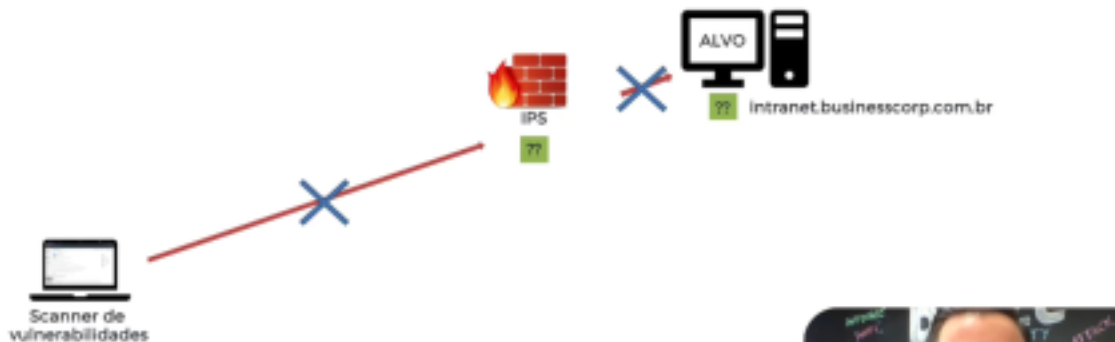


Scan Avançado (Like a Pro)

- + O objetivo aqui é passar requisitos para o scan do nessus de modo que ele seja mais assertivo no resultado
- + Como exemplo, se fizermos o scan no intranet.businesscorp.com.br, poderemos ter um resultado insatisfatório por causa do IPS

Análise Padrão: Fail

No exemplo abaixo ao executar uma análise padrão o IPS bloqueia o scanner e evitando a descoberta de informações sobre o alvo.



- + Ao realizar as pesquisas manuais, identificamos o webmin rodando na porta 10000
- + Se fizermos uma pesquisa no tenable.com/plugins por webmin, veremos que há uma falha crítica catalogada sobre webmin em CGI - abuses
- + Então, na hora de executar a ferramenta do Advanced Scan, faremos um filtro pela porta 10000 (que pode ser acessada) e então aplicaremos apenas o Plugin do CGI - abuses

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Plugins

| STATUS | PLUGIN FAMILY | TOTAL |
|----------|------------------------------------|-------|
| DISABLED | ADK Local Security Checks | 11370 |
| DISABLED | Amazon Linux Local Security Checks | 1530 |
| DISABLED | Backdoors | 126 |
| DISABLED | Brute force attacks | 26 |
| DISABLED | CentOS Local Security Checks | 2973 |
| ENABLED | CGI abuses | 4220 |
| DISABLED | CGI abuses : XSS | 682 |
| DISABLED | CISCO | 1334 |
| DISABLED | Databases | 675 |
| DISABLED | Debian Local Security Checks | 6678 |
| DISABLED | Default Unix Accounts | 171 |
| DISABLED | Denial of Service | 110 |
| DISABLED | DNS | 188 |
| DISABLED | FS Networks Local Security Checks | 861 |
| DISABLED | Fedora Local Security Checks | 15122 |

| STATUS | PLUGIN NAME |
|--------|------------------------|
| | No plugins were found. |