naROOTo & S.A.S.U.K.E.

Rootkit Programming 2014/2015

Guru Chandrasekhara, Martin Herrmann

Technische Universität München

January 26, 2015

Overview

1. naROOTo
2. S.A.S.U.K.E. - rootkit detection
3. Other Detection methods
4. Conclusion

Overview

1. naROOTo
2. S.A.S.U.K.E. - rootkit detection
3. Other Detection methods
4. Conclusion

System call hooking

- Making write-protected memory writable using the CPU control register `cr0`

System call hooking

- Making write-protected memory writable using the CPU control register `cr0`
- Changing the pointers in the system call table

System call hooking

- Making write-protected memory writable using the CPU control register `cr0`
- Changing the pointers in the system call table
- Overwriting the first few instructions in selected functions (PUSH then RET hooking)

System call hooking

- Making write-protected memory writable using the CPU control register `cr0`
- Changing the pointers in the system call table
- Overwriting the first few instructions in selected functions (PUSH then RET hooking)
- **Problem:** Some processes don't leave `read` very fast causing slow unloading

Hooked System calls

- `read`: keylogging, covert communication

Hooked System calls

- `read`: keylogging, covert communication
- `getdents`: file hiding, process hiding (via `/proc`)

Hooked System calls

- `read`: keylogging, covert communication
- `getdents`: file hiding, process hiding (via `/proc`)
- `recvmsg`: socket hiding (TCP in `ss`)

Other hooked functions

- `packet_rcv`, `packet_rcv_spkt`, `tpacket_rcv`: packet hiding

Other hooked functions

- packet_rcv, packet_rcv_spkt, tpacket_rcv: packet hiding
- show() (for /proc/tcp): socket hiding (TCP in ss)

Other hooked functions

- `packet_rcv`, `packet_rcv_spkt`, `tpacket_rcv`: packet hiding
- `show()` (for `/proc/tcp`): socket hiding (TCP in `ss`)
- `show()` (for `/proc/udp`): socket hiding (UDP in `netstat` and `ss`)

Hiding modules

- Removing them from the list containing all `struct module *`

Hiding modules

- Removing them from the list containing all `struct module *`
- Removing them from the `kernfs` tree

Hiding modules

- Removing them from the list containing all `struct module *`
- Removing them from the `kernfs` tree
- Can hide multiple modules

Hiding modules

- Removing them from the list containing all `struct module *`
- Removing them from the `kernfs` tree
- Can hide multiple modules
- Restore from backup

Port knocking

- Using the Netfilter API in the kernel (also used by `iptables`)

Port knocking

- Using the Netfilter API in the kernel (also used by `iptables`)
- Very easy to use, just register a hook using provided functions and structures

Port knocking

- Using the Netfilter API in the kernel (also used by `iptables`)
- Very easy to use, just register a hook using provided functions and structures
- **Important:** Manually send *RST* for TCP and *ICMP Port Unreachable* for UDP

Port knocking

- Using the Netfilter API in the kernel (also used by `iptables`)
- Very easy to use, just register a hook using provided functions and structures
- **Important:** Manually send *RST* for TCP and *ICMP Port Unreachable* for UDP
- Connecting to specified ports only possible after "pinging" the following ports first (within two seconds): `12345`, `666`, `23`, `1337`, `42`

Port knocking

- Using the Netfilter API in the kernel (also used by `iptables`)
- Very easy to use, just register a hook using provided functions and structures
- **Important:** Manually send *RST* for TCP and *ICMP Port Unreachable* for UDP
- Connecting to specified ports only possible after "pinging" the following ports first (within two seconds): `12345, 666, 23, 1337, 42`
- Host may now connect two all ports with enable port knocking (until another host completes the knocking sequence)

Overview

1. naROOTo
2. S.A.S.U.K.E. - rootkit detection
3. Other Detection methods
4. Conclusion

LKM

- **S**can **A**nd **S**ubvert **U**ser-manipulated **K**ernel **E**xploits

LKM

- **S**can **A**nd **S**ubvert **U**ser-manipulated **K**ernel **E**xploits
- Check the system call table

LKM

- **S**can **A**nd **S**ubvert **U**ser-manipulated **K**ernel **E**xploits
- Check the system call table
- Check the first 16 Bytes of function instructions

LKM

- **S**can **A**nd **S**ubvert **U**ser-manipulated **K**ernel **E**xploits
- Check the system call table
- Check the first 16 Bytes of function instructions
- Loop all processes (using the `struct task *` list)

LKM

- **S**can **A**nd **S**ubvert **U**ser-manipulated **K**ernel **E**xploits
- Check the system call table
- Check the first 16 Bytes of function instructions
- Loop all processes (using the `struct task *` list)
- List contents of the `module` list, the `kobject` list, and the `kernfs` tree

LKM

- **S**can **A**nd **S**ubvert **U**ser-manipulated **K**ernel **E**xploits
- Check the system call table
- Check the first 16 Bytes of function instructions
- Loop all processes (using the `struct task *` list)
- List contents of the `module` list, the `kobject` list, and the `kernfs` tree
- List all Netfilter hooks

User-mode

- Shell script that uses `kill -0` on every possible PID (filters for good processes with existing `proc` entries)

User-mode

- Shell script that uses `kill -0` on every possible PID (filters for good processes with existing `proc` entries)
- Call a C program to hook to every TCP socket.

- We were not able to compile our tools on the system

chytryroot

- Broken `ip` command, extremely slow `scp`

chytryroot

- Broken `ip` command, extremely slow `scp`
- `sshd` on port 5167 (PID 2842)

chytryroot

- Broken `ip` command, extremely slow `scp`
- `sshd` on port 5167 (PID 2842)
- Manipulated syscall pointer to `read` and `recvmsg`

chytryroot

- Broken ip command, extremely slow scp
- sshd on port 5167 (PID 2842)
- Manipulated syscall pointer to read and recvmsg
- Manipulated instructions in all three functions of the packet_rcv family

chytryroot

- Broken `ip` command, extremely slow `scp`
- `sshd` on port 5167 (PID 2842)
- Manipulated syscall pointer to `read` and `recvmsg`
- Manipulated instructions in all three functions of the `packet_rcv` family
- Found the name of the rootkit in the `kernfs`

rootkit

- Could not compile while rootkit is inserted

rootkit

- Could not compile while rootkit is inserted
- Extreme memory issues (could not run user-mode script)

rootkit

- Could not compile while rootkit is inserted
- Extreme memory issues (could not run user-mode script)
- Hidden `sshd` on port 22 (PID 2446)

rootkit

- Could not compile while rootkit is inserted
- Extreme memory issues (could not run user-mode script)
- Hidden `sshd` on port 22 (PID 2446)
- No manipulation of the system call table

rootkit

- Could not compile while rootkit is inserted
- Extreme memory issues (could not run user-mode script)
- Hidden `sshd` on port 22 (PID 2446)
- No manipulation of the system call table
- Manipulated instructions in all three functions of the `packet_rcv` family

rootkit

- Could not compile while rootkit is inserted
- Extreme memory issues (could not run user-mode script)
- Hidden `sshd` on port 22 (PID 2446)
- No manipulation of the system call table
- Manipulated instructions in all three functions of the `packet_rcv` family
- Netfilter hook for port knocking

- Random kernel panics, reboot/shutdown not working

- Random kernel panics, reboot/shutdown not working
- Two hidden processes: `nc` on port 4321 and `bash` (PIDs 2515, 2529)

- Random kernel panics, reboot/shutdown not working
- Two hidden processes: `nc` on port 4321 and `bash` (PIDs 2515, 2529)
- No manipulation of the system call table

- Random kernel panics, reboot/shutdown not working
- Two hidden processes: `nc` on port 4321 and `bash` (PIDs 2515, 2529)
- No manipulation of the system call table
- Manipulated instructions in `read`, `recvmsg`, `packet_rcv_spkt`, and `tpacket_rcv`

g6_rkit_comcon

- Hidden `sshd` on port 7865 (PID 2834)

g6_rkit_comcon

- Hidden `sshd` on port 7865 (PID 2834)
- Manipulated syscall pointer to `read`, `getdents`, and `recvmsg`

g6_rkit_comcon

- Hidden `sshd` on port 7865 (PID 2834)
- Manipulated syscall pointer to `read`, `getdents`, and `recvmsg`
- Manipulated instructions in `tpacket_rcv`

Marvin

- Could not run user-mode script (multiple errors while using pipes)

Marvin

- Could not run user-mode script (multiple errors while using pipes)
- Hidden `nc` (PID 2799)

Marvin

- Could not run user-mode script (multiple errors while using pipes)
- Hidden `nc` (PID 2799)
- Manipulated syscall pointer to `read`, `getdents`, and `open`

Marvin

- Could not run user-mode script (multiple errors while using pipes)
- Hidden `nc` (PID 2799)
- Manipulated syscall pointer to `read`, `getdents`, and `open`
- Manipulated instructions in `packet_rcv`

Marvin

- Could not run user-mode script (multiple errors while using pipes)
- Hidden `nc` (PID 2799)
- Manipulated syscall pointer to `read`, `getdents`, and `open`
- Manipulated instructions in `packet_rcv`
- Found the name of the rootkit in the list of `kobjecs`

Marvin

- Could not run user-mode script (multiple errors while using pipes)
- Hidden `nc` (PID 2799)
- Manipulated syscall pointer to `read`, `getdents`, and `open`
- Manipulated instructions in `packet_rcv`
- Found the name of the rootkit in the list of `kobjecs`
- Netfilter hook for port knocking

External Analysis

- Looking at the .vdi file

External Analysis

- Looking at the .vdi file
- Looking at the memory

External Analysis

- Looking at the .vdi file
- Looking at the memory
- Looking at traffic from and to the VM

Conclusion

- Fun experience (both writing and detecting rootkits)

Conclusion

- Fun experience (both writing and detecting rootkits)
- Important lesson: never use copy&paste!

Discussion and comments

Thank you for your attention!