Evading Linux [EX]DR

Blind Spots

Everybody hooks exec()

This approach misses:

- Shell built-ins
- Output redirection, pipes

Useful Shell Built-Ins

Commands

echo

read

cd

pwd

kill

ulimit

umask

Other functionality

Regex and substitution operators

File test operators (-f, -r, etc)

Network access via /dev/tcp/…

Don't forget

/proc

Replace Commands With Shell Built-Ins

"cat" is just a loop that reads and prints lines of a file

"cp" is "cat" with output redirection

"head", "tail", and "more" are just "cat" with stopping conditions

"cut" and "wc" are loops that leverage IFS and "read"

"grep" is "cat" with a regular expression filter

"sed" is "cat" with pattern matching and substitutions

"ls" and "find" are a directory traversal with file test operations

"ps" and "netstat" read data from /proc and print it in tabular form

With Additional Implementation…

"sort" and "uniq" should be straightforward

A simple line editor like "ed"?

A URL downloader via /dev/tcp?

What's Missing?

"rm" and "mv" because we have no "unlink" operator

No links– "ln" is not a built-in

"chown", "chmod", etc

Thanks!

Questions?

hrpomeranz@gmail.com
@hal_pomeranz@infosec.exchange