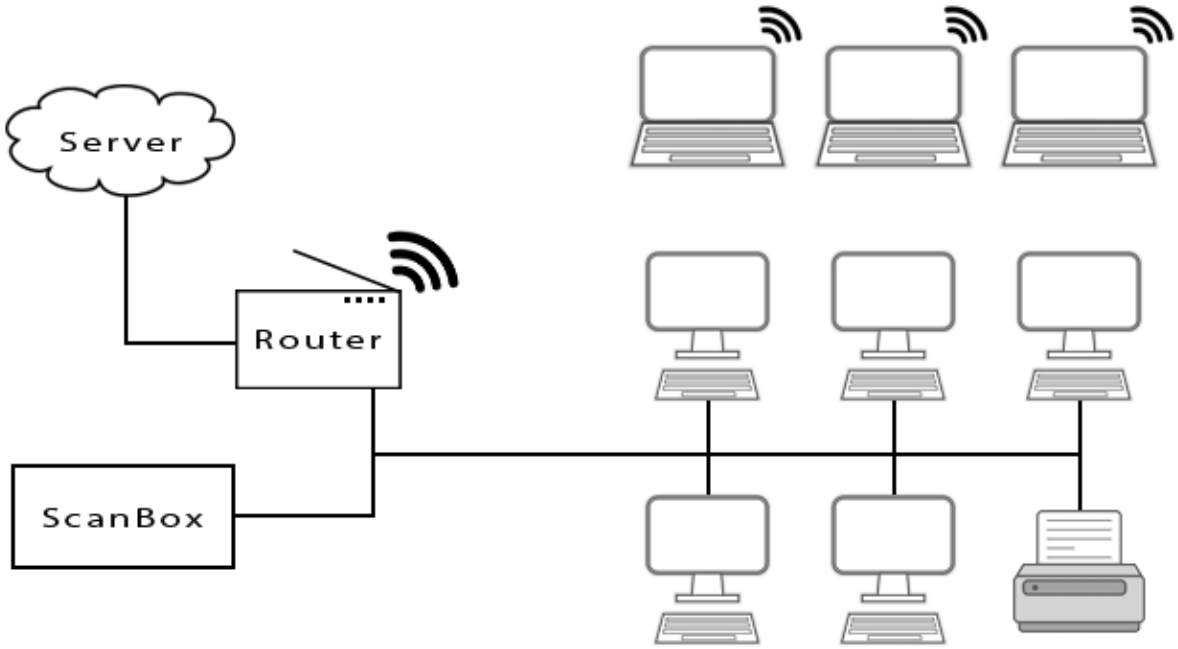
CHALMERS



ScanBox

Ett verktyg för snabb och automatisk nätverksscanning

Examensarbete i Data- och Informationsteknik

THERESE TENGDAHL
LINA THORÉN

Institutionen för Data- och Informationsteknik
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2017

EXAMENSARBETE

ScanBox

Ett verktyg för snabb och automatisk nätverksscanning

THERESE TENGDAHL
LINA THORÉN

Institutionen för Data- och Informationsteknik
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET

Göteborg, Sverige 2017

ScanBox
Ett verktyg för snabb och automatisk nätverksscanning
THERESE TENGDAHL
LINA THORÉN

Examinator: Peter Lundin

Institutionen för Data- och Informationsteknik
Chalmers tekniska högskola / Göteborgs universitet
SE-412 96 Göteborg
Sverige
Telefon: +46 (0)31-772 1000

Omslag:
En simplifierad bild utav systemet. ScanBox ansluts till ett lokalt nätverk och tar kontakt med en molnserver.

Institutionen för Data- och Informationsteknik
Göteborg, Sverige 2017

ScanBox

Ett verktyg för snabb och automatisk nätverksscanning

THERESE TENGDAHL
LINA THORÉN
Institutionen för Data- och Informationsteknik, Chalmers tekniska högskola

Examensarbete

Sammanfattning

IT-attacker utgör ett allt större problem. Trots detta är säkerhetsmedveten hos många företag på en oroväckande nivå. Möjliga orsaker kan vara brist på kunskap, att det verkar för dyrt att förbättra läget, eller kanske att det tar emot att påbörja arbetet. Bristande nätverkssäkerhet medför dock en utsatthet för angrepp. ScanBox har utvecklats som ett examensarbete hos Cybercom i Göteborg och är ett verktyg för automatisk sårbarhetsscanning av lokala nätverk. ScanBox utgörs av en Raspberry Pi med Kali Linux som styrs via en molnbaserad server och laddar upp sina resultat till denna. De resultat som produceras av ScanBox är avsedda som underlag för initiella säkerhetsdiskussioner med potentiella kunder. Genom sin grad av automation har ScanBox möjlighet att leverera resultat till ett mycket lågt pris, vilket kan underlätta för kunder att inleda en process kring säkerhetsarbete. ScanBox använder arp-scan för att snabbt kartlägga vilka enheter som är anslutna till ett lokalt nätverk. Därefter används Nmap för portscanning och initial sårbarhetsscanning. Hela förloppet tar ungefär en halvtimme. ScanBox har potential att öka kunders insikt kring nätverkssäkerhet och att visa på hur de med relativt små medel kan förbättra sitt säkerhetsläge. Projektet har inte involverat de legala frågeställningarna kring sårbarhetsscanning.

Nyckelord: Sårbarhetsscanning, nätverk, portscanning, säkerhet, arp-scan, Nmap, Raspberry Pi, Kali Linux

Abstract

While IT attacks are an ever growing problem, the security awareness of many companies is at an alarming level. Possible causes may be lack of knowledge, that it seems too expensive to improve the situation, or maybe that it is hard to get started. Lack of network security, however, leaves the network very vulnerable to attack. ScanBox was developed as a degree project at Cybercom in Gothenburg. It is a tool for automatic vulnerability scanning of local networks. ScanBox consists of a Raspberry Pi with Kali Linux, which is controlled via a cloud-based server and uploads its results to this server. The results produced by ScanBox are intended as a basis for initial security discussions with potential customers. Through its degree of automation, ScanBox has the ability to deliver results at a very low price, which can facilitate the initiation of a security process for the customer. ScanBox uses arp-scan to quickly map devices connected to a local area network. Next, Nmap is used for port scanning and initial vulnerability scanning. The whole process takes about half an hour. ScanBox has the potential to increase the customers' insight into network security and to show how they can improve their security status with relatively small funds. The project has not involved the legal issues of vulnerability scanning.

Keywords: Vulnerability scanning, network, port scanning, security, arp-scan, Nmap, Raspberry Pi, Kali Linux

Förord

ScanBox är ett examensarbete på kandidatnivå som gjorts vid institutionen för Data- och informationsteknik på Chalmers tekniska högskola i Göteborg av två studenter på högskoleingenjörsprogrammet i datateknik. Omfattningen av examensarbetet motsvarar en halv termins heltidsstudier. Examensarbetet skedde i samarbete med Cybercom Group i Göteborg.

Vi vill framföra ett stort tack till våra handledare Gunnar Ozolins och Johannes Weschke, från Cybercoms säkerhetsteam i Göteborg. Vi vill även tacka Gabriel Ibanez, ledare för Cybercom Innovation Zone i Göteborg. Sist men inte minst, ett stort och varmt tack till Sakib Sistek, vår handledare på Chalmers.

Innehåll

Beteckningar

DHCP - Dynamic Host Configuration Protocol, ett protokoll för automatisk tilldelning av IP-adresser till nya enheter från en DHCP-server.

LTS - Long Term Support, version som garanteras uppdateringar under längre tid.

MVP - Minimum Viable Product, minsta möjliga produkt. En tidig version med precis tillräcklig funktionalitet för att vara säljbar och ge underlag till fortsatt utveckling.

RPi - Raspberry Pi, en billig enkortsdator särskilt avsedd för utbildning.

SCP - Secure Copy Protocol, ett UNIX-program för filöverföring som inbegriper avlägsna enheter.

SSH - Secure Shell, ett nätverksprotokoll för krypterad kommunikation. Typiskt använt för terminalinloggning över nätverk.

WPA-PSK - WiFi-protected access (WPA) är ett säkerhetsprotokoll för trådlösa nätverk, varav version 2 är den som är aktuell idag. Pre-shared key (PSK) är en autentiseringsform som inte kräver en autentiseringsserver.

1 Inledning

I detta kapitel beskrivs bakgrunden till projektet. Därefter följer en beskrivning av dess syfte, samt en mer detaljerad redogörelse för vad som skall uppnås. Slutligen fastställs projektets avgränsningar.

1.1 Bakgrund

Datarelaterade brott ökar kraftigt i Sverige samtidigt som många företag inte är redo att hantera säkerhetsproblematiken kring IT. Henrik Davidsson, försäljningschef på NTT Security, beskriver i en intervju i Dagens industri [1] svenska företags IT-säkerhet med följande ordalag:

> *"Generellt kan man säga att mognadsgraden när det kommer till it-säkerhet är ganska låg. Tanken att det inte händer mig är en stor del av problemet"*

Enligt en medlemsundersökning av försäkringsbolaget If [2] anser hälften av svenska småföretagare att de inte har tillräckligt med kunskap för att skydda företaget. Vidare har var femte småföretagare blivit utsatt för dataintrång, samtidigt som mörkertalet tros vara stort.

Cybercom Group är ett internationellt IT-konsultföretag. Hos Cybercom i Göteborg finns ett säkerhetsteam som bland annat jobbar med penetrationstestning och hjälper företag att ta med ett säkerhetstänk redan i planeringsfasen av projekt.

Tidigare under året har ett opublicerat projektarbete utförts på Cybercom i Göteborg som syftat till att konstruera ett penetrationstestningsverktyg av en Raspberry Pi (RPi). Detta verktyg hade stort fokus på att inte bli upptäckt. Hårdvara samt vissa idéer från detta projektarbete har återanvänts i nuvarande projekt, dock bör tydliggöras att nuvarande projekt är att ses som fristående.

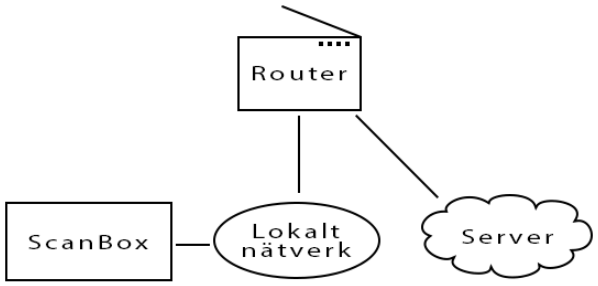
1.2 Syfte

Projektet syftar till framtagandet av ett verktyg för snabb och automatisk kartläggning samt sårbarhetsscanning av lokala nätverk. Ur ett affärsperspekiv är verktyget tänkt att nischas mot mindre företag. Verktyget skall enkelt kunna anslutas till företagets Ethernetnätverk och då automatiskt utföra en scanning. Resultatet från scanningen skall kunna användas som underlag för en första diskussion kring säkerhet med företaget. Genom att vara snabbt och automatiskt producerar verktyget då sitt resultat på ett relativt billigt sätt, eftersom ingen direkt arbetskostnad tillkommer. Detta möjliggör för Cybercom att erbjuda denna första, enkla säkerhetsutvärdering till låg kostnad eller möjligen gratis, vilket kan vara ett sätt att motivera potentiella kunder att ta tag i säkerhetsfrågan. Att utveckla verktyget snarare än att köpa in det är fördelaktigt för Cybercom så till vida att det ger god insyn i vad som ingår i verktyget; att det är enkelt att skapa fler enheter och skala upp lösningen; samt att det går att anpassa verktyget till olika situationer eller vidareutveckla det för andra användningsområden.

1.3 Mål

Projektet syftar till att ta fram ett verktyg, ScanBox, som ansluts till ett lokalt nätverk, såsom visas i figur 1.1. ScanBox skall därefter automatiskt upptäcka anslutna enheter och genomföra portscanning av dessa. Vidare skall ScanBox skapa en anslutning till en extern server och ladda upp insamlad data dit. Det skall också vara möjligt att ansluta till ScanBox från denna server.

ScanBox skall inte introducera säkerhetshål till det nätverk som scannas. Systemet skall inte orsaka att känslig data blir åtkomlig för obehöriga. ScanBox skall inte störa funktionen hos det nätverk som scannas. ScanBox bör producera resultat på ungefär en halvtimme, även för relativt stora nätverk. Resultatet skall vara någorlunda lättläst och lämpligt som underlag för en diskussion kring säkerhet. Produkten och processen för dess framtagande skall vara väl dokumenterade.



Figur 1.1: ScanBox är avsedd att kopplas in till ett Ethernetnätverk, samla in data om de enheter som tillhör samma subnät, och ladda upp sina resultat till en molnserver.

1.4 Avgränsningar

Avgränsningar för projektet:

- En Raspberry Pi 3b med 16 GB minneskort kommer att användas.
- Ingen hårdvara kommer att konstrueras.
- Inga donglar för bättre WiFi eller 4G-anslutning kommer att användas.
- Enbart scanning av lokala subnät, ej försök att ta sig in på angränsande subnät, och ingen scanning av publika nätverk.
- Inga försök att ta reda på något utan tillåtelse, såsom att avlyssna trafik ej avsedd för ScanBox eller att hacka sig in på trådlösa nätverk.
- Inga försök till exploatering av funna sårbarheter.
- Ingen social engineering, det vill säga att försöka manipulera människor till att avslöja känslig information.
- Inga försök att detektera malware eller andra enheter som utför scanning eller avlyssning.
- Inget utforskande av möjligheter att introducera ScanBox till ett nätverk i smyg.
- Ingen sökning efter potentiella kunder.
- Ingen inblandning i utformning av de avtal som krävs för att genomföra scanningar hos kund.

2 Teknisk bakgrund

Här följer en kortfattad genomgång av hårdvara och verktyg som använts i projektet. Även vissa protokoll och funktioner kommer att beskrivas.

2.1 Hårdvara och operativsystem

Nedan följer en beskrivning utav hårdvaran samt operativsystemet som användes för att skapa ScanBox. Enbart färdig hårdvara och operativsystem med öppen källkod har valts.

2.1.1 Raspberry Pi 3b

Raspberry Pi Foundation [3] presenterar RPi som en liten kapabel dator som kan göra det mesta en skrivbordsdator kan göra. Den kommer i ett flertal olika modeller, med Raspberry Pi 3b som den senaste versionen. Raspberry Pi 3b beskrivs på försäljningssidan [4] som en enkortsdator vars specifikation inkluderar en fyrkärnig 1,2 GHz 64-bitars ARM-processor och 1 GB 900 MHz RAM. Den har ett trådlöst nätverksgränssnitt och använder ett MicroSD-kort som sitt enda icke-flyktiga lagringsmedium.

2.1.2 Microsoft Azure och virtuella maskiner

Microsoft Azure [5] är en molnplattform som erbjuder software-as-a-service (SaaS), platform-as-a-service (PaaS) och infrastructure-as-a-service (IaaS). Virtuella maskiner kan skapas efter behov och ger användaren full kontroll över maskininstanserna. Virtuella maskiner hos Azure är flexibla och finns med ett flertal olika operativsystem, bland dessa ingår bland annat Ubuntu Server.

2.1.3 Kali Linux

Kali Linux är en Debian-baserad Linuxdistribution med öppen källkod specifikt designad för penetrationstestning och säkerhetsgranskning. Kali Linux är utvecklat för att vara säker och har därför enbart en minimal grupp utvecklare med möjlighet att modifiera koden, vilket görs med flera säkerhetsprotokoll. Standardversionen av Kali Linux har över 600 verktyg för testning av säkerhet [6]. Mängden verktyg är dock begränsad till en minimal mängd för den version som är designad för ARM-processorer (såsom RPi), vilket beror på att sådana system generellt har en begränsad lagringskapacitet och därmed inte har plats för en full installation. Så länge det finns utrymme finns inget hinder för att installera fler verktyg efter önskemål och behov [7]. Det är mycket viktigt att säkerställa att det är en officiell version av Kali Linux som installeras: dels för att det är viktigt för en professionell penetrationstestare att vara säker på sina verktyg, men också för att en förfalskad version av Kali skulle kunna orsaka stor skada [8].

2.1.4 Skivavbilder

En skivavbild är en datorfil innehållande både struktur och innehåll från ett lagringsmedium. I Linuxmiljö görs skivavbilder med programmet dd, som kan kopiera rådata. Eftersom hela lagringsmediet kopieras exakt går det att använda denna metod för att skriva en färdig skivavbild med operativsystem, filsystem och startsektor till ett SD-minne [9].

2.1.5 Schemalagd programkörning

Systemd är en system- och servicehanterare för Linux som kan användas för att få ett specifikt script att exekveras vid uppstart [10].

Crontab är en tidsbaserad schemaläggare för Linux. Crontab kan konfigureras till att utföra specifika kommandon exempelvis varje minut eller den första fredagen i oktober [11].

2.2 Nätverkskommunikation

Ett vanligt sätt att angripa komplexiteten kring nätverkskommunikation är att se nätverksprotokoll som tillhörandes olika lager. Enligt ISOs (International Organisation for Standardization) OSI-modell (Open Systems Interconnection model) är uppdelningen som följer:

- 7. Applikationslagret
- 6. Presentationslagret
- 5. Sessionslagret
- 4. Transportlagret
- 3. Nätverkslagret
- 2. Länklagret
- 1. Det fysiska lagret

En av tankarna med lagerprincipen är att varje lager skall erbjuda specifika tjänster och fungera oberoende av övriga lager. Exempelvis kan olika länklagerprotokoll, såsom Ethernet och Wireless LAN (WiFi), kombineras med Internet Protocol (IP) på nätverkslagret [12].

2.2.1 Nätverksprotokoll, lager 3

IP-adresser används för att avgöra vilka nätverksgränssnitt som är paketets avsändare respektive mottagare. Tre adressintervall är reserverade för privata nätverk, och kan aldrig routas utanför dessa [13]:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

I princip är IP-adresser, liksom portnummer, desamma under hela den väg ett paket kan ta genom olika IP-nätverk, men i praktiken används ofta Network Address Translation (NAT) för att översätta adresser och portnummer. Det mest välkända fallet är att ett hem- eller företagsnätverk använder privata IP-adresser och översätter dessa till en eller ett fåtal publika adresser då trafiken routas ut ifrån det lokala nätverket [12].

2.2.2 Länklagerprotokoll, lager 2

Emedan IP är ett mycket viktigt protokoll då paket skickas mellan routrar, är länklagerprotokollen väsentliga att ha i åtanke när trafik inom ett lokalt nätverk diskuteras. Både Ethernet och WiFi använder sig av Media Access Control-adresser (MAC) för att identifiera olika nätverksgränssnitt. Enheter kan inte kommunicera på ett Ethernetnätverk utan att känna till varandras MAC-adresser [12].

Address Resolution Protocol (ARP) har till uppgift just att översätta emellan IP- och MAC-adresser. När dator A vill skicka ett paket till dator B undersöker dator A om den har sparat en MAC-adress som korresponderar till dator Bs IP-adress i sin ARP-tabell. Är inte så fallet skickar dator A en ARP-förfrågan, vilket är en lokal broadcast. Dator B noterar att det är dess IP-adress som angivits och skickar ett ARP-svar, där dess MAC-adress ingår. Dator A lägger adressen på minnet och kan nu adressera dator B [12].

2.2.3 Transportprotokoll, lager 4

Transportlagrets två stora protokoll är TCP (Transfer Control Protocol) och UDP (User Datagram Protocol). TCP erbjuder en tillförlitlig, anslutningsbaserad tjänst, medan UDP erbjuder en simplare, anslutningslös tjänst. TCP använder en trevägs handskakning (SYN, SYN-ACK, ACK) för att upprätta en anslutning och har system för att numrera paket, bekräfta när de kommit fram, och skicka dem igen om bekräftelse uteblir [12].

Både TCP och UDP använder sig av portnummer för att avgöra vilken applikation som är paketets avsändare och vilken som är dess mottagare. Portnummer beskrivs med 16 bitar och är indelade i tre intervall:

- 0-1023 systemportar/välkända portar
- 1024-49151 användarportar/registrerade portar
- 49152-65535 dynamiska portar/privata portar/kortlivade portar

Av dessa tilldelas välkända och registrerade portar av Internet Assigned Numbers Authority (IANA), medan de dynamiska portarna aldrig tilldelas [14].

2.2.4 Portscanning och fingerprinting

För att kunna identifiera sårbarheter hos ett system behöver vägar in identifieras. Detta görs bland annat genom att scanna portar för att se vilka som är öppna och genom att operativsystemet för enheten identifieras.

Portscanning

Det finns enligt Nmap-sidan för portscanning [15] flera olika tekniker för portscanning, men den vanligaste är TCP SYN-scan. Detta är en snabb scan som är relativt diskret då den inte fullföljer TCP-anslutningar, vilket också gör att den kallas halvöppen scanning. Nmap skickar SYN-packet, vilket öppna portar besvarar med SYN-ACK. När en port är stängd svarar operativsystemet med RST.

Fingerprinting

I boken *Nmap Network Scanning* [16] förklaras det att när ett nätverk utforskas kan det vara användbart att veta vilket operativsystem, inklusive vilken version, en enhet använder sig utav. Detta för att kunna hitta sårbarheter och brister specifika för just den enheten och då kunna utnyttja dessa. Då detta är användbar information för angripare försöker många system att inte avslöja exakt vilket operativsystem som används.

Några anledningar till att det är önskvärt att fingerprinta operativsystem är:

- För att upptäcka sårbarheter hos enheter. Att veta vilket operativsystem som används kan hjälpa till att identifiera vilka sårbarheter som faktiskt finns hos en applikation, då dessa ibland är beroende utav version av operativsystemet.
- För att skräddarsy exploateringar. Även efter att en sårbarhet har hittats är kännedom om operativsystemet användbar för att veta hur sårbarheten kan exploateras.
- För att upptäcka obehöriga och farliga enheter. Exempelvis kan anställda på ett företag använda sig utav företagsnätverket på ett sätt som introducerar sårbarheter, såsom att installera en trådlös accesspunkt.

2.2.5 SSH och SCP

Secure Shell Protocol (SSH) är ett mjukvarupaket för säker systemadministration och filöverföring över osäkra nätverk. Det används i mycket stor utsträckning, och ersätter äldre protokoll såsom telnet, ftp och rlogin [17]. SSH File Transfer Protocol (SFTP) är ett säkert filöverföringsprotokoll som använder SSH. SCP är ett filöverföringsprogram för SFTP i Linux [18]. SSH tunneling, även kallat SSH port-forwarding, är en kraftfull teknik som har många användningsområden: det är ett billigt sätt att tillhandahålla krypterad kommunikation för gamla applikationer, det är ett sätt att ta sig igenom brandväggar, och det är också ett sätt för malware att öppna bakdörrar till interna nätverk från internet. Lokal portmappning används för att koppla en lokal port till en port på en SSH-server. Remote portmappning används för att koppla en port på en SSH-server till en lokal port. Det senare är svårt att förhindra då företag ofta har anledning att tillåta utgående SSH-anslutningar och trafiken är hårt krypterad [19, 20].

2.3 Säkerhet och sårbarhetsscanningsverktyg

Penetrationstestning är ett bra sätt att testa säkerheten hos ett system, och beskrivs i boken *Kali Linux: assuring security by penetration testing* [21] som en process där säkerheten för ett system grundligt testas och granskas. Detta genom att riktiga attacker simuleras för att se vilka sårbarheter som finns och vad som skulle kunna läcka vid en eventuell attack. Ett annat alternativ är sårbarhetsgranskning där testet slutar när sårbarheterna hittats och identifierats, utan att försök till exploatering utav sårbarheter sker.

Genom att ta reda på om en viss port är öppen och vad för tjänst som används bakom porten är det sedan möjligt att kolla upp om det finns några sårbarheter hos just den versionen. Sådana sårbarheter finns tillgängliga i olika databaser, exempelvis *SecurityFocus* [22] eller *Exploit Database* [23], där de samlas för att underlätta för penetrationstestare och övriga säkerhetsintresserade.

2.3.1 Arp-scan

Arp-scan, som beskrivs utförligt av *Arp-scan User Guide* [24], är ett verktyg som används för att upptäcka enheter på ett subnät, även de som blockerar IP-trafik, samt för enklare fingerprinting. Detta gör det för både Ethernet- och WiFi-nätverk. Arp-scan skapar och skickar ut ARP-förfrågningar till givna IP-adresser. Detta gör att arp-scan behöver root-privilegier, eftersom det krävs för att kunna läsa och skriva Ethernet-paket. Verktyget används via kommandotolken och visar där upp alla svar det får.

De enheter som svarar på arp-scans utskickade ARP-förfrågningar sparas med IP-adress, MAC-adress och tillverkare av nätvärkskort för varje enhet. ARP-förfrågningar skickas till alla IP-adresser på det aktuella nätverket, dock fungerar ARP bara på det lokala Ethernet-segmentet och kan därför inte användas för att upptäcka enheter bakom routrar.

Arp-scan använder som standard en bandbredd på 256000 bitar per sekund, men detta kan ställas in om snabbare resultat önskas. Det kan dock förekomma problem om bandbredden ökas för mycket. Det är möjligt att störa nätverket eller, om bandbredden är högre än vad nätverksgränssnittet klarar av, att fylla kärnans överföringsbuffer. Med en bandbredd på 256000 bitar per sekund är det möjligt att scanna 65536 enheter på strax över 2 minuter.

Arp-scan kan också användas för olika typer av fingerprinting, bland annat kan den automatiskt avkoda tillverkaren av nätverkskortet från MAC-adressen. Detta gör den genom att jämföra MAC-adressen mot tre olika listor på tillverkare, som den sparar lokalt.

2.3.2 Nmap

Verktyget Nmap förklaras utav utvecklarens resurssida *Nmap: the Network Mapper* [25] och kan användas för att upptäcka nätverk och för säkerhetsgranskning; det anses också användbart för uppgifter som nätverksinventering och övervakning av enheters och tjänsters drifttid. Nmap använder IP-paket för att upptäcka tillgängliga enheter, de tjänster som är aktiva på enheterna, deras operativsystem, och många fler egenskaper.

Nmap finns tillgängligt för alla större operativsystem, är exekverbart både i kommandotolken samt via ett inkluderat GUI, och fungerar bra både mot stora nätverk och enstaka enheter. Det kommer också med flera verktyg för att hantera och analysera resultaten, som exempelvis Ndiff (jämför skillnader mellan olika resultat) eller Nping (paketgenerering och responsanalys).

Nmap är flexibelt och stödjer flera tekniker för kartläggning av nätverk, det är kraftfullt nog för att kunna scanna flera hundratusen maskiner, och det är enkelt att börja använda trots en rik uppsättning av avancerade tjänster. Nmap är också gratis, då målet med programmet är att hjälpa Internet att bli säkrare, och det är väl dokumenterat.

2.3.3 Masscan

Enligt uppgift i repositoriet för Masscan [26] är masscan den snabbaste portscannern. Även om den är användbar på mindre, interna nätverk, så är den designad med hela Internet i åtanke. Med en hastighet på 10 miljoner paket per sekund, vilket kräver speciell hårdvara, kan den scanna hela Internet på under 6 minuter. Detta gör att den kan överbelasta det egna nätverket, men för att inte skada avlägsna nätverk slumpar masscan mål-IP i ett försök att sprida ut sin scanning.

Masscan producerar liknande resultat som Nmap och används även på liknande sätt. Detta eftersom Nmap är den mest kända portscannern och masscan då blir mer familjär för Nmap-användare. Två viktiga skillnader är dock att de portar som skall scannas måste specificeras explicit, och att masscan är mindre flexibel gällande syntaxen för angivandet av IP-adresser [26].

3 Metod

Projektets utförande kan beskrivas som en flexibel iterativ process med Scrum-influerad prioritering av uppgifter. Git har använts för versionshantering av kod. Arbetet har genomförts hos Cybercom Group i Göteborg som en del av arbetsgruppen i Innovation Zone. Dagliga ”stand up”-möten i gruppen var ett kontinuerligt inslag.

I ett initialt skede fokuserade arbetet på att specificera vad som skulle åstadkommas. Det tidigare arbetet som projektet baserades på analyserades och intresserade parter rådfrågades. Därefter definierades grundläggande funktionalitet för detta projekts verktyg. Samtidigt som projektets definitionsfas pågick inleddes även en informationsinhämtningsprocess, vilken i synnerhet fokuserade på ramverk för penetrationstestning, programvaror för nätverksscanning samt Bash-scripting.

Då det tidigare projektet gällde ett penetrationstestningsverktyg, som dessutom skulle vara svårupptäckt, bedömdes dess huvudsakliga egenskaper som irrelevanta för det nuvarande projektet. Därför fattades beslutet att enbart behålla generella idéer samt hårdvara från det föregående projektet, men att helt skriva om programkoden. Även operativsystemet på RPi installerades om. Beslutet kring serverns varande och natur togs upp till granskning. Experimenterande, implementering, viss testning, informationsinhämtning samt rapportskrivning fortskred därefter parallellt.

3.1 Minsta möjliga produkt (MVP)

ScanBox skall baseras på en RPi. ScanBox skall vid uppstart ta emot en dynamisk IP-adress via DHCP och därefter ha förmågan att automatiskt göra följande:

- Skapa en omvänd SSH-tunnel till en server.
- Detektera de IP-adresser som används på det Ethernetnätverk/subnät som ScanBox förmodas ha anslutits till, och skriva dessa IP-adresser till fil tillsammans med korresponderande MAC-adresser.
- För de enheter som befunnits vara aktiva, genomföra portscanning i syfte att ta reda på vilka portar som är öppna, och skriva resultatet till fil.
- Ladda upp resultatfilerna till servern genom krypterad kommunikation.
- Stänga av sig.

Till projektets grundläggande funktionalitet räknas även:

- Det skall gå att ställa in huruvida ScanBox skall genomföra en scanning vid uppstart och huruvida den skall stänga av sig efteråt.
- ScanBox skall skriva vad den gör till loggfiler.
- Servern skall ta emot och hantera data på ett sätt som förhindrar obehörig åtkomst.
- Auktoriserade användare skall ha möjlighet att logga in till ScanBox via servern.
- Resultatet skall presenteras i enkel men läsbar form.
- En scanning skall kunna genomföras på ungefär en halvtimme även på stora nätverk.

3.2 Ytterligare funktionalitet

ScanBoxen färdigställdes först i en MVP-version och byggdes därefter på iterativt. Ytterligare funktioner valdes utifrån lämplighet, användarpotential och intresse. Följande funktionalitet övervägdes, ej i rangordning:

- Sårbarhetsscanning, utöver portscanningen.
- Möjlighet till mer grundlig sårbarhetsscanning av specifika enheter.

- Möjlighet att välja mellan olika typer av scanning att genomföra.
- Scanning av trådlösa nätverk.
- Möjlighet att på ett smidigt sätt ange inställningarna för ScanBox till servern.
- Webbgränssnitt för interaktion med ScanBox. Kundspecifika användare som bara har tillgång till sina resultat. Hög säkerhet krävs.
- Möjlighet att ange inställningar med en app.
- Förberedelse av plattformen för användning av flera ScanBoxar, med varsitt användarkonto på servern och ingen tillgång till data som inte rör deras nuvarande kund.
- Bättre presentation av resultatet än i textfilsformat.
- Införande av resultat i databas.
- Visualisering av data.
- Ytterligare bearbetning av resultat i syfte att undersöka vad för information som går att få ut av dem.
- Definition av process för uppdatering av operativsystem och verktyg.

3.3 Testning

Då resultatet är ett verktyg som gör en lättare sårbarhetscanning har testning skett genom att ta med ScanBox till några olika nätverk av varierande storlek, ansluta den till Ethernet och eventuellt även WiFi. Därefter gjordes en lättare analys av resultaten för att kontrollera att allt gått som planerat. Dessa resultat skulle sedan kunna användas för en grundligare analys och då även som grund för diskussion om säkerhet med ansvarig för nätverket.

4 Genomförande

Systemets grundprincip är att ScanBox kopplas in till ett Ethernetnätverk och ett eluttag. Den startar när den får ström och utför sedan en rad uppgifter automatiskt: den tar kontakt med en server, kontrollerar om den ska använda några speciella inställningar, genomför en nätverksscanning, laddar upp resultatet till servern, och stänger sedan av sig. Det är möjligt att interagera med servern med en annan enhet, antingen för att ändra inställningar, hämta resultat, eller för att ansluta direkt till ScanBox.

4.1 Systemdesign

Sedan det tidigare projektet har den generella systemdesignen byggt på en mobil liten låda som själv skapar en anslutning till en server med publik IP-adress. Denna anslutning, kallad en omvänd SSH-tunnel, ger servern möjlighet att i sin tur ansluta till lådan. Detta även om lådan är bakom en brandvägg som inte är konfigurerad för att släppa in inkommande anslutningar, eftersom anslutningen skapats från insidan. Servern fungerar både som command & control-server och som lagringsplats för data. För det tidigare projektet, som var ett explicit penetrationstestningsverktyg, var denna design en nödvändighet, då tanken var att användaren ansluter enheten till målnätverket i smyg och därefter inte har någon garanterad tillgång till den.

Denna övergripande design har ifrågasatts, vilket dock inte lett till avvikelser ifrån den. Ett alternativ vore en låda som bara sparar data lokalt, då detta skulle ta bort behovet av en server. Möjliga vidareutvecklingar som automatiska schemalagda scanningar/remote åtkomst för scanning, samt verktyg för penetrationstestning, har motiverat en design med låda och server, medan användningsområden som automatisk scanning inte nödvändigtvis har gjort det. Vissa konsekvenser följer dock av att användningen av RPi som hårdvara inte ifrågasatts. En RPi saknar inbyggd skärm, tangentbord, mus; med andra ord, för att interagera med enheten behöver man antingen föra med sig en rad tillbehör, eller interagera via en annan enhet. Därmed blir lösningen med en server mer attraktiv: dels går det att ansluta via en fast IP-adress, och dels går det att ansluta oavsett var man själv respektive lådan befinner sig. Andra fördelar är också att det minskar mängden data som behöver lagras lokalt på ScanBox, vilket kan vara lämpligt ur ett säkerhetsperspektiv, samt att det möjliggör bearbetning av data på en mer kraftfull enhet. Vidare är en RPi känslig för plötsligt förlust av ström, varmed det är sannolikt att datan är i mer säkert förvar på en server. Slutligen, iaktta möjligheten att flera enheter kommunicerar med en gemensam central server, då torde detta arrangemang underlätta datahanteringen.

4.1.1 Raspberry Pi och Kali Linux

Till Raspberry Pi 3b har använts ett 16GB micro-SD-kort, som tjänstgör som enhetens enda hårddisk. Det var ett enkelt val att använda operativsystemet Kali Linux, som mycket ofta används för liknande syften. Kali Linux är specialdesignat för penetrationstestning, är väl underhållet med uppdateringar inklusive uppdateringar av relevanta verktyg, och är väl dokumenterat.

Beslutet fattades att genomföra hela processen med ominstallation av Kali Linux, trots tillgång till en gammal skivavbild från det tidigare projektet. Installationsprocessen inbegrep uppsökande av lämplig version av Kali Linux att ladda ned, närmare bestämt den som är specifikt avsedd för RPi; verifiering av filens äkthet; samt uppsökande av ett Windowsprogram kapabelt att skriva en skivavbild bit för bit till ett SD-kort, inklusive att finna en metod för att i Windows hantera ett SD-kort med en befintlig ext-partition. När operativsystemsavbilden väl var skriven till minneskortet återstod bara att sätta in det i RPi.

Det fanns en rad anledningar till att beslutet om ominstallation fattades. Dokumentationen sedan tidigare var bristande, med följden att det var oklart vilka inställningar och förändringar som gjorts. Det fanns en önskan om att dokumentera processen bättre. Slutligen tillgodosåg det önskemål om lärande, samt gav en upplevelse av ägande av projektet.

Efter att Kali Linux installerats utökades operativsystempartitionen för att möjliggöra utnyttjande av hela SD-kortet. Utöver detta skedde viss konfiguration av systemet. Nya SSH-nycklar genererades. Tidszon ställdes in. Systemet uppdaterades. Ett fåtal paket installerades, utöver vad som ingår i den slimmade ARM-versionen

av Kali Linux avsedd för RPi, såsom arp-scan. Inga ytterligare användare skapades, eftersom det är standard att använda root-kontot på Kali Linux, då många program avsedda för penetrationstestning kräver rootprivilegier.

4.1.2 Server

Valet av server utvärderades och i slutändan beslöts att skapa en virtuell maskin i Microsoft Azure-molnet. Ett annat alternativ hade varit att installera en server på en fysiskt tillgänglig maskin. Fördelar med en virtuell maskin är att processen är smidigare: ingen IT-avdelning behöver involveras för att tillhandahålla maskinen och konfigurera brandväggar och portvidarebefordran. En virtuell maskin på Microsoft Azure är en något mer kostsam lösning än en virtuell maskin på Linode, vilket var den lösning som användes av det tidigare projektet. Däremot framhölls att valet av Azure öppnar upp för att enkelt kunna dra nytta av de databearbetningsmöjligheter som erbjuds av plattformen, att erfarenhet av att interagera med Azure var önskvärt, samt att Cybercom gärna använder sig av Microsofts teknologier.

Efter beslutet att använda en virtuell maskin i Microsoft Azure-molnet återstod många mindre val. Den virtuella maskin som valdes var relativt minimalistisk, vilket var en kostnadsmässig fördel. Operativsystemet som utsågs var Ubuntu Server 16.04 LTS, då detta erbjöds som en färdig skivavbild speciellt avsedd för plattformen. Både Ubuntu och Kali härrör från Debian Linux, med följden att de olika versionerna är relativt lika varandra, vilket ansågs underlätta deras användning. Server-versionen av Ubuntu inbegriper inte något grafiskt gränssnitt per default, men detta ansågs vara en fördel då all interaktion med maskinen sker via SSH.

Ubuntu-servern konfigurerades så till vida att ett användarkonto utan sudo-privilegier skapades för ScanBox; i det fall att flera ScanBoxar används är tanken att de skall ha varsitt användarkonto. Den inkommande SSH-porten ändrades från standardvalet TCP-port 22 till TCP-port 443, med andra ord den som är standard för HTTPS. Detta är inte särskilt effektivt ur ett säkerhetsperspektiv, snarast bör det förväntas att alla publikt åtkomliga portar blir scannade. Fördelen är att det ökar ScanBoxens chanser att skapa sin SSH-tunnel till servern genom en brandvägg som inte är konfigurerad för att tillåta denna användning, därför att SSH-trafik till port 443 utan djup paketinspektion liknar HTTPS, med andra ord begäran av en krypterad webbsida. Serverns brandvägg fick konfigureras via Azure-portalen för att ackommodera portbytet. Tidszon ställdes in på servern, vilket underlättar tolkning av loggar.

Serverns huvudsakliga uppgift är att fungera som fast anslutningspunkt för ScanBox samt som lagringsutrymme för data från genomförda scanningar. Detta innebär att servern i stort sett är passiv, dock skapades ett script för att ange inställningar för ScanBox, vilka hämtas utav ScanBox vid uppstart (beskrivs närmare i kapitel 4.2.1).

4.2 Scripting

Då det tidigare projektet haft fokus på att RPi skulle uppträda diskret, för att minimera risken för upptäckt, beslutades det att inte återanvända någon kod. Som programmeringsspråk beslöts att använda Bash-scripting, då detta tillåter systemanrop på ett mycket smidigt sätt.

4.2.1 Översiktlig funktionalitet

ScanBox, genom Kali Linux, använder *systemd* för att köra ett script vid uppstart. I detta scripts uppgifter ingår att initiera den omvända SSH-tunneln till servern, samt att använda SCP för att kopiera inställningsfiler från servern. Angivet i dessa inställningsfiler är bland annat om det är önskvärt att ScanBox genomför en scanning vid uppstart, om det är Ethernet-nätverket eller ett WiFi-nätverk eller båda som skall scannas, samt om ScanBox skall stänga av sig när scanningen slutförts. Skall en scanning genomföras ansvarar scriptet ifråga för att initiera denna process.

Genom användning av *crontab* ser ScanBox med korta intervall till att undersöka om den omvända SSH-tunneln är aktiv, och, om så inte är fallet, skapa tunneln. Servern använder samma metod för att logga om tunneln är aktiv. Loggning ingår i det mesta ScanBox gör, såsom uppstart, startande av SSH-tunneln, olika scanningar, och uppladdning av resultat till servern.

4.2.2 Nätverksanslutning

Det är nödvändigt att verktyget ansluts till ett Ethernetnätverk, då det är programmerat att annars stänga av sig. Det hade varit möjligt att designa systemet på annat sätt, men beslutet motiverades med att denna lösning var enklare och mer tillförlitlig, samt att WiFi-anslutning inte ingick i MVP. Betänk att det handlar om en liten låda som inte förutsätts ha något direkt användargränssnitt, och som aldrig bör pluggas ur utan att först stängas av; detta hände en gång under projektet, med följden att minnet hamnade i ett felaktigt tillstånd. Anslutning till trådlösa nätverk kan fallera, bland annat därför att felaktiga uppgifter angivits. Kombinationen av RPis Ethernet- och WiFi-gränssnitt har också funnits ge inkonsistenta resultat. I synnerhet kan det hända att det inte går att ansluta tillbaka till RPi genom SSH-tunneln; i dessa fall brukar det dock gå att ansluta direkt via SSH, och det anses positivt att ha en sista väg att nå RPi ifall något går fel och den inte skulle stänga av sig. För att underlätta detta meddelar ScanBox servern sin lokala Ethernetadress vid uppstart.

Verktyget scannar aldrig andra subnät än de det är anslutet till. Det är alltid anslutet till ett trådad Ethernetnätverk, men hurudvida detta skall scannas är en inställning som anges till servern. Det är också möjligt att ansluta till och scanna WiFi-nätverk, genom att ange SSID och lösenord för ett WPA-PSK-nätverk till serverns konfigurationsscript. Är det angivit att ScanBox skall scanna både Ethernet och WiFi, och det visar sig att båda använder samma subnät, medför detta att enbart det trådade gränssnittets nätverk scannas. Beslutet att begränsa sig till denna typ av trådlösa nätverk grundade sig i att det är en bra funktion för att undersöka företags gästnätverk, som torde ha relativt lättåtkomliga inloggningsuppgifter, samt att det var mer tidseffektivt att enbart implementera denna typ av trådlös funktionalitet.

4.3 Scanning

Scanningsprocessen följer en viss sekvens av steg. I det fall att både ett trådat och ett trådlöst nätverk skall scannas upprepas proceduren två gånger. De verktyg som används är arp-scan och Nmap.

Arp-scan

Verktyget arp-scan används för att upptäcka enheter på nätverket, då alla nätverksgränssnitt med IP-adresser måste besvara ARP-förfrågningar. Specifikt valdes arp-scan för att det är mycket snabbt. Utöver att lista aktiva IP-adresser ger arp-scan information om MAC-adresser och vilka tillverkare av nätverkskort dessa korresponderar till.

```
arp-scan -I "\$interface" -l > output_file 2> error_output_file
```

Figur 4.1: Det arp-scan kommando som användes utav ScanBox.

I arp-scan-kommandot i figur 4.1 anges vilket nätverksgränssnitt som skall användas *(-I)*, samt vilket intervall av adresser som skall scannas; i det här fallet hela det lokala subnätet *(-l)*.

Nmap

Efter den initiella kartläggningen används verktyget Nmap för sårbarhetsscanning. ScanBox är programmerad att automatiskt välja mellan tre olika scanningnivåer, i syfte att ta hänsyn till antalet aktiva enheter och slutföra scanningen inom 30 minuter, trots låg trafikhastighet. Är antalet aktiva enheter på nätverket maximalt 25 scannas de 1000 vanligaste TCP-portarna, samt de 100 vanligaste UDP-portarna. Finns det mellan 26 och 40 aktiva enheter scannas enbart de 1000 vanligaste TCP-portarna. Skulle antalet aktiva enheter vara högre än 40 begränsas scanningen till de 100 vanligaste TCP-portarna. Det går också att ange önskad scanningnivå med serverns konfigurationsscript.

I sin mest noggranna scanningnivå scannar ScanBox både TCP- och UDP-portar, enligt de kommandon som visas i figur 4.2. Adresser att scanna anges i en fil som innehåller de IP-adresser som parsats från resultatet från arp-scan. Hastigheten begränsas till 100 paket per sekund. Den TCP-scanning som görs är en vanlig halvöppen SYN-scanning (*-sS*), vilket betyder att anslutningarna inte fullbordas. I kombination med denna

```
nmap -sS -O -sV -oA output_file_TCP --privileged --disable-arp-ping -Pn -n --max-rate 100
    --defeat-rst-ratelimit --max-os-tries 1 --max-retries 3 --host-timeout 2400
    --max-hostgroup 100 -iL input_file
nmap -F -sU -oA output_file_UDP --privileged --disable-arp-ping -Pn -n --max-rate 100
    --max-retries 3 --host-timeout 1800 --max-hostgroup 100 -iL input_file
```

Figur 4.2: De Nmap kommandon som ScanBox använde sig utav.

scanning görs fingerprinting av operativsystem (*-O*) samt de tjänster som påträffas bakom öppna portar (*-sV*). Defaultalternativet är att de 1000 vanligaste portarna scannas, medan en snabbare version (*-F*) bara scannar de 100 vanligaste portarna. Det senare är alltid fallet med ScanBoxens UDP-scanning (*-sU*).

Nmap erbjuder sina resultat i flera filtyper, däribland XML. XML-filerna konverteras med programmet xsltproc till HTML-filer, som är lämpliga att titta på med en webbläsare.

När scanningsprocessen är avslutad laddas samtliga resultat upp till servern med SCP. Detta sker separat från SSH-tunneln och har hittills alltid fungerat, även då SSH-tunneln gått ner. I det typiska fallet är ScanBox konfigurerad för att stänga av sig därefter.

4.4 Testning

ScanBoxens funktion har testats på ett företagsnätverk och fyra hemnätverk. Scanningarna har utformats för att testa de olika konfigurationerna utav ScanBox som finns tillgängliga. Detta innebär att både automatisk och påtvingad nivå för scanningen har kontrollerats. Även scanning utav enbart Ethernet, enbart WiFi samt båda två samtidigt har testats. Resultatens rimlighet har enbart lätt analyserats, inklusive en väldigt lätt analys av sårbarheter.

5 Resultat

Kali Linux har installerats på en RPi och en molnbaserad server har konfigurerats, så som beskrivits i genomförandet (kapitel 4.1.1 respektive kapitel 4.1.2). Både scanning av system och uppladdning utav resultaten till server sker automatiskt på de sätt som beskrivits i genomförandet om scanning (kapitel 4.3).

5.1 ScanBox som resultat

ScanBox lever upp till de krav som beskrivits som MVP och har viss funktionalitet utöver detta.

5.1.1 Uppnådd funktionalitet utöver MVP

- ScanBox utför förutom ren portscanning även enklare sårbarhetsscanning med fingerprinting av operativsystem samt versioner av de tjänster som påträffas bakom öppna portar.
- Portscanningen kan ske i tre olika nivåer, som skiljer sig åt i avseende på hur många portar som scannas samt om enbart TCP-portar eller även UDP-portar scannas.
- Scanningens nivå kan anpassas automatiskt efter antalet aktiva enheter som detekterats på subnätet.
- Inställningar för ScanBox kan anges till servern, som har ett script för inmatning av inställningar.
- ScanBox undersöker vid uppstart vilka inställningar som gjorts till servern och applicerar dessa.
- ScanBox har möjlighet att scanna WiFi-nätverk av formen WPA-PSK efter att SSID och nyckel tillhandahållits servern. Scanningen är av samma typ som för trådade Ethernetnätverk.
- Utöver scanning vid uppstart samt avstängning efter scanning har ScanBox inställningar även för scanningsnivå, automatisk eller forcerad scanningsnivå, scanning av Ethernet, samt scanning av WiFi.
- Resultatet från sårbarhetsscanningen presenteras bland annat i ett lättläst HTML-format.

5.1.2 Beskrivning av scanningsprocessen

När ScanBox kopplas in i ett Ethernet-uttag och ett strömuttag, varvid den startar, kontrollerar den först om den har en IP-adress. Får den ingen IP-adress via DHCP stänger den av sig efter ett litet tag. Annars skapar den en omvänd SSH-tunnel till servern. Misslyckas detta gör den ytterligare ett par försök, men stänger slutligen av sig om det inte fungerar. När SSH-tunneln skapats hämtar ScanBox inställningar från servern och konfigurerar sig automatiskt.

De inställningar som hämtades av ScanBox från servern vid uppstart kan ange att ingen scanning skall genomföras, att ScanBox inte skall stänga av sig efter genomförd scanning, samt att en viss nivå av scanning ska genomföras oavsett antal enheter. De kan också ange att bara Ethernet-nätverket skall scannas, att bara ett WiFi-nätverk skall scannas, eller att båda skall ske. Om inställningarna anger att ScanBox skall scanna ett WiFi-nätverk konfigureras RPis trådlösa gränssnitt och den startar om. Omstarten är ett sätt att undvika problem som ibland uppstått vid aktivering av det trådlösa gränssnittet. Efter omstarten fortsätter ScanBox direkt med scanningfasen.

I det fall att både Ethernet- och WiFi-nätverk skall scannas kontrolleras om de IP-adresser som tilldelats gränssnitten tillhör samma subnät, vilket sker genom att deras broadcastadresser jämförs. Tillhör adresserna samma subnät genomförs bara en scanning utgående från det trådade gränssnittet.

Det skapas en katalog för scanningen vars namn baseras på aktuell tid. Därefter påbörjas scanningen med programmet arp-scan. Arp-scan listar IP-adresser under användning, tillhörande MAC-adresser, samt vilka tillverkare av nätverkskort dessa korresponderar till. De IP-adresser som funnits vara aktiva skrivs till en ny fil, vilken används som input för Nmap. Är ScanBox konfigurerad för att automatiskt avgöra scanningsnivå bestäms denna nivå utifrån antalet aktiva IP-adresser. Därefter kör Nmap en TCP SYN-scanning med OS fingerprinting och version fingerprinting, på antingen 100 eller 1000 TCP-portar, valda utifrån vilka Nmap

rankar som vanligast. Därefter kör Nmap, enbart vid den högsta scanningsnivån av tre, även en UDP-scan på de 100 vanligaste UDP-portarna.

Nmap ger resultat i flera format, däribland XML. XML-filerna används för att skapa HTML-filer. Samtliga resultat laddas upp till servern. ScanBox stänger sedan av sig, om detta angivits i konfigurationen.

5.2 Resultat genererade av ScanBox

Nedan följer de resultat som sparas på servern efter varje genomförd scanning.

5.2.1 Arp-scan

Resultatet från arp-scan har det format som kan ses i figur 5.1. För varje enhet som svarat skrivs IP-adress, MAC-adress samt namn på tillverkaren av nätverkskortet. Det senare härleds ifrån listor över MAC-adressprefix som tilldelats olika tillverkare. MAC-adresserna är suddiga i figuren då de utgör känslig information. Ett exempel på ett större resultat kan ses i bilaga A.

```
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (
http://www.nta-monitor.com/tools/arp-scan/)
192.168.0.1 [illegible]    D-Link International
192.168.0.101 [illegible]    ASUSTek COMPUTER INC.
192.168.0.102 [illegible]    ASUSTek COMPUTER INC.
192.168.0.105 [illegible]    Sony Interactive Entertainment Inc.
192.168.0.104 [illegible]    Liteon Technology Corporation
192.168.0.108 [illegible]    Intel Corporate
192.168.0.106 [illegible]    Nintendo Co., Ltd.
192.168.0.107 [illegible]    (Unknown)

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 8225.039 seconds (0.03
hosts/sec). 8 responded
```

Figur 5.1: Den enhetslista som arp-scan producerar efter att ha scannat ett litet nätverk.

5.2.2 Nmap

Ett utdrag ur ett HTML-konverterat resultat av Nmaps TCP-scan kan ses i figur 5.2, där resultatet för en enhet visas. Ett komplett resultat finns i bilaga B. Överst visas IP-adress för enheten, samt MAC-adress och namn på tillverkaren av nätverkskortet. MAC-adressen är suddig då detta är känslig information. Nedanför detta visas de portar som funnits öppna i genomförd scan. Resultatet från genomfört försök till fingerprinting av operativsystem visas som sannolikheten för att vissa operativsystem används av enheten.

Även resultatet från Nmaps UDP-scan sparas som HTML. Ett utdrag finns att se i figur 5.3 där resultatet följer samma struktur som i figur 5.2, med skillnaden att protokollet UDP använts istället för TCP. Även här går det att hitta ett komplett resultat i bilaga B.

192.168.1.12

Address

- 192.168.1.12 (ipv4)
- [redacted] - Sharp (mac)

Ports

The 991 ports scanned but not shown below are in state: **closed**

- 991 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	SHARP MX-2640N printer ftpd	01.06.00.0c.54	
23	tcp	open	telnet	syn-ack	Sharp MX-2640N printer telnetd	01.06.00.0c.54	
80	tcp	open	http	syn-ack	RapidLogic httpd	1.1	Sharp MX-2700N printer
443	tcp	open	https	syn-ack			
515	tcp	open	printer	syn-ack			
631	tcp	open	ipp	syn-ack			
5900	tcp	open	tcpwrapped	syn-ack			
9100	tcp	open	jetdirect	syn-ack			
50001	tcp	open	bandwidth-test	syn-ack	MikroTik bandwidth-test server		

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- OS match: **Sharp AR-C260M or AR-M351N printer** (**88%**)
- OS match: **Kyocera FS-3800 network printer** (**88%**)
- OS match: **Canon imageRUNNER 2020 or Kyocera FS-4000DN printer** (**85%**)

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=136 (Good luck!)
IP ID Sequence Generation	Incremental

Figur 5.2: Del utav det resultat som Nmap producerar efter genomförd TCP-scan.

192.168.1.100

Address

- 192.168.1.100 (ipv4)

Ports

The 93 ports scanned but not shown below are in state: **closed**

- 93 ports replied with: **port-unreaches**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
68	udp	open|filtered	dhcpc	no-response			
111	udp	open	rpcbind	udp-response			
137	udp	open	netbios-ns	udp-response			
138	udp	open|filtered	netbios-dgm	no-response			
1900	udp	open|filtered	upnp	no-response			
2049	udp	open	nfs	udp-response			
5353	udp	open|filtered	zeroconf	no-response			

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set

Figur 5.3: Del utav det resultat som Nmap producerar efter genomförd UDP-scan.

6 Analys

6.1 ScanBox

Projektets mål bedöms ha uppnåtts, dock med ett frågetecken gällande säkerheten kring data lagrad på servern då denna inte är krypterad. Även ett antal funktioner utöver MVP har implementerats.

6.1.1 Grundläggande

Vår bedömning är att ScanBox inte introducerar säkerhetshål till det nätverk som scannas. Visserligen öppnas en kommunikationsväg utåt genom den omvända SSH-tunneln, men då 4096-bitars RSA-nycklar används för att logga in till servern anses detta tillräckligt säkert.

ScanBox scannar mycket långsammare än vad den hade kunnat göra, närmare bestämt omkring 100 paket per sekund. Det används inte heller testmetoder som är kända för att kunna orsaka problem hos dåligt konfigurerade enheter. Därmed är det mycket osannolikt att ScanBox orsakar problem eller stör funktionen hos det nätverk som scannas.

Produkten och processen för dess framtagande är tillräckligt väl dokumenterade, dock ingår inte processens dokumentation i denna rapport.

Det är ett möjligt säkerhetsproblem att RPis SD-minne inte är krypterat, vilket möjliggör avläsning vid fysisk tillgång. Problemet bedöms som relativt litet då ScanBoxen är avsedd att användas kortvarigt och sedan tas om hand, det kan också vara svårt att åtgärda på en RPi. Inte heller är data krypterad på servern, vilket är en brist, men data är dock krypterad i kommunikationen medservern.

ScanBox bedöms logga vad som händer i tillräcklig grad.

6.1.2 Ytterligare funktionalitet

ScanBox utför viss sårbarhetsscanning, utöver den portscanning som ingick i MVP, där det bland annat sker fingerprinting av operativsystem på scannade enheter. Det går att ställa in denna scanning på tre olika nivåer, och detta kan också ske automatiskt. Dock är inte mer avancerad sårbarhetsscanning riktad mot utvalda enheter implementerat.

Scanning av trådlösa nätverk är implementerat i viss mån, begränsat till WPA-PSK-nätverk där SSID och nyckel i förhand angivits. Detta bedömdes som den huvudsakliga användningen av funktionen.

Det fungerar väl att ge inställningar till servern, istället för att behöva ansluta till ScanBox. De inställningar som upplevts som behövliga finns tillgängliga.

Mer avancerade gränssnitt till systemet, såsom webbgränssnitt för servern och möjlig app har inte implementerats.

Resultaten införs inte i en databas, visualiseras ej och bearbetas ej vidare. Däremot presenteras de på ett någorlunda användarvänligt sätt.

Plattformen är inte förberedd för flera ScanBoxar i tillfredsställande mån. Närmare bestämt behöver isolering av enheterna och deras data undersökas.

En process för uppdatering av operativsystem och verktyg har definierats.

6.2 Resultat genererade av ScanBox

Både arp-scan och Nmap ger tydliga och användbara resultat, vilka analyseras nedan.

6.2.1 Arp-scan

Resultaten i figur 5.1 ger en smidig överblick utav subnätet som ScanBox anslutits till, med tillräcklig information för att kunna identifiera de flesta enheter. Detta kan vara användbart till exempel då gästnätverk scannas och det inte är lika lätt att ha kontroll över vilka enheter som är anslutna.

Efter listan med anslutna enheter kommer ett oväntat resultat. Där påstår arp-scan att det tog 8225 sekunder att scanna nätverket, vilket är helt orimligt. Detta dels för att hela scanningens förlopp tog mindre än en halvtimme, men också för att andra scanningar utav nätverk med liknande storlek har tagit omkring fyra sekunder att genomföra. Det enda som påverkats är den tid arp-scan påstår att scanningen tog, men inte själva resultatet eller faktisk förfluten tid.

6.2.2 Nmap

Resultatet från Nmap ger mer information om varje enhet, såsom kan ses i figur 5.2. Nmap skriver ut MAC-adress och namn på tillverkaren utav nätverkskortet. Att både Nmap och arp-scan gör detta kan vara användbart då resultaten inte alltid är identiska, ett exempel på vilket kan ses i figur 5.1 och bilaga A för enheten med IP-adress 192.168.0.107, där arp-scan misslyckas med att identifiera tillverkaren medan Nmap sluter sig till att det är Samsung. Resultatet från Nmap visar även öppna portar för varje enhet, samt vilken tjänst som använder sig av porten. Vidare visas resultatet från ett försök till OS-fingerprinting, där Nmap även skriver ut sannolikheten för att resultatet är korrekt.

Snabb analys av resultat för enheten i figur 5.2

Det är mycket sannolikt att enheten är en skrivare. Denna slutsats baseras bland annat på att port 515, 631 och 9100 är vanliga skrivarportar och att förslagen för operativsystemet på enheten alla föreslår olika skrivare.

Vid analys utav ett par portar går det snabbt att komma fram till följande:

- **Telnet, port 23.** Detta är ett gammalt okrypterat protokoll för terminalinloggning över nätverk, som skickar lösenord i klartext och bör ersättas med SSH.
- **FTP, port 21.** FTP är ett gammalt okrypterat protokoll för filöverföring och det är lämpligt att byta till exempelvis SFTP.
- **HTTP, port 80.** Det är rimligt att ifrågasätta om HTTP behövs, eftersom HTTPS också används.

Från detta går det att dra slutsatsen att det vore lämpligt att sluta använda ett par protokoll och istället använda säkrare versioner. Det är viktigt att ta bort de tjänster som inte längre används, då färre öppna portar innebär färre möjliga angreppspunkter.

7 Diskussion

Först kommer resultat (kapitel 5) och analys (kapitel 6) att diskuteras, därefter val av verktyg, sedan vidare till tankar om säkerhet, olika miljöaspekter och slutligen övriga tankar och funderingar.

7.1 Resultat och analys

Det är intressant att arp-scan och Nmap gör lite olika tolkningar av MAC-adresserna. Arp-scan har tre listor som mappar adressområden till tillverkare, varav två uppdateras via inkluderade script men den sista listan uppdateras manuellt. Nmap däremot använder bara en av dessa listor, vilket gör det lite underligt att arp-scan misslyckades med att identifiera en tillverkare, såsom påpekades i analysen (kapitel 6.2.2).

För att ScanBox skall vara användbart för verkliga kundbesök behövs någon med rimligt mycket erfarenhet för att analysera resultaten hos kund, då även den delen gärna bör gå relativt snabbt.

7.2 Val av verktyg

Trots att Nmap hade kunnat användas både för att upptäcka enheter och för att portscanna dem gjordes valet att arp-scan skulle användas till upptäckandet. Detta dels därför att arp-scan utför uppgiften snabbare, men också för att antalet enheter skall kunna utgås ifrån när nivån för Nmap skall bestämmas. Då ScanBox skall vara väldigt snabb anpassas nivån för Nmap beroende på antalet aktiva enheter, vilket inte hade kunnat ske automatiskt utan att göra flera anrop till Nmap.

Ett annat verktyg som övervägdes istället för Nmap är masscan, som är specifikt designat för att vara en extremt snabb portscanner. Det har däremot mycket mer begränsad funktionalitet än Nmap och lämpar sig bäst för scanning av publika nätverk, såsom att scanna en specifik port över en mycket stor mängd adresser. Tester visade på att det är snabbare än Nmap, men resultaten är mer begränsade, och scanning av UDP-portar erbjuds ej.

7.3 Säkerhetsmässigt viktiga tankar

Då projektet syftat till att ta fram ett snabbt verktyg för sårbarhetsscanning har det inte funderats så mycket på långvarig hantering av insamlad data. Inte mer än att sådan enbart sparas på en server som ett fåtal personer har tillgång till, samt på ScanBox som det krävs fysisk access till (eller SSH via servern eller från det lokala nätverket). Även här skulle någon rutin för borttagning utav känslig data tas fram vid fortsatt användning utav ScanBox. Vid det här projektets avslut kommer all insamlad data att raderas då den inte är intressant mer än ur analys- och verifieringssyfte.

Skulle ScanBox fortsätta användas behöver den säkras mot fysiskt intrång, genom att lösenordsinloggning tas bort och endast inloggning via SSH lämnas kvar. Anledningen till att detta inte är gjorts är att möjligheten att koppla in tangentbord, mus och skärm underlättar vid implementering utav nya funktioner samt felsökning. Trots att ScanBox uppfyller de mål som fastställts i projektet har den ändå varit under utveckling hela tiden och valet gjordes att lämna kvar möjligheten till fysisk åtkomst.

7.4 Miljö och etik

Vissa delar utav penetrationstest är simpla och repetitiva. Genom att använda sig av ScanBox för en snabb första överblick av ett system kan delar av arbetet snabbas på. Detta kan innebära en förbättring av penetrationstestarens arbetsmiljö.

Trots att hårdvaran inte har ifrågasatts har den ändå diskuterats. Många system använder sig utav överdimensionerad hårdvara, kanske för att den fanns tillgänglig eller för att kunna expandera i framtiden. Ett sådant tankesättet leder dock till onödigt hög energiåtgång. Det kan verka som en liten skillnad, men tankesättet att

nöja sig med ”tillräckligt” bra saker går att applicera på många olika områden i vardagen och kan då på sikt få stor positiv påverkan på miljön.

ScanBox tar inte hänsyn till vilken typ av nätverk den kopplas in till eller huruvida nätverkets ägare tillåter att det scannas. På grund av graden av automation vore det mycket enkelt att använda ScanBox på ett olagligt sätt. Så länge som den konfiguration som angivits till servern är att utföra scanning vid uppstart kommer ScanBox då den kopplas in att scanna nätverket och ladda upp insamlad data till servern. ScanBox kommer då också att fungera som en illegal och dold ingång till nätverket, antingen tillfälligt eller tills vidare, om den inte är konfigurerad att stänga av sig. Kali Linux gör det enkelt att utnyttja detta på illvilliga sätt.

7.5 Övriga tankar och funderingar

Det är smidigt att ha MAC-adresser samt namn på tillverkaren av nätverkskort både på resultatet från arp-scan och från Nmap, eftersom det då inte är nödvändigt att bläddra mellan resultaten för att kolla upp denna data. Arp-scan visar samtliga anslutna enheter på ett enkelt och smidigt sätt, medan Nmap går in på mer detalj kring varje enhet, men inte visar helheten lika smidigt. Detta gör att båda resultaten fyller sin funktion och är rimliga att spara på.

Det har under projektets gång gjorts en undersökning kring att utöka med ytterligare verktyg, dessa var Nessus och OpenVAS. Det visade sig dock att Nessus inte är ett alternativ då det inte är kompatibelt med processorn på RPi. OpenVAS övervägdes som ett alternativ innan WiFi-scanning implementerades men övergavs till fördel för just WiFi. Detta dels för att det ansågs som ett för stort tillägg, både i scanningstid och i tid för implementering, men också för att WiFi-scanning ansågs som en mer intressant funktion att ha som diskussionsunderlag med potentiella kunder. OpenVAS är ett kraftfullt verktyg, men dess stora nackdel är att det tar ganska lång tid att scanna. Därför har det inte automatiskt en plats i ScanBox.

8 Förslag till fortsatt arbete

Det har inte varit svårt att hitta möjligheter till fortsatt arbete, då grunden till ScanBox är mycket flexibel och kan ha många olika användningsområden. Nedan listas några utav de mer intressanta möjligheterna:

- **Framtagning av komplett produkt.** För detta skulle det behöva tas fram färdiga säkerhetsrutiner, både för att hålla mjukvaran på ScanBox uppdaterad samt för hantering utav insamlad data.
- **Detektion av nya enheter.** Den skulle då behöva göras intrångssäker, ha automatiska uppdateringar, regelbundet scanna nätverk och skicka ut alarm eller notis vid förändring.
- **För skydd.** Möjliggöra detektion utav malware.
- **Penetrationstestningsverktyg.** ScanBox behöver göras intrångssäker, med diskret utformning. Förses med möjlighet till tysta inställningar, anslutning via 4G, exploatering av funna sårbarheter, och så vidare.
- **Återkommande sårbarhetsscanningar.** Om samma nätverk scannas vid flera olika tillfällen kan trendanalys utav datan göras, med mer avancerade rapporter. Där exempelvis visualisering utav datan kan peka på förändringar.
- **Utökad hantering utav resultat.** Såsom att lägga till länkar för *Service* i resultaten från Nmap, för att snabbare kunna kontrollera saker vid analys av resultat. Att skapa en bättre presentation utav insamlad data, eller att använda sig utav Azures databehandlingsmöjligheter.
- **Supersnabb nätverksutvärdering.** Utveckla ScanBox för att snabbt testa ett nätverk innan en annan maskin kopplas upp, för att testa att nätverket är tillräckligt säkert. Om så är fallet signalera till användaren att det är okej.

Referenser

[1] C. Hofbauer. Svensk it-säkerhet håller inte måttet. *Dagens industri* 13 november (2017), 10.

[2] *Viktigare med IT-säkerhet när Internet attackerar.* https://www.if.se/foretag/forsakringar/ansvarsforsakring/databrottsforsakring/databrott/internet-attackerar. Hämtat: 2017-11-07.

[3] *Raspberry Pi FAQs - Frequently Asked Questions.* https://www.raspberrypi.org/help/faqs/. Hämtat: 2017-11-17.

[4] *Raspberry Pi 3b.* https://www.raspberrypi.org/products/raspberry-pi-3-model-b/. Hämtat: 2017-11-07.

[5] *Intro to Microsoft Azure | Microsoft Docs.* https://docs.microsoft.com/en-us/azure/fundamentals-introduction-to-azure. Hämtat: 2017-11-17.

[6] *What is Kali Linux? | Kali Linux.* https://docs.kali.org/introduction/what-is-kali-linux. Hämtat: 2017-10-25.

[7] *Kali Linux – Raspberry Pi | Kali Linux.* https://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi. Hämtat: 2017-10-25.

[8] *Downloading Kali Linux.* https://docs.kali.org/introduction/download-official-kali-linux-images. Hämtat: 2017-11-10.

[9] *Kali Linux - Raspberry Pi2.* https://docs.kali.org/kali-on-arm/kali-linux-raspberry-pi2. Hämtat: 2017-11-10.

[10] *systemd (5) - Linux Man Pages.* http://man7.org/linux/man-pages/man5/systemd.unit.5.html. Hämtat: 2017-11-10.

[11] *crontab (5) - Linux Man Pages.* http://man7.org/linux/man-pages/man5/crontab.5.html. Hämtat: 2017-11-10.

[12] J. F. Kurose och K. W. Ross. *Computer Networking: A Top-Down Approach.* English. 6. utg. Pearson Education, 2013. ISBN: 978-0-273-76896-8.

[13] *RFC 1918: Address Allocation for Private Internets.* http://www.ietf.org/rfc/rfc1918.txt. Hämtat: 2017-11-10.

[14] *RFC 6335: Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry.* https://tools.ietf.org/html/rfc6335. Hämtat: 2017-11-10.

[15] *Port Scanning Techniques | Nmap Network Scanning.* https://nmap.org/book/man-port-scanning-techniques.html. Hämtat: 2017-11-17.

[16] G. ‘ Lyon. *Nmap Network Scanning.* English. ISBN: 978-0-9799587-1-7.

[17] *SSH (Secure Shell).* https://www.ssh.com/ssh/. Hämtat: 2017-11-10.

[18] *SFTP - SSH Secure File Transfer Protocol.* https://www.ssh.com/ssh/sftp/. Hämtat: 2017-11-10.

[19] *SSH Tunnel.* https://www.ssh.com/ssh/tunneling/. Hämtat: 2017-11-10.

[20] *SSH Port Forwarding Example.* https://www.ssh.com/ssh/tunneling/example. Hämtat: 2017-11-10.

[21] L. Allen, S. Ali och T. Heriyanto. *Kali Linux: assuring security by penetration testing.* English. 2. utg. Birmingham: Packt Publishing, 2014. ISBN: 9781849519496.

[22] *SecurityFocus.* http://www.securityfocus.com/. Hämtat: 2017-12-05.

[23] *Exploits Database by Offensive Security.* https://www.exploit-db.com/. Hämtat: 2017-12-05.

[24] *Arp-scan User Guide - NTA-Wiki.* http://www.nta-monitor.com/wiki/index.php/Arp-scan_User_Guide. Hämtat: 2017-10-31.

[25] *Nmap: the Network Mapper - Free Security Scanner.* https://nmap.org/. Hämtat: 2017-11-10.

[26] *GitHub - robertdavidgraham/masscan: TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.* https://github.com/robertdavidgraham/masscan. Hämtat: 2017-11-13.

A Resultat från arp-scan

```
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (
http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1 [redacted]   ASUSTek COMPUTER INC.
192.168.1.11 [redacted]   Dell Inc.
192.168.1.12 [redacted]   Raspberry Pi Foundation
192.168.1.17 [redacted]   Cisco Systems, Inc
192.168.1.18 [redacted]   D-Link International
192.168.1.25 [redacted]   D-Link International
192.168.1.62 [redacted]   Raspberry Pi Foundation
192.168.1.74 [redacted]   D-Link International
192.168.1.78 [redacted]   ASUSTek COMPUTER INC.
192.168.1.94 [redacted]   ASUSTek COMPUTER INC.
192.168.1.108 [redacted]   NETGEAR
192.168.1.110 [redacted]   D-Link International
192.168.1.130 [redacted]   Cisco-Linksys, LLC
192.168.1.131 [redacted]   BUFFALO.INC
192.168.1.43 [redacted]   Apple, Inc.
192.168.1.71 [redacted]   D-Link International
192.168.1.165 [redacted]   Cisco Systems, Inc
192.168.1.166 [redacted]   Hewlett Packard
192.168.1.76 [redacted]   D-Link International
192.168.1.178 [redacted]   Hewlett Packard
192.168.1.201 [redacted]   D-Link International
192.168.1.218 [redacted]   Samsung Electronics Co.,Ltd
192.168.1.239 [redacted]   Cisco Systems, Inc
192.168.1.150 [redacted]   D-Link International
192.168.1.247 [redacted]   Samsung Electronics Co.,Ltd
192.168.1.249 [redacted]   (Unknown)
192.168.1.196 [redacted]   Gigaset Communications GmbH
192.168.1.117 [redacted]   Apple, Inc.
192.168.1.90 [redacted]   HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.217 [redacted]   D-Link International
192.168.1.164 [redacted]   D-Link International
192.168.1.222 [redacted]   D-Link International
192.168.1.187 [redacted]   (Unknown)

34 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 3569.166 seconds (0.07
hosts/sec). 34 responded
```

B Resultat från Nmap

TCP

Nmap Scan Report - Scanned at Tue Nov 14 18:32:23 2017

Scan Summary | **192.168.0.1** | **192.168.0.101** | **192.168.0.102** | **192.168.0.104** | **192.168.0.105** | **192.168.0.106** | **192.168.0.107** | **192.168.0.108**

Scan Summary

Nmap 7.60 was initiated at Tue Nov 14 18:32:23 2017 with these arguments:
nmap -sS -O -sV -oA /root/Documents/data/2017-11-14_16-15-14_scan/2017-11-14_16-15-14_nmap_TCP_1000_eth0 --privileged --disable-arp-ping -Pn -n --max-rate 100 --defeat-rst-ratelimit --max-os-tries 1 --max-retries 3 --host-timeout 2400 --max-hostgroup 100 -iL /root/Documents/data/2017-11-14_16-15-14_scan/2017-11-14_16-15-14_active_IP_addresses_eth0

Verbosity: 0; Debug level 0

Nmap done at Tue Nov 14 18:38:32 2017; 8 IP addresses (8 hosts up) scanned in 372.63 seconds

192.168.0.1

Address

- 192.168.0.1 (ipv4)
- [redacted] - D-Link International (mac)

Ports

The 991 ports scanned but not shown below are in state: **closed**

- 991 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [2])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack	dnsmasq	2.45	
80	tcp	open	http	syn-ack	lighttpd	1.4.26	
7911	tcp	open	omapi	syn-ack	ISC (BIND|DHCPD) OMAPI		
8080	tcp	open	http-proxy	syn-ack			
8081	tcp	open	blackice-icecap	syn-ack			
9000	tcp	open	ws-discovery	syn-ack	Ricoh WS Discovery		
20005	tcp	open	btx	syn-ack			

Remote Operating System Detection

- Used port: **53/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **35097/udp (closed)**
- OS match: **Linux 2.6.19 - 2.6.36 (100%)**

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set
System Uptime	284037 seconds (last reboot: Sat Nov 11 11:44:35 2017)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

System Uptime	284037 seconds (last reboot: Sat Nov 11 11:44:35 2017)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=201 (Good luck!)
IP ID Sequence Generation	All zeros

192.168.0.101

Address

- 192.168.0.101 (ipv4)
- [redacted] - Asustek Computer (mac)

Ports

The 993 ports scanned but not shown below are in state: **filtered**

- 993 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows 7 - 10 microsoft-ds		workgroup: WORKGROUP
554	tcp	open	rtsp	syn-ack			
2869	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
10243	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

Remote Operating System Detection

- Used port: **135/tcp (open)**
- OS match: **Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)**
- OS match: **Microsoft Windows Embedded Standard 7 (100%)**
- OS match: **Microsoft Windows Phone 7.5 or 8.0 (100%)**
- OS match: **Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)**
- OS match: **Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)**

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set
System Uptime	2857319 seconds (last reboot: Thu Oct 12 17:56:33 2017)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=263 (Good luck!)
IP ID Sequence Generation	Incremental

192.168.0.102

Address

- 192.168.0.102 (ipv4)
- [redacted] - Asustek Computer (mac)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Ports

Ports

The 995 ports scanned but not shown below are in state: **filtered**

- 995 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows 7 - 10 microsoft-ds		workgroup: WORKGROUP
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
49156	tcp	open	unknown	syn-ack			

Remote Operating System Detection

- Used port: **135/tcp (open)**
- OS match: **Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)**
- OS match: **Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)**

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set
System Uptime	15867 seconds (last reboot: Tue Nov 14 14:14:05 2017)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=250 (Good luck!)
IP ID Sequence Generation	Busy server or unknown class

192.168.0.104

Address

- 192.168.0.104 (ipv4)
- [redacted] - Liteon Technology (mac)

Ports

The 999 ports scanned but not shown below are in state: **filtered**

- 999 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

Remote Operating System Detection

- Used port: **5357/tcp (open)**
- OS match: **Microsoft Windows Server 2008 or 2008 Beta 3 (100%)**
- OS match: **Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)**
- OS match: **Microsoft Windows Embedded Standard 7 (100%)**
- OS match: **Microsoft Windows 8.1 R1 (100%)**
- OS match: **Microsoft Windows Phone 7.5 or 8.0 (100%)**
- OS match: **Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)**
- OS match: **Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)**

Go to top
Toggle Closed Ports
Toggle Filtered Ports

(100%)
- OS match: **Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)**

Misc Metrics (click to expand)

192.168.0.105

Address

- 192.168.0.105 (ipv4)
- [redacted] - Sony Interactive Entertainment (mac)

Ports

The 1000 ports scanned but not shown below are in state: **closed**

- 1000 ports replied with: **resets**

Remote Operating System Detection

Unable to identify operating system.

- Used port: **1/tcp (closed)**
- Used port: **39056/udp (closed)**

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set
Network Distance	1 hops

192.168.0.106

Address

- 192.168.0.106 (ipv4)
- [redacted] - Nintendo (mac)

Ports

The 1000 ports scanned but not shown below are in state: **closed**

- 1000 ports replied with: **resets**

Remote Operating System Detection

Unable to identify operating system.

- Used port: **1/tcp (closed)**
- Used port: **31863/udp (closed)**

Misc Metrics (click to expand)

192.168.0.107

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Address

192.168.0.107

Address

- 192.168.0.107 (ipv4)
- [redacted] - Samsung Electro-mechanics(thailand) (mac)

Ports

The 837 ports scanned but not shown below are in state: **filtered**

- 837 ports replied with: **no-responses**

The 163 ports scanned but not shown below are in state: **closed**

- 163 ports replied with: **resets**

Remote Operating System Detection

Unable to identify operating system.

- Used port: **6100/tcp** (**closed**)

Misc Metrics (click to expand)

192.168.0.108

Address

- 192.168.0.108 (ipv4)
- [redacted] - Intel Corporate (mac)

Ports

The 1000 ports scanned but not shown below are in state: **closed**

- 1000 ports replied with: **resets**

Remote Operating System Detection

Unable to identify operating system.

- Used port: **1/tcp** (**closed**)
- Used port: **33559/udp** (**closed**)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Misc Metrics (click to expand)

UDP

Nmap Scan Report - Scanned at Tue Nov 14 18:38:33 2017

Scan Summary | **192.168.0.1** | **192.168.0.101** | **192.168.0.102** | **192.168.0.104** | **192.168.0.105** | **192.168.0.106** | **192.168.0.107** | **192.168.0.108**

Scan Summary

Nmap 7.60 was initiated at Tue Nov 14 18:38:33 2017 with these arguments:
nmap -F -sU -oA /root/Documents/data/2017-11-14_16-15-14_scan/2017-11-14_16-15-14_nmap_UDP_100_eth0 --privileged --disable-arp-ping -Pn -n --max-rate 100 --max-retries 3 --host-timeout 1800 --max-hostgroup 100 -iL /root/Documents/data/2017-11-14_16-15-14_scan/2017-11-14_16-15-14_active_IP_addresses_eth0

Verbosity: 0; Debug level 0

Nmap done at Tue Nov 14 18:39:26 2017; 8 IP addresses (8 hosts up) scanned in 52.86 seconds

192.168.0.1

Address

- 192.168.0.1 (ipv4)

Ports

The 67 ports scanned but not shown below are in state: **open|filtered**

- 67 ports replied with: **no-responses**

The 31 ports scanned but not shown below are in state: **closed**

- 31 ports replied with: **port-unreaches**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	udp	open	domain	udp-response			
520	udp	open	route	udp-response			

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set

192.168.0.101

Address

- 192.168.0.101 (ipv4)

Ports

The 99 ports scanned but not shown below are in state: **open|filtered**

- 99 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
137	udp	open	netbios-ns	udp-response			

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Misc Metrics (click to expand)

Metric	Value
Ping Results	user-set

192.168.0.102

Address

- 192.168.0.102 (ipv4)

Ports

The 99 ports scanned but not shown below are in state: **open|filtered**

- 99 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
137	udp	open	netbios-ns	udp-response			

Misc Metrics (click to expand)

192.168.0.104

Address

- 192.168.0.104 (ipv4)

Ports

The 99 ports scanned but not shown below are in state: **open|filtered**

- 99 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
137	udp	open	netbios-ns	udp-response			

Misc Metrics (click to expand)

192.168.0.105

Address

- 192.168.0.105 (ipv4)

Ports

The 97 ports scanned but not shown below are in state: **closed**

- 97 ports replied with: **port-unreaches**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
68	udp	open|filtered	dhcpc	no-response			
1900	udp	open|filtered	upnp	no-response			
5353	udp	open	zeroconf	udp-response			

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Misc Metrics (click to expand)

192.168.0.106

Address

- 192.168.0.106 (ipv4)

Ports

The 100 ports scanned but not shown below are in state: **closed**

- 100 ports replied with: **port-unreaches**

Misc Metrics (click to expand)

192.168.0.107

Address

- 192.168.0.107 (ipv4)

Ports

The 100 ports scanned but not shown below are in state: **open|filtered**

- 100 ports replied with: **no-responses**

Misc Metrics (click to expand)

192.168.0.108

Address

- 192.168.0.108 (ipv4)

Ports

The 58 ports scanned but not shown below are in state: **closed**

- 58 ports replied with: **port-unreaches**

The 42 ports scanned but not shown below are in state: **open|filtered**

- 42 ports replied with: **no-responses**

Misc Metrics (click to expand)

Go to top
Toggle Closed Ports
Toggle Filtered Ports