Dia 29: naar nieuwe windows upgraden

Dia 31: kan inloggen met een null sessie, geen gebruikersnaam of wachtwoord

Dia 32: Server Message Block disabled, wilt zeggen dat packets niet gesigned worden en de ontvanger kan dus niet nagaan wie het gestuurd heeft en van waar het komt. Als dit wel ge-enabled zou worden kan men voorkomen dat er aan packets geprutst is geweest en man-in-the-middle attacks.

Dia 33: De remote host maakt gebruik van een netwerk stuurprogramma dat ethernet frames opvult met verschillende gegevens die kunnen variëren van packet tot packet. Ook bekend als etherleak, kan dit een potentiële aanvaller in staat steller om gevoelige data te verzamelen van de host op de voorwaarde dat hij zich op hetzelfde fysieke subnet bevindt als de host.

Dia 34: Er zit een bug in de random number generator die de remote x509 certificaat (certificaat dat nagaat dat een public key bij iemand hoort) genereert. Dit probleem ontstaat door een Debian packager die bijna alle bronnen van entropie verwijdert. Hierdoor kan een mogelijke aanvaller zeer gemakkelijk aan het deel van de remote sleutel komen die eigenlijk privé moet blijven. Hiermee kan hij dan de remote sessie ontcijferen of een "man in the middle attack" uitvoeren.

Dia 35: De rexecd service zorgt ervoor dat gebruikers van een bepaald netwerk commands remotely can uitvoeren. In dit geval voorziet rexecd geen goede authenticatie van de gebruiker

Dia 36: Een shell is aan het "luisteren" op de remote port en kan dus misbruikt worden

Dia 37: OS niet meer ondersteund

Dia 38: wachtwoord van vnc server is password

Dia 40: Als deze vulnerability geexploit wordt kan deze de server service doen stoppen door een speciaal netwerk bericht te sturen naar een systeem die de server service runt

Dia 41: Als de exploit lukt kan het de remote ongeverifiëerde aanvaller er tot in staat stellen om code uit te voeren, een denial of service uit te voeren of langs het authenticatie mechanisme te geraken via brute force technieken

Dia 42: Door te connecteren op poort 135 en juiste queries uit te voeren kan de aanvaller meer informatie bemachtigen over de remote host

Dia 44: X11 is een client-server protocol en heeft de leiding over het scherm. De clients connecteren ermee en sturen verschillende requests zoals het showen van een window of menu. De server stuurt events terug naar de client, zoals een muisklik, of een toetsaanslag. Een X server die niet fatsoenlijk is geconfigureerd accepteerd van eender welke client. Dit stelt een aanvaller er tot in staat om te connecteren met de X server en toetsaanslagen te recorden.

Dia 45: Als de exploit lukt, kan er willekeurige code uitgevoerd worden, of een dos uitgevoerd worden.

Dia 46: Een backdoor is geïnstalleerd op de remote host => code uitvoeren door aanvaller

Dia 47: distcc 2.x stelt remote aanvallers er tot in staat om willekeurige commands uit te voeren door de server zonder authorizatie checks

Dia 49: misbruikt een stack buffer overflow in de RPCSS service en kan de aanvaller er tot in staat stellen code uit te voeren met system privileges

Dia 50: zelfde als hierboven

Dia 52: ook backdoor

Dia 53: foute configuratie in symantec messaging gateway, wachtwoord is bekend en kan inloggen als support en kan gebruikt worden om op de SSH in te loggen

Dia 54: CakePHP is een populair PHP framework om web applicaties te bouwen. De versie 1.3.5 en eerder is kwetsbaar voor een attack die uitgevoerd kan worden om ongeauthorizeerde aanvallers code te laten uitvoeren die kwetsbaar is met de permissies van de webserver zelf

Dia 55: bot die geexploiteerd word en heeft functionaliteiten zoals nmap scanning, tcp, http, sql en udp flooding, kan system logs verwijderen, root access verkrijgen en vnc scanning

Dia 56: module die zich voordoet als legitiem server en een zogezegde nieuwe update aanbied, maar zit een payload in