COMPUTERWORLD

The Hacking Dojo 5 - Sådan hacker du - Det første rigtige hackerværktøj

I denne artikel tager jeg fat på det første rigtige hacker værktøj. NetCat er en klassiker der stadig bruges den dag i dag, både i praksis og på de fleste kurser du kommer ud for. Denne artikel er også forudsætnings skabende for de kommende artikler

Skrevet den **13. Nov 2010** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Indtil nu har vi kigget på værktøjer og teknikker som både bliver brugt af hackerne og som også bliver brugt af dygtige netværks administratorer og sikkerhedseksperter i deres daglige arbejde. Det vi nu skal til, er et decideret hackerværktøj som man ikke vil finde i en almindelig administrators værktøjskasse og samtidig er et virkelig klassisk værktøj som en hver hacker kender og bruger ofte

NetCat

NetCat er et rigtigt fleksibelt værktøj som af hackere og andre ofte kaldes "The Swiss army knife of hacking". Hvis man skal beskrive hvad NetCat kan uden at det blive meget teknisk, så handler det om at skrive til eller læse fra TCP eller UDP porte, med andre ord at virke som både klient og server.

NetCat kaldes ofte også for en bagdør, men den betegnelse er jeg ikke vild med selvom den egentlig er dækkende. Når folk høre betegnelsen bagdør, så forestiller de sig at man uploader NetCat til en computer og får den kørt, så man kan bruge bagdøren til at komme ind af og det er ikke sådan NetCat bruges.

I stedet for at forsøge at beskrive præcist hvad NetCat er, så har det mere mening at gøre lidt ud af øvelserne, idet de illustrere hvordan NetCat anvendes.

Lab opsætning.
Igen får du brug for mere end en computer, og jeg vil anbefale dig at arbejde med både Windows og Linux idet du som hacker får brug for at kunne opsætte Netcat på begge styresystemer og kunne bruge NetCat til at overføre filer og kommunikerer fra maskiner med forskellige styresystemer. Du bør lave alle øvelserne både fra Windows til Linux og omvendt samt fra Linux til Linux og fra Windows til Windows.

Du skal her være opmærksom på at de fleste antivirus programmer fanger NetCat og sletter den, hvorfor du som minimum bør disable den slags. Hvis du vælger at prøve at bruge NetCat via et netværk, bør du kontakte netværksadministratoren så han ikke bliver forskrækket over den trafik der genereres og vil du forsøge over internettet skal du være meget forsigtig. Husk at du når du sætter NetCat op som en bagdør på din egen maskine ikke rigtig kan kontrollerer hvem der bruger den. Du bør derfor sidde ved maskinen hele tiden mens du laver øvelserne og du bør fjerne NetCat når du er færdig.

Øvelser

1. Vi starter som sædvanligt med Google og kommandoen man netcat på din virtuelle Linuxboks. Læs hvad der er at læse, find de gode eksempler og beskrivelser og forklaringer på de begreber du ikke lige har styr på. Google er din ven.

2. NetCat bruges ofte som en slags omvendt bagdør. Hackeren opsætter NetCat på sin egen maskine til at lytte på en port, hvorefter han med et exploit får den maskine han hacker til at forbinde sig ud til sin egen maskine. I denne første lille øvelse opsætter du Netcat til at lytte på port 4444 på din egen maskine og

forbinder derefter fra en anden maskine med NetCat på samme port. I denne øvelse bruger du NetCat både som klient og server. Du vil kunne fine denne øvelse beskrevet flere steder på nettet

3. NetCat kan selvfølgelig bruges til andet og mere end blot at forbinde sig fra en maskine til en anden. Prøv at opsætte NetCat på to maskiner til at Chatte eller til at overføre filer med. Denne øvelse kan laves simpelt og avanceret og du bør lave begge. Den simpel metode opsætte to forskellige kanaler en fra den ene maskine til den anden og en omvendt, Chat øvelsen kan også laves mere avanceret hvor en kanal bære både kommunikation og fra hver maskine. Dette er både mere elegant og bedre ud fra et hacker synspunkt da den kun brugeren port. Husk også at NetCat sagtens kan anvendes sammen med andre utilities og kommandoer f.eks. cat, cmd, < og andet hvilket ofte er nødvendigt.

Hint:
flyt en fil fra serveren til klienten:
server: nc -l -p [port] < [filnavn]
klient: nc [serverIP] [port] > [filnavn]

skub en fil fra clienten til en server:
servere: nc -l -p [port] > [filnavn]
klient: nc [serverIP] [port] < [filnavn]

4. NetCat bruges ofte i informationsindhentnings fasen til enkle port scanninger og banner grapping. Læs via google hvordan du gør og prøv derefter i praksis på din virtuelle miljø at portscanne samt at grabber bannere fra f.eks. en web server. Det at grabbe et banner er faktisk ikke en ulovlig handling idet banneret er en del at protokollerne. Du kan således forsøge dig med banner grapping på det rigtige internet, men forsigtighed tilrådes, øv dig først før du går skarpt.

Hint:
nc -v -w3 -z [targetIP] [start port] - [slut port]

5. Et relay er en mellemstation og NetCat bruges ofte netop som relay. Der kan være flere grunde til dette, moderne netværk kan være opdelt i zoner med firewalls eller anden form for filtrering mellem, hvor kun enkelte maskiner kan kommunikerer mellem zonerne via enkelte porte eller protokoller. I en sådan situation kan et NetCat Relay være en af metoderne til at tunnele ting ind og ud. En anden grund til at bruge et NetCat Relay er at skjule sig selv. Ved at hoppe mellem forskellige maskiner på LAN eller på internettet f.eks. i flere forskelle lande, gør man det meget svært for andre at finde frem til den oprindelige angriber.

NetCat Relays bruges også til at sinke fjenden. Ved at opsætte relays på det netværk man hacker, kan men få den der skal undersøge hvad der er sket, til at bruge meget lang tid på at rode rundt med maskiner der ikke rigtigt har været brugt til det der batter.

Øvelsen går ud på at opsætte et relay med mindst en mellemstation. Brug gerne den avancerede metode fra øvelse 3 og har du mulighed for det så prøv også med 2 eller flere mellemstationer og hust at sniffe på netværket mens du gør det.

Hint:
The three-netcat approach: nc -l -p 11111 | nc next_hop 54321 | nc orevious_hop 22222
The batch file approach: nrrelay.bat (nc next_hop 54321). Kommando nc -l -p 11111 -e ncrelay.bat
The inetd approach (linux): 11111 stream tcp mowait nobody /usr/sbin/tcpd /usr/bin/nc next_hop 54321
The backpipe approach:
$ mknod backpipe p
$ nc -l -p 11111 0<backpip | nc next_hop 54321 1>backpipe

Backpipe metoden er klart den mest elegante. Brug google og se hvad du kan finde, men brug alle metoder og husk at sniffe mens du gør det.

6. NetCat er et relativt gammelt værktøj, og selvom det er blevet løbende opdateret, så findes i dag en række tilsvarende værktøjer der kan mere, søg med google og se hvad du kan finde, kig efter mulighederne for at anvende SSL og anden form for kryptering af forbindelserne.

7. Endelig skal du tilbage til google og bruge noget af det du har har prøvet. Søg f.eks. på Hak5's sider og se om du kan finde en episode hvor NetCat bruges af Mubix og Snubs eller kig forbi vimeo, youtube, DefCon eller Blackhat.

Som du måske har opdaget bliver oplysningerne mindre og mindre præcise og med færre hints og hjælp. Dette sker selvfølgelig for at tvinge dig ud i selv at kunne finde informationerne, det får du nemlig brug for når du løber ind i uforudsede ting eller skal lære dig nye teknikker. Dette betyder selvfølgelig ikke at du står helt uden hjælp.

Disse netcat øvelser er meget vigtige, for du skal bruge netcat i de fremtidige hacks jeg planlægger at skrive om.

Du er stadig velkommen til at kontakte mig via mail på kim@bufferzone.dk. Skriv til mig, fortæl mig hvad du har prøvet, giv mig links til de sider du har søgt hjælp på og beskriv præcist hvad det er du vil. Husk også at medtage snifs der viser hvad du har sniffet, de kommandoer du har prøvet, gerne screen dumps og andre relevante oplysninger. Du vil opdage at hackerne har meget lidt tålmodighed med folk der ikke prøver selv først og som ikke viser at de griber problematikkerne systematisks an. Hvis du derimod viser at du gerne vil lære og ikke har noget imod at læse og prøve først, så vil du ofte kunne få hjælp at de fleste.