# Introduction to Networking

## Networking Overview

Ցանցը թույլ է տալիս երկու համակարգիչներին հաղորդակցվել միմյանց հետ: Կան բազմաթիվ տոպոլոգիաներ (ցանց/ծառ/աստղ), միջոցներ (ethernet/fiber/coax/wireless) և պրոտոկոլներ (TCP/UDP/IPX), որոնք կարող են օգտագործվել ցանցի ապահովման համար: Անվտանգության մասնագետների համար կարևոր է հասկանալ ցանցային տեխնոլոգիաները, քանի որ երբ ցանցը ձախողվում է, սխալը կարող է լինել աննկատ, ինչը մեզ կարող է ստիպել բազմաթիվ բաներ բաց թողնել:

Մեծ, հարթ ցանցի կազմակերպումը չափազանց դժվար չէ, և այն կարող է լինել հուսալի ցանց, առնվազն գործնականում: Այնուամենայնիվ, հարթ ցանցը նման է տուն կառուցելու հողատարածքում և համոզված լինել, որ այն անվտանգ է, քանի որ դռանը կողպեք կա: Ստեղծելով բազմաթիվ ավելի փոքր ցանցեր և ապահովելով դրանց միջև հաղորդակցությունը, մենք կարող ենք ավելացնել պաշտպանական շերտեր: Ցանցի շուրջ պտտվելը դժվար չէ, բայց այն արագ և անաղմուկ կատարելը դժվար է և կդանդաղեցնի հարձակվողներին: Վերադառնալով տան օրինակին, դիտարկենք հետևյալ օրինակները.

## Example No. 1

Օրինակ № 1

Փոքր ցանցեր կառուցելն ու դրանց շուրջ հասանելիության վերահսկողության ցուցակներ տեղադրելը նման է սեփականության սահմանի շուրջ ցանկապատ կառուցելուն, որն ստեղծում է կոնկրետ մուտքի և ելքի կետեր: Այո, հարձակվողը կարող է ցանկապատը թռչել, բայց սա կասկածելի է և տարածված չէ, ինչը թույլ է տալիս արագ հայտնաբերել այն որպես չարամիտ գործողություն: Ինչո՞ւ է տպագրիչի ցանցը խոսում սերվերների հետ HTTP-ով:

## Example No. 2

Յուրաքանչյուր ցանցի նպատակը քարտեզագրելու և փաստաթղթավորելու համար ժամանակ հատկացնելը նման է տարածքի շուրջ լույսեր տեղադրելուն՝

համոզվելու համար, որ բոլոր գործողությունները տեսանելի են: Ինչո՞ւ է տպիչների ցանցը ընդհանրապես կապվում ինտերնետի հետ:

## Example No. 3

Պատուհանների շուրջը թփեր ունենալը խանգարում է մարդկանց՝ պատուհանը բացելու փորձերը: Ինչպես Suricata կամ Snort ներխուժումների հայտնաբերման համակարգերը խանգարում են ցանցային սկանավորումների իրականացմանը: Ինչո՞ւ է պորտի սկանավորումը սկսվել printer ցանցից:

Այս օրինակները կարող են անհեթեթ թվալ, և ողջամիտ է արգելափակել տպիչի կողմից վերը նշված բոլոր գործողությունները կատարելու հնարավորությունը: Այնուամենայնիվ, եթե տպիչը գտնվում է «հարթ /24 ցանցում» և ստանում է DHCP հասցե, ապա նման սահմանափակումներ կիրառելը կարող է դժվար լինել:

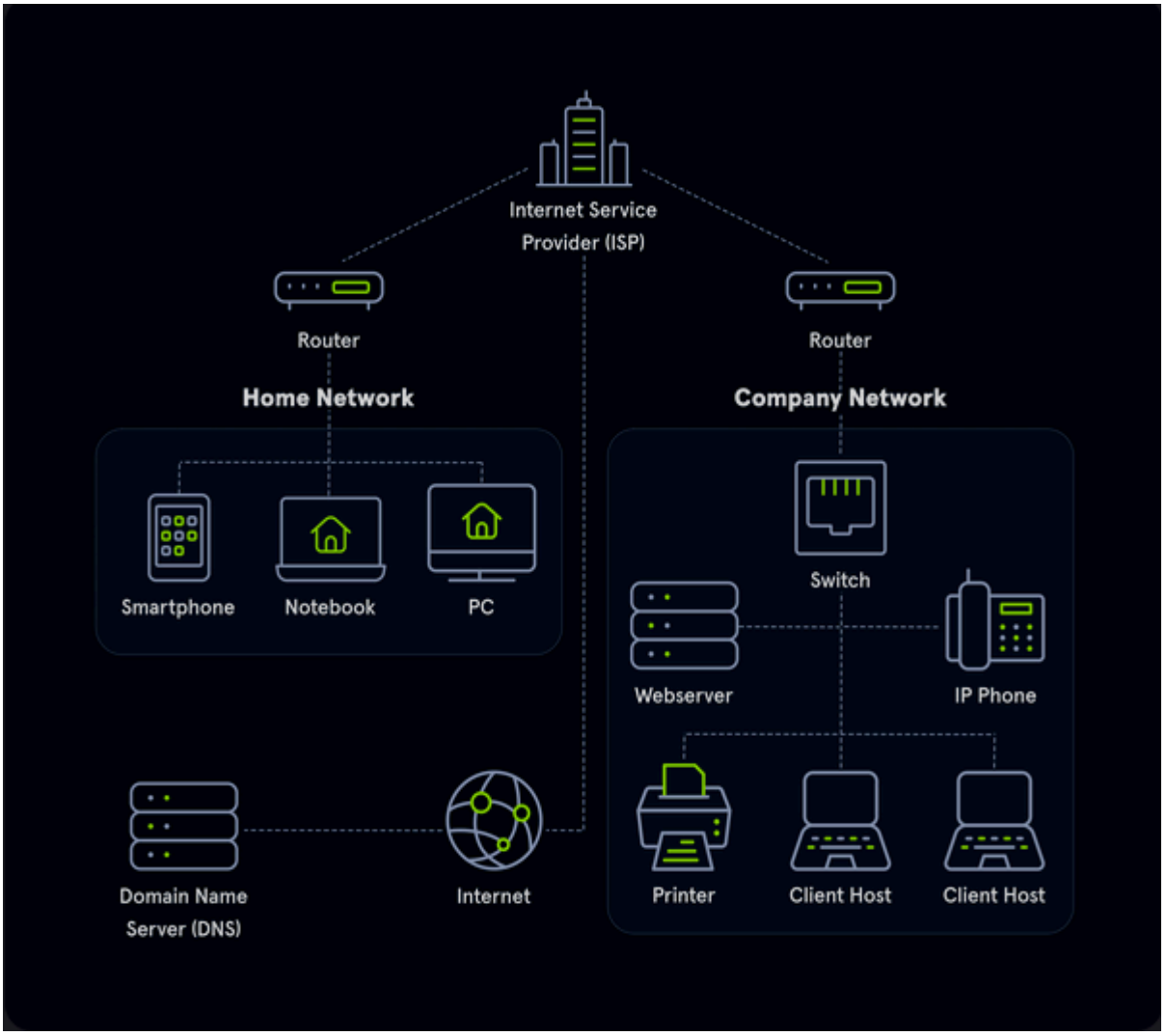
## Story Time - A Pentesters Oversight

Շատ ցանցեր օգտագործում են /24 ենթացանց, այնքան որ շատ ներթափանցումային փորձարկողներ առանց ստուգելու կարգավորում են այս ենթացանցի mask-ը (255.255.255.0): /24 ցանցը թույլ է տալիս համակարգիչներին հաղորդակցվել իրար հետ, եթե IP հասցեի առաջին երեք օկտետները նույնն են (օրինակ՝ 192.168.1.xxx): Subnetդիմակը /25 դարձնելը կիսում է այս տիրույթը կեսի, և համակարգիչը կարող է հաղորդակցվել միայն "իր կեսի" համակարգիչների հետ: Մենք տեսել ենք ներթափանցումային փորձարկումների զեկույցներ, որտեղ փորձագետը պնդում էր, որ Դոմենի կոնտրոլերը անջատված է, երբ իրականում այն պարզապես գտնվում էր այլ ցանցում: Ցանցի կառուցվածքը հետևյալն էր՝

- `Server Gateway: 10.20.0.1/25`
- `Domain Controller: 10.20.0.10/25`
- `Client Gateway: 10.20.0.129/25`
- `Client Workstation: 10.20.0.200/25`
- `Pentester IP: 10.20.0.252/24 (Set Gateway to 10.20.0.1)`

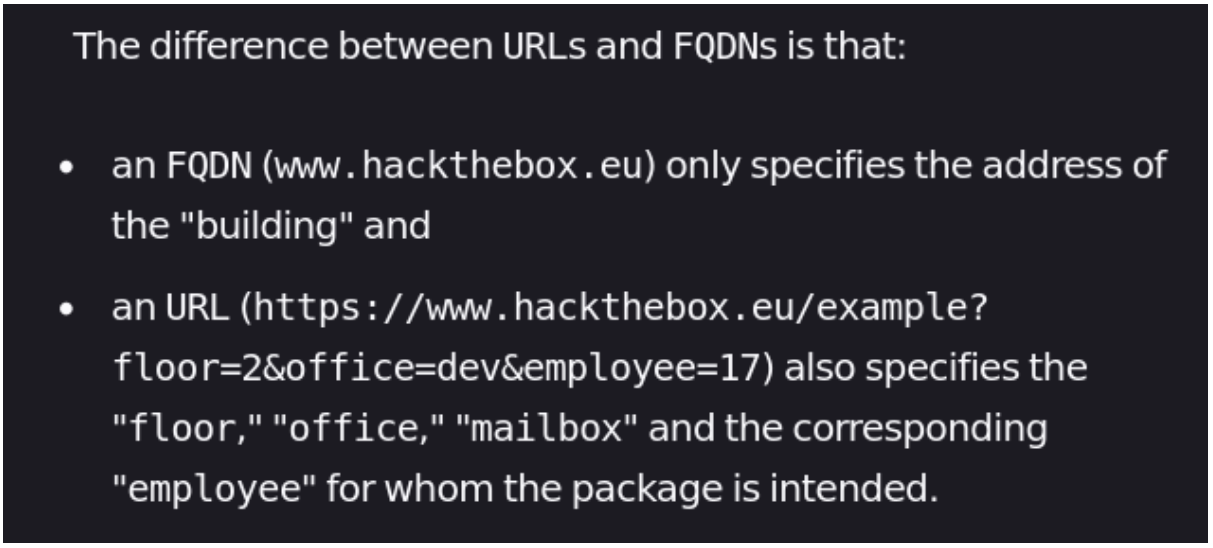
Հետազոտողը կապ է հաստատել Հաճախորդի աշխատակայանների հետ և կարծել է, որ նրանք գերազանց աշխատանք են կատարել, քանի որ նրանց հաջողվել է Impacket-ի միջոցով գողանալ աշխատակայանի գաղտնաբառը: Այնուամենայնիվ, ցանցը հասկանալու անկարողության պատճառով նրանց երբեք չի հաջողվել դուրս գալ Հաճախորդի ցանցից և հասնել ավելի «բարձր արժեք» ունեցող թիրախների, ինչպիսիք են տվյալների բազայի սերվերները: Հուսով եմ, եթե սա ձեզ համար խճճված է թվում, դուք կարող եք վերադառնալ այս հայտարարությանը մոդուլի վերջում և հասկանալ այն:

## Basic Information



Ամբողջ ինտերնետը հիմնված է բազմաթիվ ենթաբաժանված ցանցերի վրա, ինչպես ցույց է տրված օրինակում և նշված է որպես «Տնային ցանց» և «Ընկերության ցանց»: Մենք կարող ենք պատկերացնել ցանցային կապը որպես մեկ համակարգչի կողմից ուղարկված և մյուսի կողմից ստացված փոստի կամ ծանրոցների առաքում:

Ենթադրենք, որ մենք պատկերացնում ենք մի սցենար, որ ուզում ենք այցելել ընկերության կայք մեր «Տնային ցանցից»: Այդ դեպքում մենք տվյալներ ենք փոխանակում ընկերության կայքի հետ, որը գտնվում է նրանց «Ընկերության ցանցում»: Ինչպես նամակներ կամ փաթեթներ ուղարկելու դեպքում, մենք գիտենք այն հասցեն, որտեղ պետք է գնան փաթեթները: Կայքի հասցեն կամ միասնական ռեսուրսների որոնիչը-Uniform Resource Locator (URL), որը մենք մուտքագրում ենք մեր զննարկիչում, հայտնի է նաև որպես լիովին որակավորված դոմեյնի անուն- Fully Qualified Domain Name (FQDN):




Ճիշտ է, մենք գիտենք հասցեն, բայց ոչ հասցեի ճշգրիտ աշխարհագրական դիրքը: Այս դեպքում փոստային բաժանմունքը կարող է որոշել ճշգրիտ դիրքը, որից հետո փաստաթղթերը փոխանցվում են ցանկալի վայր: Այսպիսով, մեր փոստային բաժանմունքը փոխանցում է մեր փաստաթղթերը գլխավոր փոստային բաժանմունք, որը ներկայացնում է մեր ինտերնետ պրովայդերը-Internet Service Provider (ISP):

Մենք ավելի պարզ և ճշգրիտ կքննարկենք ճշգրիտ ներկայացումներն ու սահմանումները այլ բաժիններում:

Մեր փոստատունը մեր ռաուտերն է, որն այն օգտագործում ենք ցանցային կապի համար "Internet"-ին միանալու համար:

Անմիջապես երբ մեր փաթեթը մեր փոստային բաժանմունքով (ռաուտեր) ուղարկվում է, փաթեթը փոխանցվում է գլխավոր փոստային բաժանմունքի (ISP): Այս գլխավոր փոստային բաժանմունքը նայում է հասցեների գրանցամատյանի/հեռախոսագրքի (Domain Name Service) ՝ որտեղ գտնվում է այդ հասցեն և վերադարձնում է համապատասխան աշխարհագրական կոորդինատները (IP հասցե): Այժմ, երբ մենք գիտենք հասցեի ճշգրիտ գտնվելու վայրը, մեր փաթեթը ուղարկվում է ուղիղ այնտեղ՝ ուղիղ թռիչքով մեր գլխավոր փոստային բաժանմունքի միջոցով:

Վեբ սերվերը ստանալով մեր փաթեթը՝ պարունակող հարցումը իրենց կայքի տեսքի վերաբերյալ, վերադարձնում է մեզ փաթեթ՝ կայքի ներկայացման տվյալներով՝ անցնելով "Company Network"-ի փոստային բաժանմունքով (ռաուտերով) դեպի նշված վերադարձի հասցե (մեր IP հասցեն):

## Extra Points

- Վեբ սերվերը պետք է գտնվի DMZ-ում (ապառազմականացված գոտում)- DMZ (Demilitarized Zone) , քանի որ ինտերնետի հաճախորդները կարող են նախաձեռնել հաղորդակցություն կայքի հետ, ինչը ավելի հավանական է դարձնում դրա խարդախության ենթարկվելը: Այն առանձին ցանցում տեղադրելը թույլ է տալիս ադմինիստրատորներին տեղադրել ցանցային պաշտպանություն վեբ սերվերի և այլ սարքերի միջև:

- Տերմինալները պետք է գտնվեն իրենց ցանցում, և իդեալական աշխարհում յուրաքանչյուր տերմինալ պետք է ունենա Host-Based Firewall կանոն, որը կխափանի նրա հաղորդակցությունը այլ տերմինալների հետ: Եթե Տերմինալը գտնվում է նույն ցանցում, ինչ Սերվերը, ցանցային հարձակումները, ինչպիսիք են spoofing-ը կամ man in the middle-ը, դառնում են ավելի մեծ խնդիր:

- Աշխատանքային կայանները պետք է լինեն իրենց սեփական ցանցում, և իդեալական աշխարհում յուրաքանչյուր աշխատանքային կայան պետք է ունենա Host-Based Firewall կանոն, որը կանխում է դրա կապը այլ աշխատանքային կայանների հետ: Եթե աշխատանքային կայանը գտնվում է սերվերի հետ նույն ցանցում, ցանցային հարձակումները,

ինչպիսիք են կեղծումը կամ man in the middle , շատ ավելի մեծ խնդիր են դառնում:

- IP հեռախոսները պետք է լինեն իրենց սեփական ցանցում: Անվտանգության տեսանկյունից սա նախատեսված է համակարգիչների կողմից հաղորդակցությանը գաղտնալսելու հնարավորությունը կանխելու համար: Անվտանգությունից բացի, հեռախոսները եզակի են նաև նրանով, որ լատենտությունը/հետաձգումը զգալի է: Դրանք սեփական ցանցում տեղադրելը կարող է թույլ տալ ցանցային ադմինիստրատորներին առաջնահերթություն տալ իրենց երթևեկությանը՝ բարձր լատենտությունն ավելի հեշտությամբ կանխելու համար:

- Տպիչները պետք է լինեն իրենց սեփական ցանցում: Սա կարող է տարօրինակ հնչել, բայց տպիչը պաշտպանելը գրեթե անհնար է: Windows-ի աշխատանքի պատճառով, եթե տպիչը տպման աշխատանքի ընթացքում համակարգչին տեղեկացնում է, որ անհրաժեշտ է նույնականացում, այդ համակարգիչը կփորձի NTLMv2 նույնականացում, ինչը կարող է հանգեցնել գաղտնաբառերի գողության: Բացի այդ, այս սարքերը հիանալի են պահպանման համար և, ընդհանուր առմամբ, դրանց ուղարկվում է մեծ քանակությամբ զգայուն տեղեկատվություն:

## Զվարճալի պատմություն

COVID-ի ժամանակ ինձ հանձնարարվեց ֆիզիկական ներթափանցման թեստ անցկացնել նահանգների սահմաններից այն կողմ, և իմ նահանգում տանը մնալու հրաման կար: Այն ընկերությունը, որը ես փորձարկում էի, գրասենյակում քիչ անձնակազմ ուներ: Ես որոշեցի գնել թանկարժեք տպիչ և օգտագործել այն՝ հակառակ շերտ տեղադրելու համար, որպեսզի, երբ այն միանար ցանցին, ինձ շերտ ուղարկեր (հեռակա մուտք): Այնուհետև ես տպիչը ուղարկեցի ընկերությանը և ֆիշինգային էլ. նամակ ուղարկեցի՝ շնորհակալություն հայտնելով աշխատակիցներին գալու համար և բացատրելով, որ տպիչը պետք է թույլ տա նրանց ավելի արագ տպել կամ սկանավորել իրերը, եթե նրանք ցանկանում են մի քանի օրով տուն բերել որոշ իրեր՝ տնային պայմաններում աշխատելու համար: Տպիչը միացավ գրեթե անմիջապես, և նրանց դոմեյնի ադմինիստրատորի համակարգիչը բավականին բարի էր տպիչին ուղարկելու իր մուտքային տվյալները:

> Եթե հաճախորդը նախագծած լիներ անվտանգ ցանց, այս հարձակումը, հավանաբար, հնարավոր չէր լինի մի շարք պատճառներով.

- Տպիչը չպետք է կարողանար միանալ ինտերնետին
- Աշխատանքային կայանը չպետք է կարողանար կապ հաստատել տպիչի հետ 445 port-ի միջոցով
- Տպիչը չպետք է կարողանա միանալ աշխատանքային կայաններին: Որոշ դեպքերում տպիչ/սկաներ համակցությունները պետք է կարողանան կապ հաստատել փոստային սերվերի հետ՝ սկանավորված փաստաթղթերը էլեկտրոնային փոստով ուղարկելու համար: