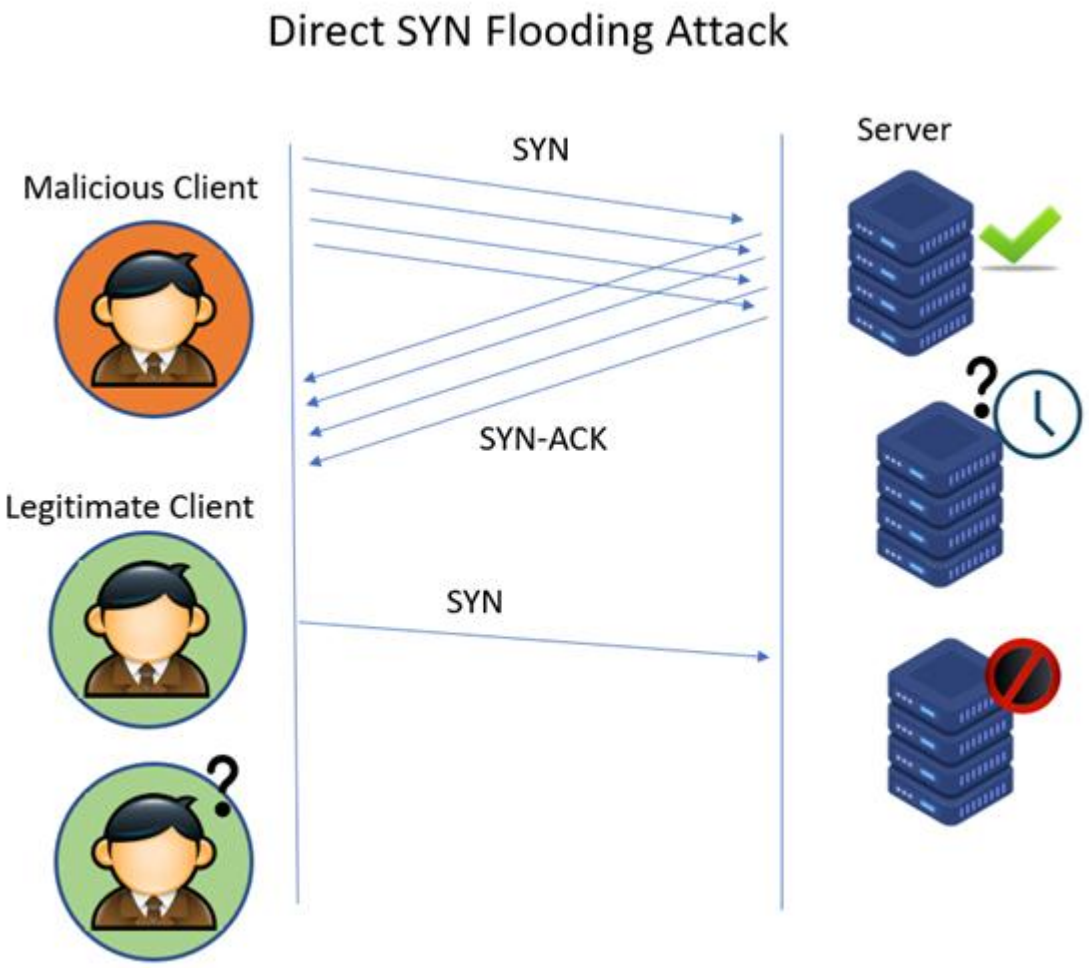
- Teardrop attack adalah suatu serangan bertipe DoS terhadap suatu server/komputer yang terhubung dalam suatu jaringan.
- Teardrop attack ini memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau pemecahan paket, dan kelemahan yang ada di TCP/IP pada waktu paket-paket yang terfragmentasi tersebut disatukan kembali.
- Dalam suatu pengiriman data dari satu komputer ke komputer yang lain melalui jaringan berbasis TCP/IP, maka data tersebut akan dipecah-pecah menjadi beberapa paket yang lebih kecil di komputer asal, dan paket-paket tersebut dikirim dan kemudian disatukan kembali di komputer tujuan.



Copyright © September 2023

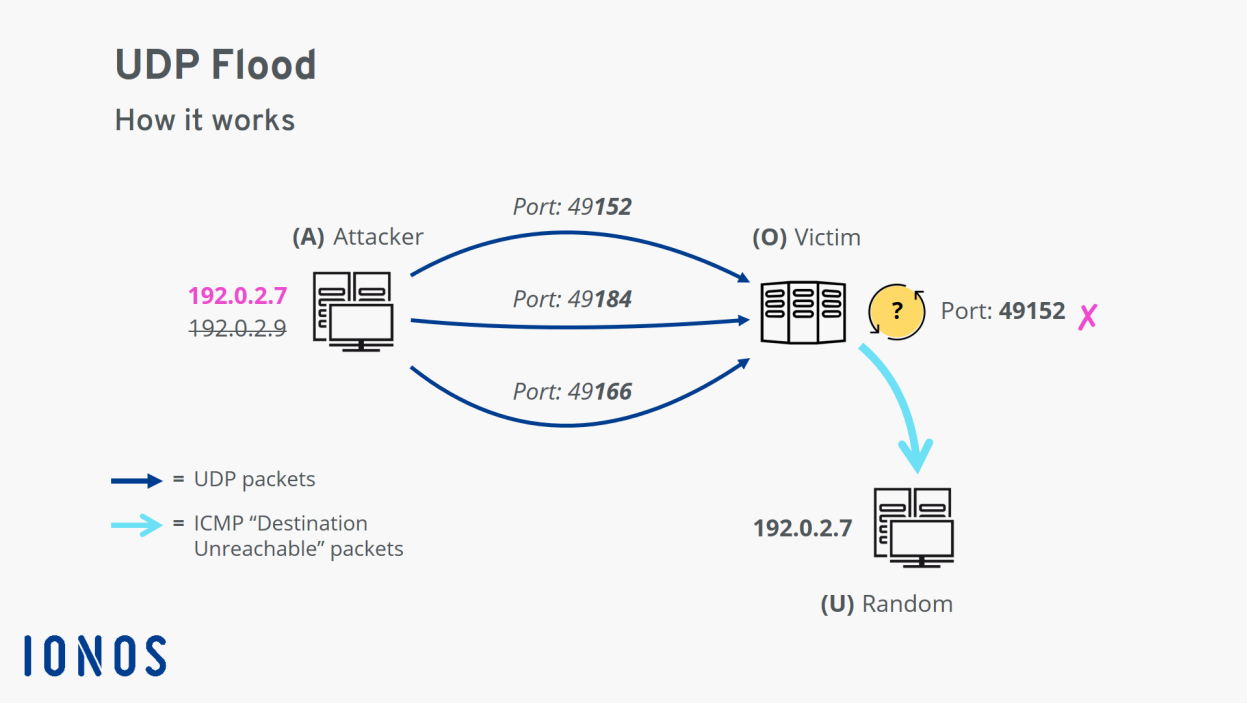
iv. SYN

- Half-open connection attack juga disebut sebagai SYN attack karena memanfaatkan paket SYN (synchronization) dan kelemahan yang ada di 3-way handshake pada waktu hubungan TCP/IP ingin dibentuk antara 2 komputer.



v. Tribal Flow Attack

Copyright © September 2023

vi. UDP Bomb Attack

- UDP Bomb attack adalah suatu serangan bertipe DoS terhadap suatu server atau komputer yang terhubung dalam suatu jaringan.
- Untuk melakukan serangan UDP Bomb terhadap suatu server, seorang penyerang mengirim sebuah paket UDP (User Datagram Protocol) yang telah dispoof atau direkayasa sehingga berisikan nilai-nilai yang tidak valid di field-field tertentu.
- Jika server yang tidak terproteksi masih menggunakan sistem operasi (operating system) lama yang tidak dapat menangani paket-paket UDP yang tidak valid ini, maka server akan langsung crash