# Capture The Flag (CTF)

شاید شما نیز اخیرا عباراتی نظیر contest, Wargame , یا CTF را شنیده باشید ؟ CTFعبارتی که به تازگی در جوامع امنیتی در ایران شنیده می شود. CTF چیست ؟

در ادبیات امنیت فضای تبادل اطلاعات، اصطلاح «هکر» به فردی اطلاق می‌شود که با یافتن نقطه ضعف امنيتي در يك سيستم، قادر خواهد بود به آن نفوذ کند.هکرها به دلایل گوناگوني دست به این کار مي‌زنند؛ سود مالي، اعتراض و یا حتي براي کنجکاوي و هیجان.هکرها از نظر رفتاري در دسته‌هاي مختلفي جاي دارند.برخي که به «کلاه سیاه» معروفند، کساني هستند که به دلایل بدخواهانه مانند سود شخصي، به صورت مخفیانه اقدام به انجام کارهاي خرابکارانه مثل دزدي اطلاعات و یا از کارانداختن سرویس نموده و امنیت کامپیوتري شخص یا شرکتي را به خطر مي‌اندازند.این دسته از هکرها، همان کساني هستند که بر اساس قانون و در اذهان عمومي، مجرم شناخته مي‌شوند.در مقابل، دسته دیگري از هکرها که به »کلاه سفیدها» مشهور هستند، به صورت قانوني و با داشتن مجوز از سوي صاحبان صنایع و شرکت‌ها اقدام به بررسي نقاط ضعف امنیتي در سیستم‌ها و شبکه‌هاي کامپیوتري مي‌نمایند تا شرکت‌ها و سازمان‌ها بتوانند با برطرف کردن این مشکلات میزان خطر نفوذ هکرهاي کلاه سیاه را کاهش دهند.به عبارتي براي آنکه بتوانید مانع حمله مهاجمان بدخواه بشوید، باید از افراد متخصص در همان زمینه کمك بگیرید.

براي به چالش کشیدن توانایي‌هاي هکرهاي کلاه سفید، همچنین تقویت و به اشتراك گذاري دانش آنها، سالانه کنفرانس‌ها، کارگاه‌هاي آموزشي و مسابقات مختلفي مانند CTF در سطح دانشگاهي و نیمه حرفه‌اي با حمایت شرکت‌هاي معتبر و بزرگ با شرکت هکرهایي از سراسر دنیا برگزار مي‌شود. CTFیا مسابقه گرفتن پرچم، يك مانور شبیه‌سازي شده در فضاي سایبري است که در آن هکرها به مقابله با یکدیگر می‌پردازند.

در این مسابقه هر تیم تلاش مي‌کند از مواضع از پیش تعیین شده در رایانه یا شبکه اختصاصي‌اش دفاع کند. در عین حال به طور همزمان سعي مي‌کند که با گذر از سد امنیتي سایر تیم‌ها، پرچم خود را در سیستم‌هاي آنها نصب کند.در حال حاضر، مسابقات CTF به عنوان يك مسابقه علمي با هدف ایجاد تجربه مشترك در امن کردن سیستم‌ها و اشتراك دانش نفوذ و انجام حملاتی است که در دنیاي واقعي قابل اجرا هستند.

اولین مسابقه CTF در کنفرانس DEFCON در سال ۲۰۰۳ توسط دانشگاه کالیفرنیا سانتا باربارا برگزار شد. در این کنفرانس، متخصصین امنیت شبکه و رمزنگاري در کنار هکرها، آخرین دستاوردهایشان را در زمینه امنیت شبکه به اشتراك مي‌گذارند.از عمده‌ترین مسابقات CTF که در حال حاضر سالانه توسط دانشگاه‌هاي دنیا برگزار مي‌گردد، مي‌توان به موارد زیر اشاره کرد:

مسابقه CTF در کنفرانس DEFCON ، ICTF در دانشگاه کالیفرنیا سانتا باربارا آمریکا و مسابقه CSAW در موسسه پلی‌تکنیک دانشگاه نیویورک آمریکا.(NYU-Poly)

قالب برگزاري مسابقات با یکدیگر متفاوت است؛ به عنوان مثال چالش‌هاي مبتني بر حمله، و یا دفاع و حمله به صورت همزمان.به طور کلي در مسابقات CTF جنبه‌های مختلفي از دانش امنیت تیم‌هاي شرکت کننده سنجیده مي‌شود؛ مهندسي معکوس (Reverse-engineering)، شنود شبکه (network sniffing)، تحلیل پروتکل، مدیریت شبکه، حملات تحت وب، برنامه‌نویسي و تحلیل رمز (cryptanalysis) از جمله توانایي‌هایي هستند که در این دسته از مسابقات مورد ارزیابی قرار می‌گیرند و شرکت‌کنندگان براي

شرکت در این رقابت‌ها بدان نیازمند هستند. که رشته های مورد ارزیابی در ادامه کامل توضیح داده می شود.

با وجود اینکه اجرای چنین طرح‌هایی در دنیا سابقه‌ای نزدیك به یک دهه دارد، ولی هنوز در کشور ما رواج چنداني پیدا نکرده است.شاید به عنوان تنها نمونه عملي آن بتوان به برگزاري رقابت‌هاي نفوذ و دفاع در فضاي مجازي که در تابستان سال 1390 توسط مرکز آپا(مرکز آگاهی‌رسانی، پشتیبانی و امداد در افتا) دانشگاه صنعتي شریف برگزار شد، اشاره کرد.دومین دوره این مسابقات نیز در خرداد ماه سال 1391 در دانشگاه صنعتی شریف با هدف محک‌زنی گروه‌ها و افراد متخصص حوزه آزمون نفوذ و ارزیابی امنیتی و ارتقای دانش تخصصی این افراد در این حوزه توسط مرکز آپا این دانشگاه برگزار گردید. در هر حال برگزاری این دسته از مسابقات تخصصی می‌تواند انگیزش قابل توجهی را در دانش‌آموختگان و متخصصین حوزه امنیت فضای تبادل اطلاعات در گرایش به این موضوعات و استفاده از توان تخصصی حاصله در ارزیابی امنیتی سیستم‌های ارتباطی و اطلاعاتی و ارتقای سطح امنیتی آنها در کشور ایجاد نماید.

که شاخه های مورد نظر به شرح ذیل می باشد.

1- Trivia
2- Cryptography
3- Forensics
4- reverse engineering
5- Web application attack
6- Secure Coding
7- Programing
8- Log Analys
9- Network Pen test
10- Exploitnig

توضیح کوتاه در مورد شاخه های ذکر شده :

1- Trivia : عمدتا در این قسمت سوالاتی در زمینه های امنیت شبکه مطرح می گرددکه در مورد روش های bypass کردن protection ها می باشد که جهت پیدا کردن جواب سوالات باید دانش نسبی در مورد موضوع مطرح شده داشته باشید تا بتوانید با سرچ کردن این موضوع را از اینترنت پیدانمایید.
2- Cryptography : در این قسمت سوالاتی در زمینه الگوریتم های رمز نگاری و روشهای رمز گشایی مطرح می گردد که برخی از سوالات ترکیب چندین رمز نگاری می باشد که تیم شرکت کننده باید با دانش کافی این رمز نگاری ها را کشف کرده و اقدام به رمز گشایی نماید.
3- Forensics : در این قسمت تیم شرکت کننده باید اقدام به کشف جرم نماید و روال به این صورت است که سیستم هک شده ای در اختیارتیم قرار می دهند که باید از طریق سیستم هک شده اطلاعاتی از شخص نفوذ گر پیدا کنند.
4- reverse engineering : در این قسمت مهندسی معکوس توسط تیم های شرکت کننده بر روی فایل ها ی ارایه شده توسط تیم برگزاری انجام می گیرد که عمدتا از این روش برای پی بردن به نحوه عملکرد یک ویروس استفاده می شود.
5- Web application attack : در این قسمت تیم شرکت کننده باید با انواع حملات رایج تحت وب بتوانند چالش های وب را حل کنند .

6- Secure Coding : در این قسمت از تیم شرکت کننده خواسته می شود تا سیستم امنی برا طراحی نمایند تا در مقابل حملات ایمن باشد.
7- Programing : در این قسمت سوالاتی مطرح می شود که بیشتر جنبه تست هوش دارد و برای راحتی و سریع تر رسیدن به جواب سوال باید برنامه ای طراحی شود .
8- log analysis : در این قسمت تیم تحلیل گر با بررسی مستندات ارایه شده از طرف کمیته فنی برگزارکننده مسابقات و با بررسی log فایل ها اقدام به تشخیص راه نفوذ می نمایند.
9- Network Pen test : در این قسمت تیم شرکت کننده باید با انواع روشهای رایج شبکه تحت بررسی را موردبررسی امنیتی قرار دهد . و سپس راه نفوذ را پیدا کند .
10- Exploitnig : در این قسمت باید با نوشتن کدهایی مخرب سیستم آسیب پذیر را exploit کرده و سپس سیستم آسیب پذیر را در اختیار خود بگیرند.

از مهمترین برگزار کنندگان مسابقات contest می توان به BlackHat و Defcon اشاره نمود. که در مرحله مقدماتی و نهایی برگزار می گردد که مرحله مقدماتی و نهایی در شاخه های ذکر شده در 2 سطح مقدماتی و پیشرفته برگزار می گردد که عموما مرحله مقدماتی به صورت غیرحضوری و اینترنتی برگزار می گردد و از میان تیم های شرکت کنندگان تیم هایی که حد نساب امتیاز را کسب نمایند به عنوان تیم های برگزار کننده به مرحله دوم راه می یابند . که در مرحله دوم نیز در سطح پیشرفته تمامی شاخه مربوطه دوباره توسط شرکت کنندگان طی 1 الی 2 روز مورد بررسی قرار می گیرد که در نهایت به تیم های برنده هدایای اهدا می گردد و عمدتا 2 روز دیگر نیز برای بررسی جذیدترین روش های ایمن سازی و نفوذ گری مقالاتی ارایه می گردد که از بهترین مزایای این مسابقات 2 -3 روز آخر می باشد که مقالاتی که ارایه می شود درمورد جدیدترین روش های هکینگ می باشد که از بهترین و معتبرترین مقالات می توان از مقالاتی که در blackhat ودر سطح پایین تر در Defcon نام برد.

از آنجایی مسابقات BlackHat و Defcon از اهمیت ویژه ای برخورد می باشند لذا برای آماده سازی این مسابقات ، مسابقات دیگری از طرف تیم های دیگر نیز برگزار میگردد. که می توان از وب سایت های زیر نام برد.

http://hackinglab.com

http://nullcon.net

http://strip.com

http://captf.com

http://ictf.cs.ucsb.edu/

https://csawctf.poly.edu/

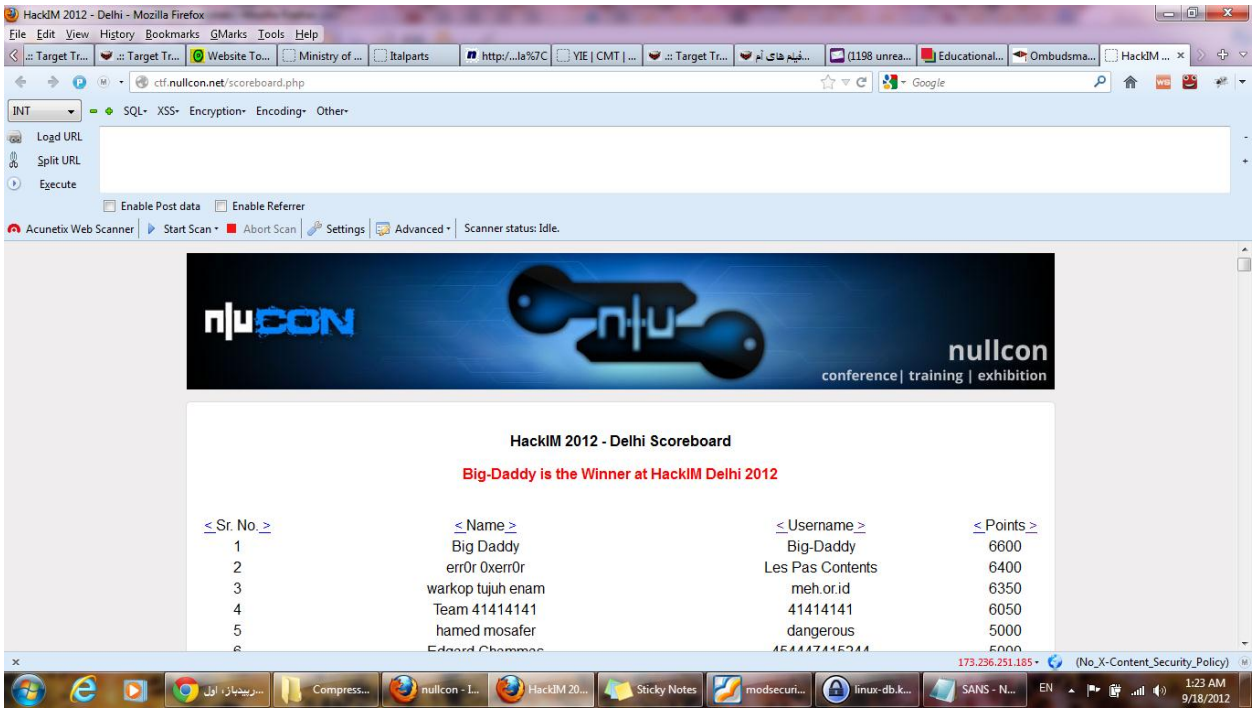
http://www.smashthestack.org/

http://www.intruded.net/

که آخرین CTF که جدیدا در سطح جهان برگزار گردیده است و بین 500 تیم برگزار شد. CTF مربوط به nullcon بوده است که در این بین این حقیربا نام hamed mosafer و با نام کاربری dangerous در این مسابقات شرکت کردم و بین 500 تیم شرکت کننده با امتیاز 5000 از 6500 امتیاز مقام پنجم را کسب نمودام که مستندات این موضوع در لینک زیر مشخص می باشد.

http://ctf.nullcon.net/scoreboard.php

که عکس از صفحه مربوطه نیز در ادامه ارسال شده است.




با توجه به حملات سایبری که طی سال های پیشین به وب سایت های دولتی شده است و همه روزه نیز شاهدحملات جدید در این زمینه به بدنه دولت هستیم همه این حملات حاکی از آن است که جنگ جدیدی به نام جنگ سایبری در حال شکل گیری می باشد . و نباید این نکته را فراموش کنیم که دشمنان هر روز در حال آموزش و همچنین استخدام نیرو های زبرده در این زمینه هستند . لذا با توجه به جنگ سایبری موجود لازم است که به افرادی که دارای جنین تخصص هایی هستند توجه بیشتری شود تا بتوان از این افراد جهت دفاع در فضای سایبری استفاده نمود. زیرا با وجود افراد متخصص کمتر شاهد اتفاقاتی نظیر ورود ویروس هایی نظیر stuxnet , Flame به شبکه های صنعتی دولت خواهیم بود.