blackcat 8:43:09 PM

Kulgram pertama dimulai dan pemateri oleh @xathrya

Tolong diam jika sudah dimulai, terimakasih. edited 8:43:19 PM

Satria Ady Pradana 8:44:43 PM

ok, thanks buat udah hadir di kulgram pertama grup ini.
materi kali ini adalah python for cyber security.

salah satu bagian yang paling penting dari IT adalah programming. Baik bagi seorang developer, sysadmin, dan terutama security consultant, programming adalah bahan yang wajib. 8:45:42 PM

nah kali ini kita akan coba membahas penggunaan python yang lebih ditujukan bagi security. Kita gak akan bahas dalam untuk setiap bagian tapi cukup untuk memberikan wawasan bahwa "oh begitu toh". Aku juga gak akan bahas python dari sangat awal dari penjelasan variabel dan tetek bengeknya. Asumsinya adalah kalian tau sedikit soal ngoding 8:47:17 PM

jadi, kenapa python? kenapa nggak ruby ato yang lain? perl mungkin?
jawabannya karena selain terserah saya, python banyak dipakai dan telah memiliki banyak library untuk bidang ini. 8:48:23 PM

beberapa program pun menyematkan (embed) python ke dalam supaya bisa menambah fleksibilitas dan kemampuan si program. Sebut saja IDA, immunity debugger, GDB. Banyak juga aplikasi yang terbuat dari python, misal sqlmap, mitmproxy, scapy, frida, dsb. 8:50:13 PM

dari sekian banyak itu, setidaknya ada beberapa "jurusan" ato bagian pengaplikasiannya. 8:52:04 PM
- exploit development
- reverse engineering
- networking (packet crafting, mitm, injection, dll)
- scraping
- segala macam server.

dsb

nanti akan kuberikan case by case untuk setiap bagian.

tambahan: 8:53:50 PM
- forensic
- system administration

oke, kasus pertama. 8:57:59 PM
misal dalam pentesting, kalian butuh host suatu program, misalnya malware yang akan didownload oleh server korban setelah exploit berhasil. Kita bisa memanfaatkan modul python untuk mengubah sembarang directory menjadi web server.

$ python2 -m SimpleHTTPServer

dia akan listen ke HTTP pada port 8080

bayangkan kalian melakukan sesuatu yang mirip seperti yang metasploit lakukan, tapi dengan cara yang sangat dasar.

Exploit -> berhasil -> download malware -> mlware dieksekusi

ini lebih memperpendek waktu daripada harus nyalain xampp ato sejenisnya. 8:58:40 PM

oke, itu untuk cuman sekedar make. Kalo kita bisa ngoding, kita bisa make mitmproxy buat bikin mitm. Oke kenapa nggak tool kayak burpsuite aja? bedanya dengan mitmproxy kayak apa? dengan python dan mitmproxy kita bisa ngelog traffic yang lewat sama kayak si burp suite. Tapi kita juga bisa secara programmatic mengubah isi request / response tertentu, sesuai yang kita inginkan. 9:07:36 PM

Kasusnya kayak gimana?
misalnya kita tahu bahwa aplikasi traffic bertukar data lewat POST, kita ingin dapatkan isi pada field tertentu, dan menggantinya. Katakanlah lagi transfer duit, maka kita ubah field rekening tujuan. Semudah bikin script

bahkan mitmproxy mendukung proxying untuk tcp polos. Dampaknya apa? misal suatu device terhubung ke router. Dia gak konek ke server via web tapi pake tcp biasa dengan protokol sendiri yang diserialisasi pake teks doang. Di sinilah kita bisa dump itu pake mitmproxy dan analisis protokolnya 9:13:30 PM

oke, itu tadi untuk web. Selanjutnya contoh penggunaan python untuk networking secara umum.
ada library namanya scapy. Scapy bisa kita gunakan untuk manipulasi paket dan mengirimkan paket secara interaktif.
Kenapa kita butuh? 9:16:42 PM

Satria Ady Pradana 9:23:09 PM

ada banyak banget tools buat networking. Ada buat fingerprinting, scanning, sniffing, packet forging (bikin paket), dsb. Tapi kebanyakan mereka cuman spesifik buat 1 hal.

siapa di sini yang hafal kegunaan dari tools ini: wireshark, hping, fping, nmap, amap, unicornscan, xprobe, dnsspoof, ettercap, dsniff, yersinia, dll.

ketika buat hal sederhana sih gampang. Tapi gimana kalo kalian nemu kasus yang unik? Gimana cara gabungin tools yang ada?

Misal. kita punya tools buat ARP cache poisoning, kita punya tools buat bikin paket double 802.1q encapsulation. Gimana caranya melakukan ARP cache poisoning dengan double 802.1q?

ato misalnya kita punya server, ketika kita kirim ICMP dia ternyata ngeleak sesuatu di padding (disebut etherleaking). Tools biasa gak bisa mendeteksi hal itu karena diprogram untuk mendeteksi

Satria Ady Pradana

siapa di sini yang hafal kegunaan dari tools ini: wireshark, hping, fping, nmap, amap, unicornscan, xprobe, dnsspoof, ettercap, dsniff, yersinia, dll.

ketika buat hal sederhana sih gampang. Tapi gimana kalo kalian nemu kasus yang unik? Gimana cara gabungin tools yang ada?

Misal. kita punya tools buat ARP cache poisoning, kita punya tools buat bikin paket double 802.1q encapsulation. Gimana

802.1q?
caranya melakukan ARP cache poisoning dengan double ato misalnya kita punya server, ketika kita kirim ICMP dia ternyata ngeleak sesuatu di padding (disebut etherleaking). Tools biasa gak bisa mendeteksi hal itu karena diprogram untuk mendeteksi

data dengan format tertentu yang ditentukan oleh pembuat. Lalu? bikin tools baru dong.

kekuatan dari python adalah dia scripting. 9:25:28 PM
bahasa scripting artinya dia fleksibel, bisa diubah-ubah dengan cepat sesuai kebutuhan kita.

dan python sangat erat sekali dengan reverse engineering dan pwning, apalagi exploit development. 9:26:35 PM

bahas reversing gak ada habisnya, jadi kalo mau bahas lebih dalam silahkan ke https://t.me/ReversingID (tg://resolve?domain=ReversingID) 9:27:38 PM

> Telegram
> **Reversing.ID** 
>
> (https://t.me/ReversingID)
>
> **(https://t.me/ReversingID)**
> Grup membahas Reverse Engineering.

tapi akan kukasih contoh bagaimana python kugunakan untuk membantu dalam reversing. 9:28:10 PM

http://pythonarsenal.com/ (http://pythonarsenal.com/) 9:33:30 PM

RE itu berkutat bagaimana cara bedah program dan mempelajarinya. Ada banyak sekali tekniknya. Misal kita ingin menjelajahi isi program dan menanamkan backdoor. Maka kita butuh cara untuk membaca header program, cari tau instruksi awal dimana, tulis kode sendiri di bagian yang kosong di program, dan mengarahkan agar instruksi yang pertama kali dijalankan adalah instruksi kita.

gak bisa dijelasin rinci sebenarnya, agak dalam, tapi akan kuberikan satu teknik yang menarik. 9:34:28 PM

kasusnya seperti ini. 9:36:11 PM

Satria Ady Pradana

kita punya aplikasi di android yang terhubung ke server buat komunikasi. Kita gak bisa intercept pake proxy karena kalo sertifikatnya palsu, si aplikasi menolak untuk jalan.

Apa yang kalian pikirkan untuk mengakalinya?

kita buka sesi tanya jawab dulu sejenak, silahkan keluarkan kreatifitasnya

apa aja yang kalian pikirkan 9:36:26 PM

Randy 007 9:37:34 PM

Byspass?

Satria Ady Pradana 9:37:48 PM

silahkan jawab sebebas-bebasnya, sebelum kulanjut :D

gimana bypasnya? gambaran kasar aja 9:38:04 PM

Randy 007 9:39:35 PM

Ak jga jadi binggung tau istilahnya aja di byspass gitu

Https nya yg di byspas 9:40:16 PM

dword 9:40:21 PM

Mungkin intersep di binarynya supaya ngehasilin sertifikat yg sesuai yg kita punya. Belum pengalaman sih

Randy 007 9:40:23 PM

Bahasa kasarnya gitu

Satria Ady Pradana 9:40:44 PM

oke, ada yang lain?

miutwo 9:42:34 PM

bagaimana klo downgrade httpsnya?

Arjan Ridwan 9:43:25 PM

Aplikasinya di RE ?

Satria Ady Pradana 9:44:11 PM

oke, semua tadi bisa aja, tapi sebagai pentester kita harus mempertimbangkan waktu dan efektivitasnya.

muhammad :: rizky :: rahmattullah 9:44:14 PM

seperti ssltrip ?

miutwo 9:44:24 PM

> **muhammad :: rizky :: rahmattullah**
> seperti ssltrip ?

iya ni

localanu 9:44:48 PM

Eh,sslstrip masih mempan di wifi?

Randy 007 9:45:09 PM

Ane pernah coba tapi gagal ntah knpa?

localanu 9:46:47 PM

> **Randy 007**
> Ane pernah coba tapi gagal ntah knpa?

Ane coba malah gak kena juga,efek wifi sepi

Satria Ady Pradana 9:47:18 PM

oke, lanjut yak

tadi batasannya aadalah kalo ada anomali di koneksi maka si aplikasi akan membatalkan koneksi. Salah satu tekniknya disebut sebagai SSL pinning. Alias dia punya sertifikat pegangan jadi kalo kita bikin sertifikat palsu dia tolak. kalo koneksinya gak secure dia juga nolak.

tapi.. karena itu aplikasi android, kita punya keleluasaan untuk melakukan apapun terhadap hape kita kan?

nah pasti kalian akan berpikir, oh aplikasinya kita RE aja, diubah aja supaya gak ngecek sertifikat. 9:48:42 PM
bisa... tapi repot

nah ada salah satu teknik namanya Dynamic Binary Instrumentation (DBI), dimana kita mengubah alur program tanpa melakukan RE terlebih dahulu. Salah satu tools-nya adalah frida 9:49:47 PM

jadi dengan frida kita bisa membuat script untuk mengubah alur kerja program. Ketika dia memanggil fungsi pengecekan sertifikan, langsung saja kembalikan true untuk menandakan sertifikat cocok 9:51:18 PM

next, python untuk forensic, contohnya ... mengolah log. 9:52:46 PM

log untuk windows event, log untuk web server access, log untuk error, dsb. Mau nggak mau kita harus baca semua itu dan parsing kejadian menarik di dalamnya termasuk membuat timeline 9:54:16 PM

di forensic sebenarnya penggunaan python untuk menemukan barang bukti, bisa dari log, dari file yang hidden, dsb 9:55:23 PM

oke itu dulu bagaimana luasnya penggunaan python untuk bidang cyber security. Kita dah bahas beberapa bidang dari mulai mengolah paket jaringan sampai mengolah log. 9:56:21 PM

aku yakin pasti ada banyak pertanyaan, so silahkan

nanti harusnya bisa dispesifikkan lagi bahas apa. Ini kita bahas yang sangat generik dulu karena waktunya terbatas hehe 9:56:57 PM