Ethical Hacking - week 3 - Python: Socket en Scapy

Socket module voor netwerkcommunicatie - Een tcp server-client

De Socket-module in Python's Standard Library biedt een krachtig framework voor netwerkcommunicatie en -interactie, cruciaal voor professionals in cybersecurity en netwerkbeheer.

Sockets, in de context van netwerken, zijn eindpunten in een communicatiekanaal dat meestal tussen twee programma's op het netwerk of op hetzelfde systeem wordt gecreëerd. Python's Socket-module faciliteert het maken van dergelijke communicatiekanalen, waarbij data verzonden kan worden tussen verschillende applicaties, over zowel lokale netwerken als het internet.

Voor iemand met een focus op cybersecurity, biedt de socket-programmering de mogelijkheid om op laagniveau netwerkcommunicatie te beheersen, waardoor je in staat bent om data packets te analyseren, manipuleren en zelfs te ontwerpen. Dit kan worden gebruikt om netwerkprotocollen te testen, aanvallen te simuleren en beveiligingssystemen te valideren. Aan de andere kant, voor automatiseringsspecialisten, stelt de Socket-module je in staat om op afstand met servers te communiceren, data te verzenden/ontvangen, en zelfs op afstand bestuurde handelingen of taken uit te voeren.

De eenvoud en veelzijdigheid van Python, samen met de capaciteiten van de Socket-module, maken het een essentiële tool in de toolkit van netwerkspecialisten en cybersecurity-experts.

https://docs.python.org/3/library/socket.html

demo5.py en demo6.py:

AF_INET => ip-versie 4 SOCK_STREAM => we gaan voor een tcp-connectie (udp, sneller, minder betrouwbaar)

De verbinding wordt hier heel eenvoudig gebruikt om een boodschap te sturen van server naar client => maar heel complexe (interactieve) use cases zijn hier mogelijk.

Experimenteer!

https://realpython.com/python-sockets/

Scapy module

Scapy is een krachtige en flexibele Python-bibliotheek, uiterst waardevol voor netwerkspecialisten en cybersecurity-experts met een specialisatie in netwerkanalyse en netwerkbeveiligingsauditing. Deze bibliotheek stelt ontwikkelaars en netwerkprofessionals in staat om met een verbluffende diepte en precisie door netwerkpakketten te navigeren.

Scapy staat niet alleen het creëren van je eigen pakketten toe, maar stelt je ook in staat ze te onderscheppen, te manipuleren, en te verzenden door het netwerk, hetgeen onmisbaar is voor het uitvoeren van uitgebreide netwerktests en -analyses. Voor cybersecurity is dit een belangrijk wapen; het gebruiken van Scapy stelt experts in staat om netwerken te verkennen, potentiële kwetsbaarheden te identificeren en de robuustheid van systemen te testen tegen aanvallen zoals packet spoofing of dos-aanvallen.

Voor het automatiseren van netwerktaken stelt Scapy professionals in staat om aangepaste scripts te maken die specifieke pakketten kunnen genereren, verzenden en analyseren, wat een krachtig hulpmiddel is voor het automatiseren van netwerkdiagnoses en -tests.

Jullie zullen Scapy waarderen als een rijke bibliotheek die een diepgaande en hands-on benadering van netwerkinteractie mogelijk maakt.

https://scapy.net/

https://github.com/secdev/scapy

! pip install scapy

Voorgesteld experiment voor week 3: je bouwt met behulp van Scapy een tool die in staat is tot:

- HOST DISCOVERY: gegeven een bepaalde IP-range het netwerk te doorzoeken naar beschikbare hosts (bvb via ARP)
- SERVICE DISCOVERY: gegeven het IP-adres van één of meerdere hosts (bvb als resultaat van de hierboven beschreven sweep) voer je een poort scan uit (voor alle poorten onder 1024)
- REMOTE OS DETECTIE: je voert een actieve fingerprinting uit op één of meerdere hosts (bvb als resultaat van de hierboven beschreven sweep) en detecteert op basis hiervan het OS van de host
- PCAP ANALYSE: je analyseert één of meerdere hosts op de aanwezigheid van HTTP-verkeer (één of meerdere andere soorten verkeer mogen uiteraard ook: SMTP, POP3, IMAP)
- Je tool werkt interactief in de terminal en via command-line argumenten (argparse)
- Loggen van de bevindingen naar een tekstbestand (html, csv of pdf mogen ook)
- Test enkel in een veilige gecontroleerde setting

OF ... je bouwt een alternatieve tool met gebruik van Scapy (bij voorkeur even na goedkeuring van je docent uiteraard 😉)