CT01

Quan sát thấy hàng loạt yêu cầu xác thực kerberos, chứng tỏ attacker đăng brute-force bằng cách này để tìm xem tài khoản hợp lệ bên trong hệ thống.

No.	Time	Source	Destination	Protocol	Length	Value	Info
13	5.003653	10.10.5.100	10.10.5.1	KRB5	267		AS-REQ
21	5.014016	10.10.5.100	10.10.5.1	KRB5	347		AS-REQ
92	15.436492	10.10.5.100	10.10.5.1	KRB5	280		AS-REQ
100	15.438179	10.10.5.100	10.10.5.1	KRB5	360		AS-REQ
9207	360.778271	10.10.5.102	10.10.5.1	KRB5	171		AS-REQ
9756	408.524932	10.10.5.102	10.10.5.1	KRB5	243		AS-REQ
9765	408.529647	10.10.5.102	10.10.5.1	KRB5	244		AS-REQ
9774	408.534122	10.10.5.102	10.10.5.1	KRB5	243		AS-REQ
9783	408.540228	10.10.5.102	10.10.5.1	KRB5	241		AS-REQ
9794	408.566236	10.10.5.102	10.10.5.1	KRB5	244		AS-REQ
9803	408.568436	10.10.5.102	10.10.5.1	KRB5	246		AS-REQ
9812	408.572024	10.10.5.102	10.10.5.1	KRB5	315		AS-REQ
9821	408.574375	10.10.5.102	10.10.5.1	KRB5	243		AS-REQ
9830	408.575781	10.10.5.102	10.10.5.1	KRB5	244		AS-REQ
9839	408.577146	10.10.5.102	10.10.5.1	KRB5	246		AS-REQ
9848	408.578424	10.10.5.102	10.10.5.1	KRB5	245		AS-REQ
9857	408.579671	10.10.5.102	10.10.5.1	KRB5	244		AS-REQ
9866	408.583323	10.10.5.102	10.10.5.1	KRB5	243		AS-REQ
9875	408.591111	10.10.5.102	10.10.5.1	KRB5	244		AS-REQ
9884	408.594735	10.10.5.102	10.10.5.1	KRB5	244		AS-REQ
9893	408.600653	10.10.5.102	10.10.5.1	KRB5	243		AS-REQ
9902	408.605994	10.10.5.102	10.10.5.1	KRB5	242		AS-REQ
9911	408.609725	10.10.5.102	10.10.5.1	KRB5	245		AS-REQ
9920	408.613036	10.10.5.102	10.10.5.1	KRB5	243		AS-REQ
9929	408.619246	10.10.5.102	10.10.5.1	KRB5	313		AS-REQ

Từ dữ kiện trên ta xác định được IP của attacker là **10.10.5.102**

Quan sát 2 loại kết quả trả về:

14173	411.093105	10.10.5.1	10.10.5.102	KRB5	148		KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
14182	411.098376	10.10.5.1	10.10.5.102	KRB5	148		KRB Error: KRB5KRB_ERR_GENERIC
10766	409.124218	10.10.5.1	10.10.5.102	KRB5	237	LAB.LOCALanhtt203	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED

+ Nếu mã trả về lỗi PREAUTH_REQUIRED nghĩa là tài khoản có trên hệ thống

+ Ngược lại các mã khác thì tài khoản không tồn tại.

9804	408.568696	10.10.5.1	10.10.5.102	KRB5	238	LAB.LOCALcuongnc16	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
9921	408.613442	10.10.5.1	10.10.5.102	KRB5	236	LAB.LOCALhainh45	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
10613	409.022316	10.10.5.1	10.10.5.102	KRB5	237	LAB.LOCALthaint10	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
10766	409.124218	10.10.5.1	10.10.5.102	KRB5	237	LAB.LOCALanhtt203	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
10856	409.182828	10.10.5.1	10.10.5.102	KRB5	236	LAB.LOCALkhoaha4	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
11072	409.320456	10.10.5.1	10.10.5.102	KRB5	234	LAB.LOCALminhdn	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
12142	409.991810	10.10.5.1	10.10.5.102	KRB5	237	LAB.LOCALhiepdt10	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
12160	410.006410	10.10.5.1	10.10.5.102	KRB5	237	LAB.LOCALthiennc6	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED

Ngoài ra, ta xét đến trường hợp đăng nhập thành công bằng kiểm tra AS-REP.

	Time	Source	Destination	Protocol	Length	Value	salt	Info
10541	408.984330	10.10.5.1	10.10.5.102	KRB5	1584		LAB.LOCALhuycd1	AS-REP

Ở đây ta thấy có tài khoản của huycd1 xác thực thành công. Như vậy ta có tổng cộng 9 tài khoản.