Port Scanner

Internetprogrammering – Stationära enheter HT17

Gesällprov Lasse Sjöblom

Introduktion

Detta gesällprov är en utökning av portscannern utförd för uppgift 4.2.3. Utökningen består av att denna version även utför TCP stealth scan samt ACK scan, dessa utförs via python biblioteket scapy. Ytterligare så finns det även en UDP scanner baserat med användning av samma bibliotek. För att kunna importera och exportera denna data så finns det stöd för I/O-operationer i form av XML, MySQL samt AES krypterad XML. På grund av scapys implementation så krävs sudo rättigheter för att köra programmet ska kunna utföra UDP scanningen och de ny implementerade TCP scanning teknikerna.

Systemarkitektur

Programmet är strukturerat med MVC i åtanke. Modellen är implementerad som en restful API med hjälp av Pythons flask ramverk. Detta möjliggör att lätt kunna omvandla systemet till en ren server men kan ändå användas för en skrivbordsapplikation. Som vy används Electron ramverket, vilket ger möjlighet till att använda diverse webbverktyg så som bootstrap, css, javascript med mera för att designa applikationen. En tydlig nackdel är electrons minnes konsumtion.

Dependencies

Då detta program har flera olika delar i olika språk så medföljer en rad olika beroenden. För modellen så behövs dels python men även scapy, för att kunna utföra de utökade port scannings metoderna. För att använda XML I/O så behövs lxml biblioteket medans för MySQL anslutningarna så används pymysql. För krypteringen så används PyCrypto.

För vyn så behövs nodejs som underliggande motor för vyn. Electron som huvudsakliga ramverk för att hantera användare interaktionen. Delar av gränssnittet använder sig av bootstrap samt w3 css. För att sköta kommunikationen inom systemet så används jquery, request och request-promise.

Programmet

Programmet i startläge. Tabellen göms undersökning och en spinner ritas upp.

XML Encryption Keys	MySQL
Address localhost	Start Port 50
55	● TCP ○ UDP Start Remove
TCP RESULTS U	DP RESULTS
Search for address	
IP	PORT

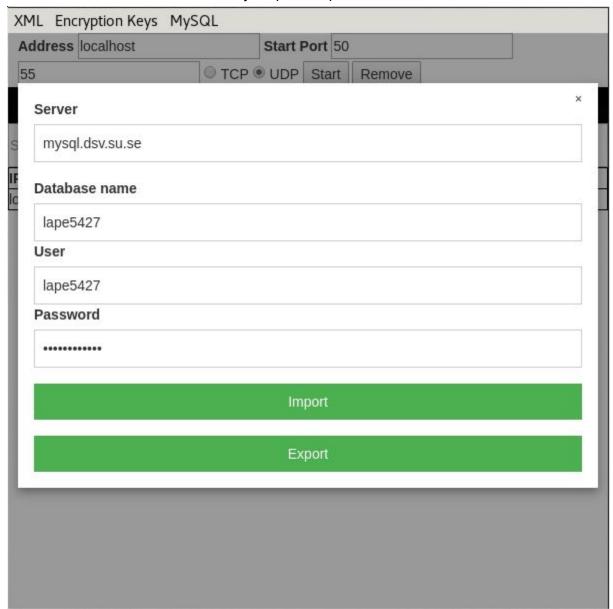
Efter en sökning gjorts populeras tabellen med de funna portarna.

XML Encryption Keys MySQL	
Address localhost Start Port 1	
65535 • TCP UDP Start	Remove
TCP RESULTS UDP RESULTS	
Search for address	
IP	PORT
localhost	42934
localhost	53820
localhost	5000
localhost	6463

Flikmenyn används för att bläddra mellan TCP och UDP resultaten.

XML Encryption R		7		
Address localhos	t gg	Start Port 5	50	
55	○ TCP	UDP Starr	Remove	
TCP RESULTS	UDP RESULTS			
Search for address.				
IP			PORT	

När användaren trycker på MySQL knappen så presenteras de av denna modal för att ange databas informationen och sedan välja import / export.



Om användaren laddar en krypteringsnyckel via "Encryption Keys' menyn syns en indikator med filnamnet som nedan.

XML Encryption	Keys MySQL				
Address localhos	t	Start F	ort 50		
55	© TCP €	UDP	Start	Remove	
TCP RESULTS	UDP RESULTS				
LOADED ENCRYP	TION KEY: aKey				
Search for address					
IP				PORT	
localhost				53	

Genom att markera en rad i en tabell så kan användaren välja att ta bort den ur registret via remove knappen.

Address localhost		Start Port 50	
55	○ TCP ●	UDP Start Remove	
TCP RESULTS	UDP RESULTS		
LOADED ENCRYPT	ION KEY: aKey		
Search for address.			
	•		
IP		PORT	
176.10.152.20		53	
176.10.152.20		548	
176.10.152.20		3333	
176.10.152.20		5555	
176.13.152.20		53	
470 40 450 00		608	
176.13.152.20		3333	
176.13.152.20 176.13.152.20			