SÄKERHETSTESTA NÄTVERKET MED KALI LINUX

LINUXBASERADE OPERATIVSYSTEM ÄR POPULÄRA. En distribution som skiljer ut sig är Kali, då fokus ligger på tester av säkerheten. Detta praktiseras i artikeln, och dessutom bjuds det på en del annat tänkvärt.

JARI HEISKANEN

Penetrationstester används allt mer av organisationer för att garantera säkerheten i informationssystem och tjänster. Svagheter i säkerheten kan då fastställas innan de blir exponerade för eventuella hot.

Intrång i nätverk, datastöld och attacker orsakade av hackare samt missnöjda anställda fortsätter att öka. De risker och kostnader som finns i samband med detta är stora.

Dyra investeringar kan vara felaktigt konfigurerade, oavsett om det gäller mjukvara eller hårdvara. Dessa svagheter kan på sikt ge en inkräktare tillgång till känslig information.

TAKTPINNEN HAR ÖVERLÄMNATS

Backtrack, baserad på Ubuntu, är en mycket populär distribution när det gäller penetrationstester. Men nu har taktpinnen tagits över av Kali Linux. Kali är det nya namnet på Backtrack.

Kali Linux har förbättrats jämfört med Backtrack på många sätt. Backtrack består i princip av Ubuntu och säkerhetsverktyg som placeras i katalogen ”pentest”. Dessa har användaren fått köra genom att navigera till katalogen. En följd var att uppdateringar blev svårare än nödvändigt, eftersom verktygen inte var riktiga installationer som skulle kunna uppdateras från pakethanteraren.

Kali har byggts om från grunden. Den grundar sig helt på Debians standarder.

AVSKALAD MILJÖ

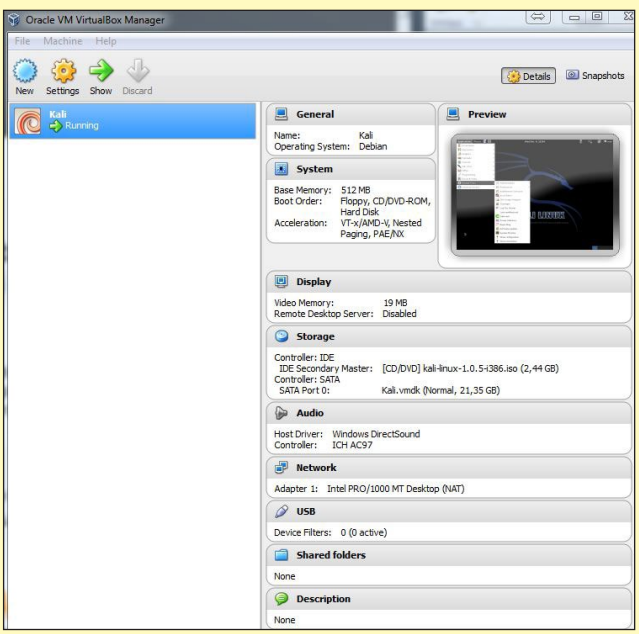
Den senaste versionen av Kali är 1.0.5. Skrivbordsmiljön som följer med är Gnome. Bland de andra standardpaketen finns webbläsaren Iceweasel, MySQL, Apache och en SSH-server.

När det gäller säkerhetsverktyg finns det fler än 300 sådana för penetrationstester. Dessa återfinns i menyn Program > Kali Linux. Bortsett från detta finns det mycket få paket.

Distributionen laddas ned från *www.kali.org/downloads/*. Startmenyn ger dig alternativ för en grafisk eller textbaserad installation. Du kan använda en live-CD eller starta installationsprogrammet för installation. Sedan är det bara att följa anvisningarna på skärmen.

Det finns även diskavbildningsfiler till Raspberry Pi, Cubox, Samsung Chromebook och flera andra. Likaså finns möjlighet att bygga en egen iso-fil.

Ett virtuellt ”penetrationslabb” är ett bra sätt att lära sig Kali. En virtualiseringsmjukvara underlättar, då den säkra miljön inte riskerar att ”sänka” ett nätverk. Kör från en iso-fil med lämpligt program, till exempel Virtualbox.



◀ Ett virtuellt ”penetrationslabb” är ett bra sätt att lära sig Kali. Du kan då laborera utan att riskera att ”sänka” ett nätverk.

JÄMFÖRT MED DEBIAN

Kali Linux är inriktad på professionella penetrationstester och säkerhetsgranskningar. Några förändringar har gjorts för att anpassa Debian. Distributionen är utformad för att köras som ”root”-användare. Kali Linux innehåller ”sysvinit hooks” som inaktiverar nätverkstjänster som standard. Dessa ”hooks” låter oss installera olika tjänster på Kali Linux samtidigt som distributionen förblir säker oavsett vilka paket som installeras. Tjänster som Bluetooth ”svartlistas”.

LATA KALI

Några utvecklare har skapat ett bash-skript som kan automatisera uppdateringar och installera nya verktyg i ditt Kalisystem. Det har gjort det mycket lättare för användarna, vilket namnet ”Lazy Kali” antyder. Du får alla uppdateringar till Kali och dina databaser på ett ställe genom att köra det här skriptet. Du kan ladda ner Lazy Kali från *https://code.google.com/p/lazykali/*.

FLER PROGRAM

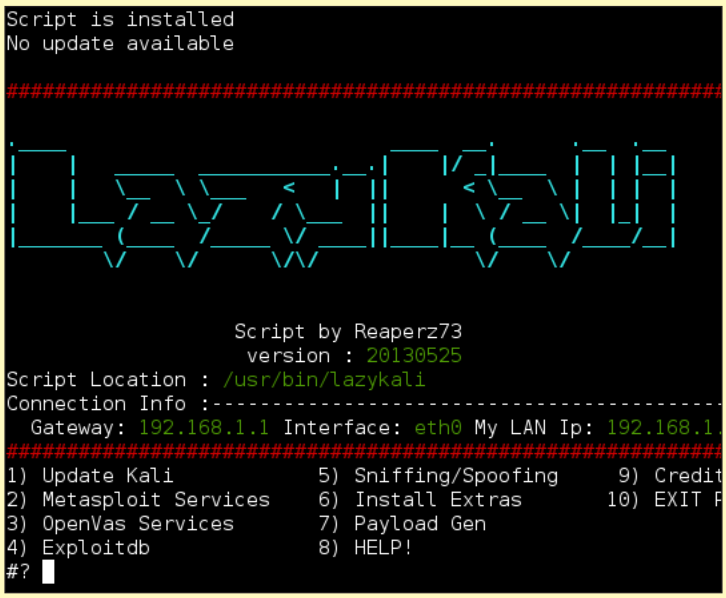
Behöver du extra program utöver dem som följer med går det snabbt att ordna.

På samma webbplats som Lazy Kali finns även ”hackpack”. Ladda ned filen från webbplatsen och packa upp katalogen. Gå till katalogen. Packa upp och kör ”install.sh”:

```
tar zxvf hackpack.tar.gz
/hackpack/install.sh
```

När du sedan klickar på programknappen i övre vänstra hörnet på skrivbordet kommer du att se en ny flik – ”HackPack”. Fliken innehåller de verktyg som finns i paketet.

Debian använder även så kallade ”unofficial repositories” som kan vara användbara för dem som använder Kali. Läs mer på: *https://wiki.debian.org/UnofficialRepositories*.



◀ Ett bash-skript kan automatisera uppdateringar och installera nya verktyg i ditt Kalisystem. Det har gjort det mycket lättare för användarna, vilket namnet ”Lazy Kali” antyder.

NÄTVERKSTJÄNSTER INAKTIVERADE

Ur säkerhetssynpunkt är det viktigt att Kali inte gör det möjligt för externa tjänster att avlyssna trafiken.

Målet är att minimera exponeringen i standardläget.

Undertecknad fick problem med lokal anslutning mot internet. Det kan hända av oklar anledning. Du kan kontrollera nätverksuppkopplingen med följande:

```
lspci |grep Ethernet
```

Här finns ”Ethernet controller” i form av Intel. Drivrutiner är på plats. Då är nätverkstjänsten inte igång. Ett nytt test:

```
nano /etc/NetworkManager/NetworkManager.conf
```

Detta gav ”managed=false”. En ändring till ”true” görs i editorn Nano. Spara och starta tjänsten igen:

```
/etc/init.d/network-manager restart
```

Nu är nätverket igång för penetrationstest.

BRA PENETRATIONSVERKTYG

Det finns en separat lista med tio populära säkerhetsverktyg. Dessa är de mest användbara och populäraste för penetrationstester, enligt företaget som har utvecklat Kali. Låt oss ta en titt på några av dem.

Några allmänna steg tas för att utföra en WLAN-säkerhetsbedömning, följt av ytterligare tätning av säkerhetshål. Det första är att kontrollera utrustningen och installationerna.

Det första som sker är en bekräftelse av en giltig WLAN-uppkoppling.

Alla kommandon skrivs i ett terminalfönster. Börja med att skriva kommandot nedan:

```
ifconfig wlan0 up
```

Detta visas genom att en diod för trådlös anslutning tänds på datorn. Du har skapat ”wlano”, vilket är den trådlösa enhet som kommer att användas.

Dessutom bör kommandot ”kill” användas för att ”döda” alla processer som skulle kunna störa testerna. Programmet ”airmon-ng” kan hjälpa dig med att identifiera processer som kan vara störande för WLAN-adaptern:

```
airmon-ng check
```

Tre processer körs som kan orsaka problem. För att undvika störningar avslutas onödiga processer med kommandot ”kill”:

```
kill 2228
kill 2327
kill 2749
```

Dags för start av WLAN. Det görs med följande:

```
airmon-ng start wlan0
```

Du bör se texten ”monitor mode enabled on mono”. Enheten ”mono” visar att du har en aktiv ”pseudo”-enhet som övervakar ”wlano”. Från och med nu kommer”mono” att användas som vår enhet. Enheten är inställd i monitorläge (wlano) som tillåter övervakning av WLAN-trafik. Du kan också injicera WLAN-paket genom den.

För att fånga in data används airodump-ng. Detta verktyg fångar den kommunikation som den trådlösa enheten kan se:

```
airodump-ng mon0
```

Sökningen börjar efter SSID på det nätverk som testas. När namnet på nätverket syns behöver BSSID spelas in för det nätverket. Förutsättningen är användning av en BSSID och en kanal. För artikeln användes undertecknads egen WLAN-uppsättning.

Terminalfönstret visar ett BSSID – här i form av 84:1B:5E:ED:97:BA på kanal tolv. Bland de fält som visas syns ENC och CIPHER som är WPA2 och CCMP. Detta talar om att det är ett WPA2-system som är säkrat av CCMP som måste knäckas.

Nu när BSSID och kanal för SSID har fångats upp startas ”airodump” med dessa detaljer. Tryck Ctrl-C för att stoppa terminalfönstret och starta sedan om programmet. Kom ihåg att byta ut BSSID nedan mot din egen BSSID och kanalen mot den som kommer upp i din terminal:

```
airodump-ng mon0 --bssid
84:1B:5E:ED:97:BA --channel 12
```

Monitorn kommer nu att hålla sig till en kanal och fokusera på endast en BSSID, vilket ger möjlighet att begränsa attacken. Eftersom loggning av data till en fil inte har börjat kommer processen att fortsätta tills det är dags att fånga data för att börja attacken.

INJICERA PAKET

Främsta skälet till att injicera ett paket är att få en enhet att utföra ett nyckelutbyte. Då kan nyckeln fångas för senare dekryptering.

Medan ”airodump-ng” fortfarande är igång kan du öppna ett annat terminalfönster. Från denna terminal kontrolleras att injektionen arbetar med WLAN-adaptern och det AP som övervakas. För injektionen används ”aireplay-ng”:

```
aireplay-ng mon0 -a 84:1B:5E:ED:97:BA
-9
```

Denna metod kommer att skicka ett falskt paket från AP till enheten samt be den att autentisera och återautentisera. Denna omverifiering bör fångas upp och användas i lösenordsattacken.

Efter en tid har en giltig WPA-handskakning identifierats för BSSID. Nu kan du börja knäcka lösenordet. Lyckas det kommer terminalfönstret att visa WPA-handskakningen.

LOGG OCH RAPPORT

Börja med att stoppa airodump med Ctrl-c. Starta loggningen med följande:

```
airodump-ng mon0 -BSSID
84:1B:5E:ED:97:BA --channel 11 -w
textfil
```

Det är ”-w” som anger att fångade data ska dumpas till en fil. Filens namn anges, i det här fallet ”textfil”. Den här filen kommer att användas i vårt försök.

För att visa filerna används följande:

```
ls textfil*
```

Detta visar flera filer. Den viktigaste är ”textfil-01.cap” som innehåller datan. Nu när du har en ”capture”-fil som innehåller en WPA-handskakning är WLAN-delen klar.

Nu testar du textfilen. Att knäcka lösenordet kan ta lång tid, men det kan göras offline och i bakgrunden.

KNÄCKA LÖSENORDET

Handskakningen innehåller en krypterad version av WLAN-lösenordet. Det är detta lösenord som ska knäckas. Eftersom lösenordet är krypterat är en rimlig metod att gissa lösenord.

För uppgiften används programmet aircrack-ng tillsammans med en ordlista. Det gäller att lokalisera en omfattande ordlista.

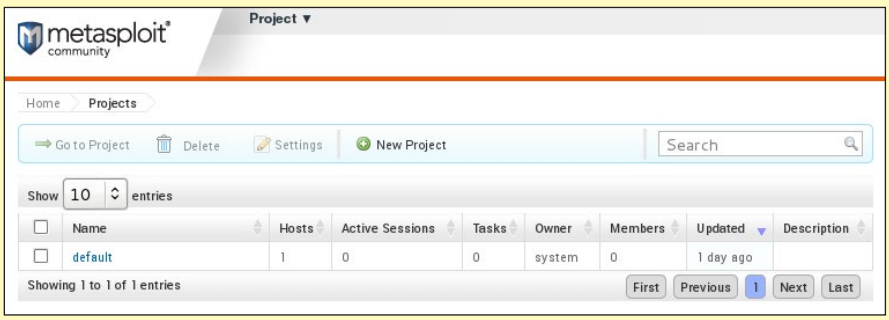
TESTA SÄKERHETEN MOT ENKLA LÖSENORD

Nu börjar du testa med ordlistan ”ord.txt”:

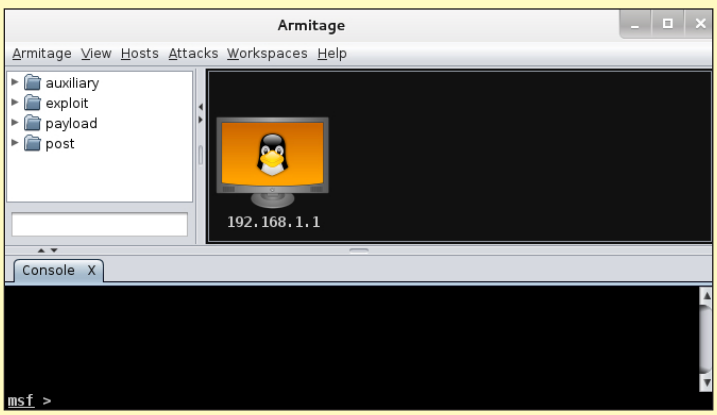
```
aircrack-ng -a 2 textfil-01.cap -b
84:1B:5E:ED:97:BA -w ord.txt
```

Handlar det om ett komplext lösenord med specialtecken kan det ta lång tid. Nu var dock testlösenordet väldigt enkelt – password. Det knäcktes på under en sekund.

För att säkra systemet måste du attackera det hårdare än en eventuell inkräktare. Lyckas du inte knäcka lösenordet med denna metod finns det andra som bör testas. Detta för att verkligen försöka upptäcka säkerhetsbrister. Testa med andra ordlistor eller en ”brute force”-attack.



▲ Metasploit är ett användbart granskningsverktyg, fritt tillgängligt för säkerhetsproffs. Ramverket finns som gratis och kommersiell version. Det har en struktur som du kan bygga vidare på för anpassning.



◀ Det underlättar med ett grafiskt användargränsnitt. Det finns ett sådant för Metasploit i form av Armitage.

MODIFIERAD ATTACK

En ”brute force” tar sannolikt för lång tid. En ordlista kanske inte täcker in lösenordet.

Då återstår en modifierad metod. Du kan skriva egna skript eller använda verktyget ”john”. Detta verktyg är utformat för att knäcka lösenordsfiler.

Programmet kan visserligen gissa lösenorden, men det kan ta lång tid. Nedan används programmet helt enkelt för att skapa en lösenordslista som ”pipas” till aircrack-ng:

```
john -w:ord.txt -stdout-rules |
aircrack-ng -a 2 textfil-01.cap -b
84:1B:5E:ED:97:BA -w -
```

Det tar bara en bråkdels sekund att knäcka lösenordet ”password”.

Detta var ett typiskt exempel på WLAN-penetrationstest. Flera program som samarbetar gör det enkelt att penetrationstesta med Kali. En god lösenordspolicy motverkar den här typen av attack.

RAMVERKET METASPLOIT

Det är svårt att inte nämna Metasploit i sammanhanget. Det är ett av de mest användbara granskningsverktygen för säkerhetsproffs. Ramverket finns som gratis och kommersiell version. Det ger en infrastruktur som du kan bygga vidare på efter egna behov.

Du hittar det under Program > Kali Linux > Exploitation tools > Metasploit. Starta tjänsterna i terminalfönstret först:

```
service postgresql start
service metasploit start
msfconsole
```

Armitage är ett grafiskt gränssnitt för Metasploit. Programmet är enkelt att använda. Det finns under Program > Kali Linux > Exploitation tools > Network exploitation > Armitage. Det kommer upp ett fönster där du anger information om värd, portnummer, användare och lösenord.

LAGLIGA METODER

Tänk på att bara använda Kali om du har tillåtelse från nätverksägaren. Distributionen är till för penetrationstester på system som du har ansvar för eller på system som du testar. Saknar du behörighet men ändå utför ett penetrationstest är det en olaglig handling.

Kali Linux är en utmärkt distribution för att identifiera säkerhetsluckor eller brister i ditt nätverk. Dessutom är distributionen relativt användarvänlig. ■

Webbresurser
Kali Linux:
www.kali.org
Offensive Security:
www.offensive-security.com