TK2100

T-07

**Nettverk og internett 2**

Notater:

Det står for Denial Of Service handler om å forhindre andre brukere frå å få tilgang til en teneste ved å enten kræsje tjenesten eller ved å overbelaste den. DOS er et vanlig angrep mot WEB servere

1. **Hva står «DNS» for?**

Det står for Domain Name System og er domenet navnet til en nettside eks vg.no der domenet navnet til landet er no

1. **Hva er forskjellen på Pharming og Phishing?**

Pharming:

Det er å legge inn falske ip adresser med eks DNS navn som har som mål å få brukeren til å laste ned en malware eller legge inn brukernavn/passord e.l

Fordelen med dette er at bruker går selv inn på nettsiden og kan bli lettere manipulert.

Phishing:

Er å lage en nettside som ser ekte ut og har som mål at brukeren oppgir sensitiv opplysninger som brukernavn og passord , kredittinformasjon.

Men ulempen med dette er at man må manipulere bruker til å trykke på en link

1. **Hva er DNS cache-forgiftning?**

Det gir DNS tjenere eller resolvere falske svar og få dem cashet.

Domenet systemet benytter seg av 16 bits Request ID

Denne Cache kan dermed f.eks. forgiftet dersom en NS:

Ser bort fra ID og har forutsigbar ID

Aksepterer DNS RR som den ikke har spurt om MIMT noen fanger opp request og sender reply som ankommer før den ekte

1. **Hvorfor kan vi bare gjette oss til DNS id? (hint: Birthday Paradox)**

Hvis du har 23 studenter i et klasserom så er det 50% sjanse for at du har bursdag samme dato. Det er et x antall DNS ideer som vil si at vi kan gjette oss fram til svaret. Man har 50% suksessrate ved 231 forsøk.

1. **Hva er en brannmur?**

En brannmur er en samling av sikkerhetstiltak som skal forhindre uautorisert tilgang til et nettverk (av computere) . Den skal isolere LAN’et og hindre at brann sprer seg inn / ut fra/til andre steder (Internett)

1. **Hva er white-og-white-listing? Hva er best?**

Black list er når pakker slipper gjennom bortsett fra de som er definert i reglene , og er den mest fleksible men naiv da den forutsetter at man kan forutsette alle trusler som kan oppstå

White List : Ingen pakker slipper gjennom , bortsett fra de som er definert i reglene.

1. **Hva er «Tunneling»?**

Tunneling forhindrer avlytting uten å endre en annen software er å bruke tunneling protokoll

I slike protokoller krypteres kommunikasjonen automatisk og gjør avlyttigen umulig/vanskelig. Pakker sendt over nettet kan automatisk krypteres med tunneling.

1. **Hva står «VPN» for?**

Det står for Virtual Private Network og er en fellesbetegnelse på ulike teknologier som tillater sikker tilgang til private nettverk over internettet og VPN skal garantere data konfidensialitet , integritet og autensiering til tross for usikker transport nettverk.

Hovedtyper:

Remote Access VPN

Site to site VPN

Og er typisk sikret med enten IPSec eller SSL/TLS

1. **Hva betyr «portscanning»? Hva brukes det til?**

Portscanning er en metode brukt av et portscanner program for å undersøke en server eller vert for åpne porter og er også en måte for å sjekke hvilke porter som er åpne i et nettverk og hvilke tjenere som er tilgjengelig på hostmaskinen

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 16:11 Vest-Europa (normaltid)

NSE: Loaded 155 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 16:11

Completed NSE at 16:11, 0.00s elapsed

Initiating NSE at 16:11

Completed NSE at 16:11, 0.00s elapsed

Initiating NSE at 16:11

Completed NSE at 16:11, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 16:11

Completed Parallel DNS resolution of 1 host. at 16:11, 0.20s elapsed

Initiating SYN Stealth Scan at 16:11

Scanning localhost (127.0.0.1) [1000 ports]

Discovered open port 135/tcp on 127.0.0.1

Discovered open port 8080/tcp on 127.0.0.1

Discovered open port 445/tcp on 127.0.0.1

Discovered open port 3306/tcp on 127.0.0.1

Discovered open port 2869/tcp on 127.0.0.1

Discovered open port 48080/tcp on 127.0.0.1

Discovered open port 3580/tcp on 127.0.0.1

Discovered open port 5357/tcp on 127.0.0.1

Discovered open port 61900/tcp on 127.0.0.1

Completed SYN Stealth Scan at 16:11, 0.17s elapsed (1000 total ports)

Initiating Service scan at 16:11

Scanning 9 services on localhost (127.0.0.1)

Completed Service scan at 16:11, 26.04s elapsed (9 services on 1 host)

Initiating OS detection (try #1) against localhost (127.0.0.1)

Retrying OS detection (try #2) against localhost (127.0.0.1)

WARNING: OS didn't match until try #2

NSE: Script scanning 127.0.0.1.

Initiating NSE at 16:11

Completed NSE at 16:12, 65.97s elapsed

Initiating NSE at 16:12

Completed NSE at 16:12, 7.05s elapsed

Initiating NSE at 16:12

Completed NSE at 16:12, 0.00s elapsed

Nmap scan report for localhost (127.0.0.1)

Host is up (0.00020s latency).

Not shown: 991 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

445/tcp open microsoft-ds?

2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

3306/tcp open mysql MySQL 8.0.26

| ssl-cert: Subject: commonName=MySQL\_Server\_8.0.26\_Auto\_Generated\_Server\_Certificate

| Issuer: commonName=MySQL\_Server\_8.0.26\_Auto\_Generated\_CA\_Certificate

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2021-08-24T10:08:48

| Not valid after: 2031-08-22T10:08:48

| MD5: 694e c736 c45d 1b98 3e99 02c6 f3d9 ada9

|\_SHA-1: 77d0 2777 14f6 39b7 6708 4270 4139 8f50 efeb 9f31

|\_ssl-date: TLS randomness does not represent time

| mysql-info:

| Protocol: 10

| Version: 8.0.26

| Thread ID: 350

| Capabilities flags: 65535

| Some Capabilities: IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, IgnoreSigpipes, SupportsLoadDataLocal, LongPassword, InteractiveClient, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, FoundRows, Support41Auth, SupportsCompression, ODBCClient, SupportsTransactions, LongColumnFlag, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins

| Status: Autocommit

| Salt: \x03gU\*41<5

| 2qt\x07\x1C(Ga\x1E\x17

|\_ Auth Plugin Name: caching\_sha2\_password

3580/tcp open http National Instruments LabVIEW service locator httpd 1.0.0

|\_http-server-header: NI Service Locator/1.0.0 (SLServer)

|\_http-title: Did not follow redirect to http://LOCALHOST:3582

| http-methods:

|\_ Supported Methods: OPTIONS GET HEAD POST

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Service Unavailable

8080/tcp open http Embedthis HTTP lib httpd

|\_http-server-header: Embedthis-http

| http-methods:

|\_ Supported Methods: OPTIONS GET HEAD POST

|\_http-title: Not Found

48080/tcp open ossec-agent OSSEC Agent

61900/tcp open ossec-agent OSSEC Agent

Device type: general purpose

Running: Microsoft Windows 10

OS CPE: cpe:/o:microsoft:windows\_10

OS details: Microsoft Windows 10 1809 - 1909

Network Distance: 0 hops

TCP Sequence Prediction: Difficulty=261 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-security-mode:

| 3.1.1:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2022-03-08T15:11:48

|\_ start\_date: N/A

NSE: Script Post-scanning.

Initiating NSE at 16:12

Completed NSE at 16:12, 0.00s elapsed

Initiating NSE at 16:12

Completed NSE at 16:12, 0.00s elapsed

Initiating NSE at 16:12

Completed NSE at 16:12, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 112.28 seconds

Raw packets sent: 1038 (48.804KB) | Rcvd: 2091 (89.540KB)