National Datacenter

DCERT

DATACENTER EMERGENCY RESPONSE TEAM

# ХАЛДЛАГАД ХАРИУ ҮЙЛДЭЛ ҮЗҮҮЛЭХ БАГ

# Тугийг эзлэх (Capture the flag /CTF/) тэмцээнд оролцохоос өмнө мэдэх ёстой 10 асуулт


CTF тэмцээнд оролцох нь хувь хүний аюулгүй байдлын мэдлэг чадварыг дээшлүүлж, компьютерийн шинжлэх ухааны хүрээнд шинэ авьяасаа тодорхойлоход тусалдаг. Оролцогчдод ямар төрлийн сорилтуудад бэлтгэх хэрэгтэй, хэрхэн уралдаанд оролцох болон бусад ложистикийн талаар авч үзье.

## CTF гэж юу вэ?

Тугийг эзлэх /CTF/ уралдаан нь дэлхийн улс орнуудад бодит орчинд хэрхэн хакердах,мэдээллийн технологийг ашиглах талаар заах сурталчилах хийсвэр арга юм. CTF нь хэдэн арван жилийн турш зохиогдсоор ирсэн бөгөөд хамгийн удаан үргэлжилж байгаа алдартай цуврал тэмцээн нь 1996 онд зохиогдсон Vegas DEFCON шоу байсан ба мянга мянган оролцогчдыг татаж чадсан юм. Түүнээс хойш дэлхийн өнцөг булан бүрт тарж, олон арван онлайн тэмцээнүүд амралтын өдөр бүр зохиогдох болжээ. Түүгээр ч барахгүй ахлах сургуулийн сурагчдад зориулагдсан CTF –үүд ч зохиогдож байна.

Сүүлийн үед олон корпорацийн мэдээллийн технологийн хэлтсүүд өөрсдийн нэрдээр уралдааныг явуулах болсон байна. Эдгээр уралдаануудыг олон хэлбэрээр явуулж болох ба өөрийн гэсэн тоглоомын талбарыг бүтээх шаардлагатай, үйл ажиллагааг амжилттай явуулах болон тэмцээнд амжилттай оролцохоос өмнө хэд хэдэн асуултад хариулах хэрэгтэй.

Ингээд дараах 10 асуултад хариулж эхэлье.

### 1. Та шинэ ажилтнуудыг элсүүлэхийн тулд CTF –ийг ашиглах уу?

Уралдааныг эхлүүлэх олон шалтгаан байдаг. Кибер аюул заналхийллийн менежментийн ерөнхий боловсрол эзэмшүүлэх эсвэл уралдааны баг бүрдүүлэх гэх мэт. Сонирхолтой зорилтуудын нэг нь танай байгууллагын доторх болон гаднах кибер аюулгүй байдлын мэргэжилтнүүдийн шинэ авьяасыг таних, илрүүлэх явдал юм. Жишээ нь Агаарын цэргийн хүчин өөрийн багаа бүрдүүлэхийн тулд CTF төрлийн шалгаруулалтыг ашиглаж байсан.

Асуудлын нэг хэсэг нь мэдээллийн аюулгүй байдлын ажлын байрны сул орон тоо юм. Атланта мужийн хэд хэдэн уралдааныг зохион байгуулахад гар бие оролцсон “Compliance Point of Duluth”, “GA”, “a security VAR” –ийн ахлах дэд захирал Greg Sparrow хэлэхдээ “Компани болон үйлдвэрийн газруудад цахим аюулгүй байдлын мэргэжилтэн, ажилчидын шаардлага нь ихэвчлэн нийлүүлэлтээсээ давж гардаг тул энэ төрлийн ажлыг хийх чадвартай хүмүүсийг олж таних маш сайн арга бол CTF юм.” гэж хэлжээ.

“Бодит ертөнцөд таны сурах зүйл хязгаартай. CTF –г явуулах нь кибер аюул заналхийллийг таних, шийдвэрлэхэд суралцах талдээр илүү бодит ач холбогдолтой байдаг. Зөвхөн онолын тухай бичсэн номыг унших нь хангалтгүй юм. “CTF нь эрх зүйн хувьд хамааралгүйгээр бодит ертөнцөд өөрийгөө сорих хамгийн том боломж юм” гэж Sparrow хэлжээ.

Нэгэн жирийн IT менежер хэлэхдээ “Бид CTF –ээ дотоод ажилчдад зориулсан аюулгүй байдлын мэдлэг олгох үйл ажиллагаа гэж харж байгаа. Бидний 2 өдрийн үйл ажиллагаа нь 2 хэсэгт хуваагдаж явагддаг: Өглөөний боловсролын хурал дээр бид хакердах арга барилын талаар сургалт зохион байгуулдаг, үдээс хойш хуралдаж, жижиг бүлгүүдтэйгээ өрсөлддөг.” гэжээ. Тэд энэ үйл ажиллагааг ашигтай гэж үзэж байгаа учир нь “Аюулгүй байдлын ерөнхий байр суурийг байгууллагын хэмжээнд бэхжүүлдэг арга барил юм.” гэжээ.

## 2. Ямар насны хүмүүс болон туршлагын түвшинг онилж тэмцээн явагддаг вэ?

CTF –үүдийг аль ч насны хүмүүст зориулан явуулж болно. Өмнө дурдсанчлан ахлах сургуулийн сурагчдын хооронд ч явуулж болно. Уралдаан зохиогдохдоо ямар оролцогчдыг хооронд нь өрсөлдүүлэхэд тохиромжтой болохыг харгалзан үзэж ангилдаг. Хэрвээ тэмцээн зохиож буй компани тойрон хүрээлж буй дотоодын хүмүүсийг тэмцээнд татан оролцуулхыг хүсвэл уралдаант шалгаруулалтын урьдчилан таамаглах асуултуудыг тавих, хэд хэдэн урьдчилсан шалгуурын асуултуудыг тавьж боломжит оролцогчдын хүрээ, мэдлэгийн хүрээг тодорхойлох боломжтой юм.

- Мэргэжилтнүүд
- Оюутнууд
- 10 жилийн сурагчид

Монгол улсын хувьд “Үндэсний дата төв”, “MNCERT”, “Төрийн мэдээлэл холбооны газар” -уудаас жил бүр “Харуул Занги” тэмцээнийг уламжлал болгон зохион байгуулдаг. Тэмцээний хувьд насанд хүрэгчдэд буюу үндсэн “Харуул Занги” тэмцээн, Ахлах ангийн сурагчдын дунд “Харуул Занги U18” гэсэн ангилал -тайгаар жил бүр зохион байгуулагдаж байна.

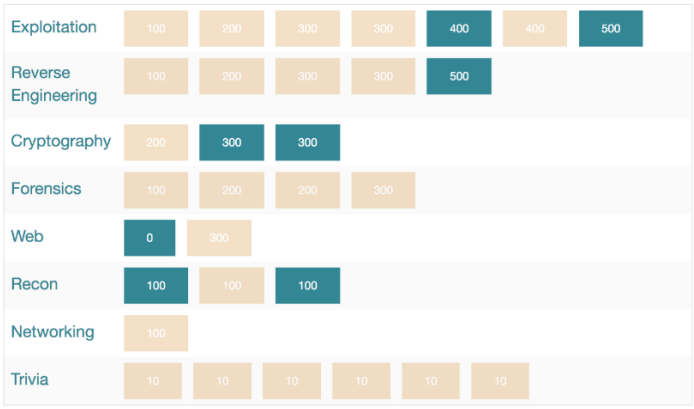
### 3. CTF –д бэлэн системийг тэмцээнд хэрэглэдэг үү эсвэл шинээр систем бэлдэн тохируулан хөгжүүлдэг үү?

Бэлэн загварчлал нь аюулгүй байдлын мэргэжлийн баг бэлтгэсэн CTF төрлийн дасгал хийхэд зориулагдсан тусгай систем юм. Энэ систем нь аюулгүй байдлын хувьд нийтлэг аюул заналхийллүүдийн эсрэг урьдчилсан бүтээсэн мөн нээлттэй эхийн програм тул зохион байгуулж буй ямарч газар өөрийн уралдаанд ашиглах боломжтой.

Бэлэн Платформ: github.com/We5ter/Awesome-Platforms/blob/master/CTF-Platforms.md

### 4. Ямар ангиллын асуултуудыг хэрэглэх вэ?

Ихэнх CTF –үүд уралдааны асуултуудаа хэд хэдэн төрлийн ангиллаас хольж бэлддэг. Жишээ нь: Стеганографи (Stegnograph), Криптографи (Cryptography), Гар утасны үйлдлийн систем (OS), Аппликейшн-д тусгайлсан зориулсан код (web, email, file sharing), Урвуу инженерчлэл(Reverse Engineering), Хайгуул илрүүлэлт (Forensic), Програмчлал(Programming), Системд нэвтрэх шалгалт(Penetration testing) , Сүлжээний сорилт(Networking) гэх мэт. Та ямар төрлөөр илүү гүнзгий судалж байгаагаас шалтгаалан зөвхөн хоёроос гурван ангилалд анхаарлаа хандуулж болно.




### 5. Ямар төрлийн CTF уралдаанууд зохиогддог вэ?

Ерөнхийдөө хоёр төрлийн уралдаан байдаг: Jeopardy болон Attack and Defence сорилтууд. Эхнийх нь телевизийн шоутай төстэй, асуултуудыг янз бүрийн ангиллаар бэлтгэсэн байдаг. Хоёр дахь нь илүү сонгодог хэлбэр бөгөөд энэ нь илүү их хүмүүсийн сонирхлыг татдаг. Хоёр групп оролцож нэг нь сүлжээ болон системийг хамгаалах /Цэнхэр баг/ нөгөө нь халдагчид болдог /Улаан баг/. Хоёр тал тодорхой хугацааны дараа байраа сольдог тул хүн бүр хоёр төрлөөр оролдож үзэх боломжтой болдог. Мөн зарим тэмцээн нь хоёр төрлийг хольж уралдааныг явуулдаг.

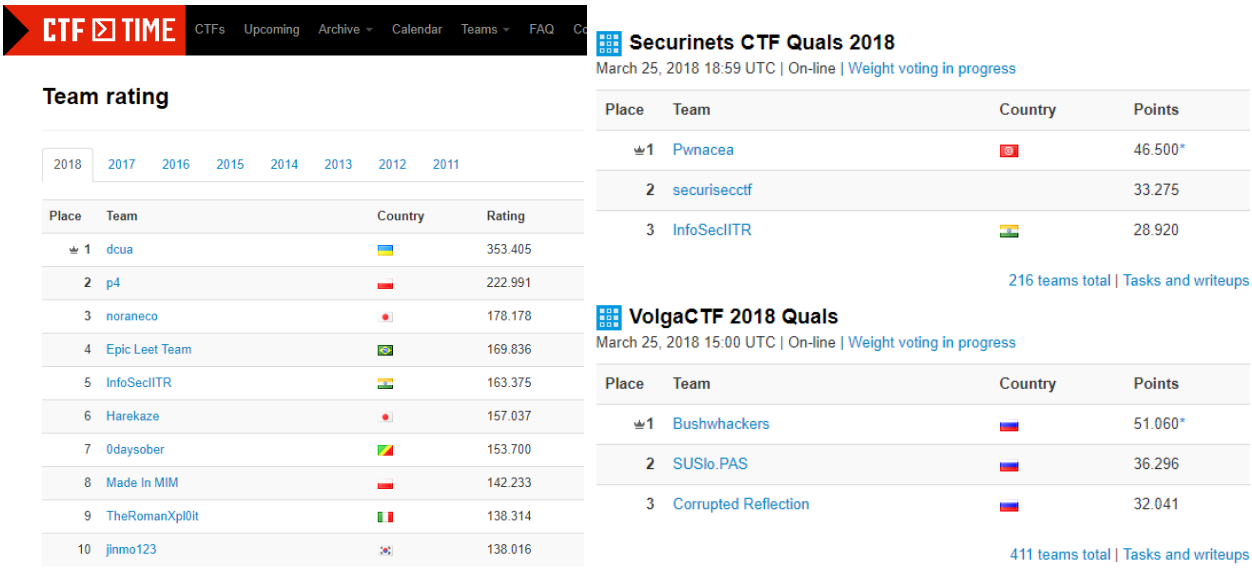
### 6. Ямар шагнал урамшуулал олгох, хэдэн цаг үргэжлэх вэ?

Тэмцээний загварыг гаргахдаа шагнал урамшуулал болон тэмцээний үргэлжлэх хугацааны мэдээллийг тодорхой нарийн гаргасан байдаг. Ихэвчлэн тэмцээний эхний 3 байр ямар нэгэн шагналын сантай байдаг.

Олон улсын томоохон тэмцээнүүд ихэвчлэн 3000-5000$ орчим шагналын санг зарлаж тэмцээнийг илүү сонирхолтой, хамрах хүрээ ихтэй болгодог.

## 7. Олон нийтэд нээлттэй болдог уу?

Зарим CTF нь зохион байгуулалттай тусгай орчинд бусад өрсөлдөгч нартайгаа тодорхой нэг газар байрлан олон нийтэд нээлттэйгээр зохион байгуулагддаг. Харин зарим нь зөвхөн онлайнаар вэб хөтөч болон өөрсдийн программуудыг ашиглан оролцдог. Мөн зөвхөн урилга өгч байгууллага болон багуудыг оролцуулж хаалттайгаар зохион байгуулагддаг. Харин та өөрт хамгийн тохиромжтойг нь сонгох хэрэгтэй.




## 8. Та сорилтын асуултуудад хэрхэн бэлдэх вэ?

Асуултууд болон сорилтуудад бэлдэх нь их цаг хугацаа, өргөн хүрээний мэдлэг шаардсан байдаг учир олон төрлийн бодлогийг өмнө нь харж туршсан байх нь илүү давуу тал болдог. “Louis” хотын “Fontbonne” их сургуулийн компьютерийн шинжлэх ухааны профессор Guanyu Tian нь ахлах сургуулийн сурагчдын дунд CTF зохион байгуулж бакалаврын зэрэг олгох хөтөлбөрт элсүүлсэн байна. Оролцсон сурагчид нь даалгаварын ихэнхийг эхний 2 цагт хийсэн нь гайхалтай байсан бөгөөд өрсөлдөөний үргэлжлүүлхийн тулд нэмэлт сорилт асуултууд хэрэгтэй болсон гэдэг.

Танд хэрэгтэй “Tool” -үүдийн жагсаалт: https://github.com/apsdehal/awesome-ctf

### 9. Та үнэлгээний ямар систем ашиглах вэ?

Зохион байгуулагчдад тулгардаг нэг асуудал бол оролцогчдыг хэрхэн цаг тухайд нь үнэлэх, асуулт болон сорилтуудыг шийдвэрлэж буй явцыг хянах явдал юм. Оролцогчдыг үнэлгээ дүгнэлтийг дэлгэц дээр бүх хүнд нээлттэйгээр харуулдаг бөгөөд та өөрийн хийсэн даалгавар болон бусад багуудын үйл явцыг ч харах боломжтой.

| | | LITTLE FINGER | THE HALFMAN | THE WALL | | NIGHT WATCHERS | THE KID WOMAN | HODOR | ARYA | YOU KNOW NOTHING | HARPY | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Алангир | 53 | 53 | - | - | 251 | 103 | 103 | 150 | - | - | 713 |
| 2 | 0xff | 51 | - | - | - | 250 | 102 | - | 150 | - | - | 553 |
| 3 | overflow | 52 | 51 | - | - | 252 | - | - | 152 | - | - | 507 |
| 4 | G_C | 50 | - | - | - | - | - | 100 | 150 | 203 | - | 503 |
| 5 | kerber0s | 50 | - | - | - | - | 101 | - | 150 | - | - | 301 |
| 6 | ymoment | 50 | - | - | - | - | - | 100 | 151 | - | - | 301 |
| 7 | B33 | - | - | - | - | 253 | - | - | - | - | - | 253 |
| 8 | Hunting Party | - | - | - | - | - | - | 102 | 150 | - | - | 252 |
| 9 | konoha | - | 52 | - | - | - | - | - | 153 | - | - | 205 |
| 10 | team1 | 50 | - | - | - | - | - | 101 | - | - | - | 151 |

### 10. Тэмцээн зохион байгуулах багаа хэрхэн бүрдүүлэх вэ?

Тэмцээнд оролцохыг зорьж буй багийн хувьд олон төрлийн өөр өөр мэдлэгтэй мэргэжилтнүүд хэрэгтэй. Өмнөх хэлсэнчлэн олон төрлийн мэдлэг шаардсан даалгаврууд байх тул багийн гишүүд ялгаатай нарийн мэргэжлээр мэргэшсэн байх нь чухал юм.

Холбоосууд:

http://www.haruulzangi.mn/

https://www.datacenter.gov.mn/

http://mncert.org/

https://dcert.gov.mn/

http://ncsc.gov.mn/

https://ctftime.org/