پیش گزارش ۲

کیان پورآذر. ۴۰۱۳۱۴۰۱

سوال اول:

ﺑﺮﻧﺎﻣـــﻪ Wireshark ﺗﺤﻠﯿﻞﮐﻨﻨـــﺪه ﭘﺮوﺗﮑـــﻞ و ﺷـــﻨﻮد ﮐﻨﻨـــﺪه ارﺗﺒـــﺎط ﻣﺘﻦﺑـــﺎز ﺑـــﺮ روي ﺳ ﯿﺴﺘﻢﻋﺎﻣﻞﻫﺎي ﺧﺎﻧﻮاده وﯾﻨﺪوز و ﻟﯿﻨﻮﮐﺲ اﺳ ﺖ ﮐﻪ ﺑﻪ ﺷﻤﺎ اﺟﺎزه ﻣﯽدﻫﯿـﺪ ﺗﺮاﻓﯿـﮏ ﺷـﺒﮑﻪ ﺧـﻮد را ﺗﺤﻠﯿﻞ ﮐﻨﯿﺪ . ﭘﺮوژهي Wireshark در ﺳﺎل 1998 ﺑﺎ ﻧﺎم Ethereal ﺗﻮﺳـﻂ Gerald Combs آﻏـﺎز ﺷـﺪ. اﯾﻦ ﭘﺮوژه در ﺳﺎل 2006ﺑﻪ Wiresharkﺗﻐﯿﯿﺮ ﻧﺎم داد. اﯾﻦ ﻧﺮماﻓﺰار ﺗﻮﺳـﻂ ﭼﻬـﺎرﭼﻮب Qt و ﺑـﺎ زﺑـﺎن ++C/C ﻧﻮﺷﺘﻪ ﺷﺪه اﺳﺖ. اﯾﻦ ﺑﺮﻧﺎﻣﻪ ﻗﺎدر ﺑﻪ ﺗﺤﻠﯿﻞ ﺑﺮﺧﻂ ﺑﯿﺶ از 1000ﭘﺮوﺗﮑـﻞ در ﻧﺴـﺨﻪ 1.10.6 اﺳﺖ. ﻫﻤﭽﻨﯿﻦ ﻗﺎدر ﺑـﻪ ﺧﻮاﻧـﺪن اﻃﻼﻋـﺎت ﺧﺮوﺟـﯽ اﻧـﻮاع ﺑﺮﻧﺎﻣـﻪﻫﺎي ﺷـﻨﻮد و ﺗﺤﻠﯿـﻞ دﯾﮕـﺮ ﻣﺎﻧﻨـﺪ Microsoft Network Monitor ،TCPdump اﺳــﺖ. ﺧﺮوﺟــﯽ اﯾــﻦ ﺑﺮﻧﺎﻣــﻪ ﻣﯽﺗﻮاﻧــﺪ ﺑﻪﺻــﻮرت PostScript،CSV،XML ﯾﺎ Plaintext ﺑﺎﺷﺪ.

سوال دوم:

در ﺳ ﯿﺴﺘﻢﻋﺎﻣﻞ ﺧﺎﻧﻮاده وﯾﻨﺪوز، ﺑﺮﻧﺎﻣـﻪ Wiresharkﺷـﻨﻮد ﺑﺴـﺘﻪﻫﺎ ﺑـﺎ اﺳـﺘﻔﺎده از ﮐﺘﺎﺑﺨﺎﻧـﻪ Winpcapاﻧﺠﺎم ﻣﯽدﻫـﺪ. ﻣﻌﻤـﺎري ﻧﺮماﻓـﺰار Winpcap به این گونه اﺳﺖ که، از دو ﺑﺎﻓﺮ ﯾﮑﯽ در ﺳﻄﺢ ﮐﺮﻧـﻞ و دﯾﮕـﺮي در ﺳﻄﺢ ﮐﺎرﺑﺮ، ﯾﮏ ﻣﺎﺷﯿﻦ ﻓﯿﻠﺘﺮ ﮐﻨﻨﺪه ﮐﻪ ﻓﯿﻠﺘﺮﻫﺎﯾﯽ را ﺑﻪ ﺑﺴﺘﻪﻫﺎ اﻋﻤﺎل ﻣﯽﮐﻨﺪ و ﻫﻤﭽﻨﯿﻦ دو ﻓﺎﯾل wpcap.dll و packet.dll ﮐﻪ اﯾﻨﺘﻔﺮﯾﺲﻫﺎي اﯾﻦ ﺑﺮﻧﺎﻣﻪ را اراﺋﻪ ﻣﯽﮐﻨﻨﺪ ﺗﺸﮑﯿﻞ ﺷﺪه اﺳﺖ. در اﺑﺘﺪا ﮐﺎرﺑﺮ ﻣﯽﺗﻮاﻧﺪ ﻓﯿﻠﺘﺮﻫﺎﯾﯽ را ﻣﺸﺨﺺ ﮐﻨﺪ ﮐﻪ اﯾﻦ ﻓﯿﻠﺘﺮﻫﺎ ﺗﻮﺳـﻂ (NPF) Netgroup Packet Filterﺑﻪ دﺳﺘﻮراﺗﯽ ﺗﺮﺟﻤﻪ ﻣﯽﺷﻮﻧﺪ ﮐﻪ ﺗﻮﺳﻂ ﻓﯿﻠﺘﺮﻫﺎ ﺑـﺮ روي ﺑﺴـﺘﻪﻫﺎ اﻋﻤـﺎل ﻣﯽﺷـﻮﻧﺪ . ﺑـﻪ « درﯾﺎﻓـﺖ ﺷـﻮﻧﺪ UDP ﭘﺮوﺗﮑـﻞ ﯾﮏ ﻓﯿﻠﺘﺮ را ﺑﻪ ﺻـﻮرت »ﺻـﺮﻓﺎ ﺑﺴـﺘﻪﻫﺎي ﻋﻨﻮان ﻣﺜﺎل ﮐﺎرﺑﺮ ﻣﯽﺗﻮاﻧﺪ ﺗﻌﺮﯾﻒ ﮐﻨﺪ. ﺑﺴﺘﻪﻫﺎ ﭘﺲ از اﯾﻨﮑﻪ ﺗﻮﺳﻂ ﮔﺮداﻧﻨﺪه ﺷـﺒﮑﻪ، از واﺳـﻂ ﺷـﺒﮑﻪ ﺧﻮاﻧـﺪه ﺷـﺪﻧﺪ ﺟﻤـﻊآوري ﻣﯽﺷﻮﻧﺪ ؛ ﺑﻨﺎﺑﺮاﯾﻦ ﮐﺎراﯾﯽ Winpcap واﺑﺴﺘﻪ ﺑﻪ ﮔﺮداﻧﻨﺪه ﺷﺒﮑﻪ اﺳﺖ. ﻫﻤﭽﻨﯿﻦ ﻣﺸﺨﺺ اﺳﺖ ﮐﻪ ﺻـﺮﻓﺎ ﯾﮏ ﮐﭙﯽ از ﺑﺴﺘﻪﻫﺎ ﺗﻮﺳﻂ Winpcapدرﯾﺎﻓﺖ ﻣﯽﺷﻮد و ﺑﺴـﺘﻪﻫﺎ ﻫﻢزﻣـﺎن ﻣﯽﺗﻮاﻧﻨـﺪ ﭘﺸـﺘﻪ ﭘﺮوﺗﮑﻠـﯽ ﺳ ﯿﺴﺘﻢﻋﺎﻣﻞ ﮐﻪ در ﺷﮑﻞ ﺑﺎ ﻧﺎم Other protocol stack ﻣﺸﺨﺺ ﺷﺪه اﺳﺖ را ﻃﯽ ﮐﻨﻨﺪ.

سوال سوم:

ﺑﺮﻧﺎﻣﻪ Wireshark دو ﻧﻮع ﻓﯿﻠﺘﺮ ﮐﻨﻨﺪه ﺑﺴﺘﻪ دارد. ﯾﮏ ﻧﻮع Capture Filter اﺳﺖ و ﻧﻮع دﯾﮕـﺮ Capture Filter .Display Filter ﻗﺒﻞ از ﺷﺮوع ﺑﻪ ﺷﻨﻮد ﺑﺴﺘﻪ ﻣﻘﺪاردﻫﯽ ﻣﯽﺷﻮد و در ﺣﻘﯿﻘﺖ ﻫﻤـﺎن ﻓﯿﻠﺘﺮي اﺳﺖ ﮐﻪ ﺗﻮﺳﻂ NPF ﺑﺮ روي ﺑﺴـﺘﻪﻫﺎي درﯾﺎﻓـﺖ ﺷـﺪه از ﮔﺮداﻧﻨـﺪه ﺷـﺒﮑﻪ اﻋﻤـﺎل ﻣﯽﮔـﺮدد؛ ﺑﻨﺎﺑﺮاﯾﻦ اﯾﻦ ﻓﯿﻠﺘﺮ ﺑﺮ ﺟﻤﻊآوري ﺑﺴﺘﻪﻫﺎ ﺗﺎﺛﯿﺮ ﻣﯽﮔﺬارد. در ﻣﻘﺎﺑﻞ Display Filter ﺻﺮﻓﺎ ﻣﺮﺑﻮط ﺑﻪ ﻓﯿﻠﺘﺮ ﮐﺮدن ﺑﺴﺘﻪﻫﺎي ﺟﻤﻊآوري ﺷﺪه اﺳﺖ. ﺑـﺎ اﺳـﺘﻔﺎده از Display Filter ﻣﯽﺗـﻮان ﺗﻌـﺪادي از ﺑﺴـﺘﻪﻫﺎي ﺟﻤﻊآوري ﺷﺪه را ﻣﺸﺨﺺ ﮐﺮد ﮐﻪ در ﭘﻨﺠﺮه Wiresharkﻧﻤﺎﯾﺶ داده ﺷﻮﻧﺪ.